

<b>UTILITY PATENT APPLICATION TRANSMITTAL</b>  <i>(Only for new nonprovisional applications under 37 CFR 1.53(b))</i>	Attorney Docket No.	87790-837121 (000160US)
	First Inventor	Racz, Patrick
	Title	DATA STORAGE AND ACCESS SYSTEMS
	Express Mail Label No.	

<b>APPLICATION ELEMENTS</b> <i>See MPEP chapter 600 concerning utility patent application contents.</i>	<b>ADDRESS TO:</b> Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450
--	---

1. <input type="checkbox"/> Fee Transmittal Form (e.g., PTO/SB/17) 2. <input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. 3. <input checked="" type="checkbox"/> Specification [Total Pages <u>50</u> ] Both the claims and abstract must start on a new page (For information on the preferred arrangement, see MPEP 608.01(a)) 4. <input checked="" type="checkbox"/> Drawing(s) (35 U.S.C. 113) [Total Sheets <u>17</u> ] 5. Oath or Declaration [Total Sheets <u>2</u> ] a. <input type="checkbox"/> Newly executed (original or copy) b. <input checked="" type="checkbox"/> A copy from a prior application (37 CFR 1.63 (d)) (for a continuation/divisional with Box 18 completed) i. <input type="checkbox"/> DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b). 6. <input checked="" type="checkbox"/> Application Data Sheet. See 37 CFR 1.76 7. <input type="checkbox"/> CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix) <input type="checkbox"/> Landscape Table on CD 8. Nucleotide and/or Amino Acid Sequence Submission (if applicable, items a. - c. are required) a. <input type="checkbox"/> Computer Readable Form (CRF). b. Specification Sequence Listing on: i. <input type="checkbox"/> CD-ROM or CD-R (2 copies); or ii. <input type="checkbox"/> Paper c. <input type="checkbox"/> Statements verifying identity of above copies	<b>ACCOMPANYING APPLICATION PARTS</b> 9. <input type="checkbox"/> Assignment Papers (copy of previously recorded assignment) Name of Assignee _____ 10. <input checked="" type="checkbox"/> 37 CFR 3.73(b) Statement <input checked="" type="checkbox"/> Power of Attorney (when there is an assignee) 11. <input type="checkbox"/> English Translation Document (if applicable) 12. <input checked="" type="checkbox"/> Information Disclosure Statement (PTO/SB/08 or PTO-1449) <input type="checkbox"/> Copies of citations attached 13. <input checked="" type="checkbox"/> Preliminary Amendment 14. <input type="checkbox"/> Return Receipt Postcard (MPEP 503) (Should be specifically itemized) 15. <input type="checkbox"/> Certified Copy of Priority Document(s) (if foreign priority is claimed) 16. <input type="checkbox"/> Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent. 17. <input type="checkbox"/> Other: _____
--	---

18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:


Continuation     Divisional     Continuation-in-part (CIP)    of prior application No: 13/212,047

Prior application information:    Examiner THIEN MINH LE    Art Unit: 2887

#### 19. CORRESPONDENCE ADDRESS

The address associated with Customer Number: 20350    OR     Correspondence address below

Name				
Address				
City	State	Zip Code		
Country	Telephone	Email		

Signature		Date	<b>April 3, 2012</b>
Name (Print/Type)	Babak Kusha	Registration No. (Attorney/Agent)	51,095

64087665 v1

## Application Data Sheet

### Application Information

Application number::

Filing Date::

Application Type:: Regular

Subject Matter:: Utility

Suggested classification::

Suggested Group Art Unit::

CD-ROM or CD-R??:

Number of CD disks::

Number of copies of CDs::

Sequence Submission::

Computer Readable Form (CRF)?:

Number of copies of CRF::

Title:: Data Storage and Access Systems

Attorney Docket Number:: 87790-837121 (000160US)

Request for Early Publication:: No

Request for Non-Publication:: No

Suggested Drawing Figure::

Total Drawing Sheets:: 17

Small Entity?:: Yes

Latin name::

Variety denomination name::

Petition included?:: No

Petition Type::

Licensed US Govt. Agency::

Contract or Grant Numbers One::

Secrecy Order in Parent Appl.: No

## **Applicant Information**

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: United Kingdom  
Status:: Full Capacity  
Given Name:: Patrick  
Middle Name::  
Family Name:: Racz  
Name Suffix::  
City of Residence:: Saint Heller  
State or Province of Residence:: Jersey  
Country of Residence:: United Kingdom  
Street of Mailing Address:: 19 Royal Street  
City of Mailing Address:: Saint Heller  
State or Province of mailing address:: Jersey  
Country of mailing address:: United Kingdom  
Postal or Zip Code of mailing address:: JE1 4WA

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: Netherlands  
Status:: Full Capacity  
Given Name:: Hermen-ard  
Middle Name::  
Family Name:: Hulst  
Name Suffix::  
City of Residence:: Amsterdam  
State or Province of Residence::  
Country of Residence:: Netherlands  
Street of Mailing Address:: Van Tuyll van Serooskerweg 75hs  
City of Mailing Address:: Amsterdam  
State or Province of mailing address::  
Country of mailing address:: Netherlands

Postal or Zip Code of mailing address:: 1076 JG

**Correspondence Information**

Correspondence Customer Number:: 20350

**Representative Information**

Representative Customer Number:: 20350

**Domestic Priority Information**

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application is a	Continuation of	13/212,047	08/17/11
13/212,047	Continuation of	12/943,872	11/10/10
12/943,872	Continuation of	12/014,558	01/15/08
12/014,558	Continuation of	11/336,758	01/19/06
11/336,758	Continuation of	10/111,716	09/17/02

**Foreign Priority Information**

Country::	Application number::	Filing Date::
PCT	GB00104110	10/25/00
United Kingdom	9925227.2	10/25/99

**Assignee Information**

Assignee Name:: Smartflash Technologies Limited  
Street of mailing address:: 1070908 Palm Grove House, P.O. Box 438  
City of mailing address:: Wickhams' Cay, Road Town  
State or Province of mailing address:: Tortola  
Country of mailing address:: British Virgin Islands  
Postal or Zip Code of mailing address::

<b>DECLARATION FOR UTILITY OR                  DESIGN                  PATENT APPLICATION</b> (37 CFR 1.63)	Attorney Docket Number		080379-000000US
	First Named Inventor		HULST, Hermen-ard
	<b>COMPLETE IF KNOWN</b>		
	Application Number	10/111,716	
	Filing Date	October 25, 2000	
	Art Unit		
Examiner Name			
<input type="checkbox"/> Declaration Submitted With Initial Filing      OR <input checked="" type="checkbox"/> Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16(e)) required)			

As the below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original and first inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**DATA STORAGE AND ACCESS SYSTEMS**

the specification of which *(Title of the Invention)*

is attached hereto

OR

was filed on (MM/DD/YYYY) **10/25/00** as United States Application Number or PCT International

Application Number **10/111,716** and was amended on (MM/DD/YYYY)  (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
9925227.2	Great Britain	10/25/1999	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

## DECLARATION — Utility or Design Patent Application

Direct all correspondence to:  Customer Number or Bar Code Label 20350 OR  Correspondence address below

Name \_\_\_\_\_

Address \_\_\_\_\_

City _____	State _____	ZIP _____
Country _____	Telephone _____	Fax _____

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: \_\_\_\_\_  A petition has been filed for this unsigned inventor

Hermen—ard Given Name (first and middle (if any))	...HULST Family Name or Surname
---	---------------------------------------

Inventor's Signature 	Date <u>June 12<sup>th</sup> 2002</u>
---	---------------------------------------

Amsterdam Residence: City	State _____	Netherlands Country	Dutch Citizenship
------------------------------	-------------	------------------------	----------------------

Van Tuyll van Serooskerkenweg 75hS  
Mailing Address

Amsterdam City	State _____	1076 JG ZIP	Netherlands Country
-------------------	-------------	----------------	------------------------

NAME OF SECOND INVENTOR: \_\_\_\_\_  A petition has been filed for this unsigned inventor

Patrick Sandor Given Name (first and middle (if any))	RACZ Family Name or Surname
---	-----------------------------------

Inventor's Signature 	Date <u>12/5/02</u>
--	---------------------

St. Heller, Jersey Residence: City	State _____	Great Britain Country	GB Citizenship
---------------------------------------	-------------	--------------------------	-------------------

19 Royal Square  
Mailing Address

St. Heller, Jersey City	State _____	JE1 4WA ZIP	Great Britain Country
----------------------------	-------------	----------------	--------------------------

Additional inventors are being named on the \_\_\_\_\_ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.

Substitute for form 1449/PTO				<b>Complete if Known</b>		
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)				Application Number		
				Filing Date		
				First Named Inventor		Racz, Patrick
				Art Unit		
				Examiner Name		
Sheet	1	of	3	Attorney Docket Number	87790-837121	

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. <sup>1</sup>	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number Kind Code <sup>2 (if known)</sup>			
	AA	US 2003/0163594	8/28/2003	Aasheim et al.	
	AB	US 2003/0168515 A1	9/11/2003	Gray	
	AC	US 2006/0179211	8/10/2006	Aasheim et al.	
	AD	US 2006/0249570	11/9/2006	Seifert et al.	
	AE	US 2007/0162300	7/12/2007	Roever et al.	
	AF	US 2008/0041938	2/21/2008	Wise	
	AG	US 2008/0314974	12/25/2008	Hulst et al.	
	AH	US 4,341,951	Jul-82	Benton	
	AI	US 4,341,951	7/27/1982	Benton	
	AJ	US 4,697,073	9/29/1987	Hara	
	AK	US 5,148,432	9/15/1992	Gordon et al.	
	AL	US 5,226,145	7/6/1993	Moronaga et al.	
	AM	US 5,226,145	7/6/1993	Moronaga et al.	
	AN	US 5,367,150	11/22/1994	Kitta et al.	
	AO	US 5,406,619	4/11/1995	Akhteruzzaman et al.	
	AP	US 5,457,746	10/10/1995	Dolphin	
	AQ	US 5,532,466	7/2/1996	Konno et al.	
	AR	US 5,588,146	12/24/1996	Leroux	
	AS	US 5,677,953	10/14/1997	Dolphin	
	AT	US 5,703,951	12/30/1997	Dolphin	
	AU	US 5,740,369	4/14/1998	Yokozawa et al.	
	AV	US 5,744,787	4/28/1998	Teicher	
	AW	US 5,754,654	5/19/1998	Hiroya et al.	
	AX	US 5,794,202	8/11/1998	Kim	
	AY	US 5,809,241	9/15/1998	Hanel et al.	
	AZ	US 5,845,201	12/1/1998	Funke et al.	
	BA	US 5,845,281 A	12/1/1998	Benson et al.	
	BB	US 5,847,372	12/8/1998	Kreft	
	BC	US 5,874,760	2/23/1999	Burns et al.	
	BD	US 5,889,860	3/30/1999	Eller et al.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				<b>Complete if Known</b>	
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  <i>(Use as many sheets as necessary)</i>				Application Number	
				Filing Date	
				First Named Inventor	Racz, Patrick
				Art Unit	
				Examiner Name	
Sheet	2	of	3	Attorney Docket Number	87790-837121

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. <sup>1</sup>	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number Kind Code <sup>2 (if known)</sup>			
	BE	US 5,901,330	5/4/1999	Sun et al.	
	BF	US 5,918,213	6/29/1999	Bernard et al.	
	BG	US 5,923,884	7/13/1999	Peyret et al.	
	BH	US 5,933,498 A	8/3/1999	Schneck et al.	
	BI	US 5,936,220	8/10/1999	Hoshino et al.	
	BJ	US 6,012,634	1/11/2000	Brogan et al.	
	BK	US 6,018,720 A	1/25/2000	Fujimoto	Corresponds to JP 11-53184
	BL	US 6,078,917	6/20/2000	Paulsen et al.	
	BM	US 6,119,945	9/19/2000	Muller et al.	
	BN	US 6,142,369	Nov-00	Jonstromer	
	BO	US 6,202,056	3/13/2001	Nuttall	
	BP	US 6,385,731	5/7/2002	Ananda	
	BQ	US 6,415,156 B1	7/2/2002	Stadelmann	
	BR	US 6,424,975	7/23/2002	Walter et al.	
	BS	US 6,442,570	8/27/2002	Wu	
	BT	US 6,473,829	10/29/2002	Dahman et al.	
	BU	US 6,510,236	1/21/2003	Crane et al.	
	BV	US 6,553,413	4/22/2003	Leighton et al.	
	BW	US 6,554,192	4/29/2003	Tingl	
	BX	US 6,574,643	6/3/2003	Walter et al.	
	BY	US 6,658,568 B1	12/2/2003	Ginter et al.	
	BZ	US 6,721,749	4/13/2004	Najm et al.	
	CA	US 6,747,930 B1	6/8/2004	Weldon et al.	
	CB	US 6,993,507	1/31/2006	Meyer et al.	
	CC	US 6,999,936	2/14/2006	Sehr	
	CD	US 7,000,836 B2	2/21/2006	Saeki	
	CE	US 7,044,362	5/16/2006	Yu	
	CF	US 7,083,081	8/1/2006	McGee et al.	
	CG	US 7,334,720	2/26/2008	Hulst et al.	
	CH	US 7,677,446	3/16/2010	Wise	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.



Substitute for form 1449/PTO				<i>Complete if Known</i>		
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)				Application Number		
				Filing Date		
				First Named Inventor		Racz, Patrick
				Art Unit		
				Examiner Name		
Sheet	3	of	3	Attorney Docket Number	87790-837121	

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No. <sup>1</sup>	Document Number		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number Kind Code <sup>2</sup> (if known)				
	CI	US 7,942,317		5/17/2011	Racz et al.	

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No. <sup>1</sup>	Foreign Patent Document			Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Country Code <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (if known)				
	CJ	EP	0 195 098		10-03-1990	FPDC, Inc.		<input type="checkbox"/>
	CK	EP	0 542 298		04-22-1998	Hitachi, Ltd.		<input type="checkbox"/>
	CL	EP	0 713 198	A2	05-22-1996	Nederland PTT		<input type="checkbox"/>
	CM	EP	0 823 694	A1	02-11-1998	Citibank NA		<input type="checkbox"/>
	CN	EP	0 843 449	A2	05-07-1998	Sunhawk Corp. Inc.		<input type="checkbox"/>
	CO	EP	0 914 001	A1	05-06-1999	Canal Plus SA		<input type="checkbox"/>
	CP	JP	10-269291	A	10-09-1998	Sony Corp.		<input type="checkbox"/>
	CQ	JP	11-212785	A	08-06-1999	Casio Comput. Co. Ltd.		<input type="checkbox"/>
	CR	JP	11-213010	A	08-06-1999	Planet Computer:KK		<input type="checkbox"/>
	CS	JP	11-272762	A	10-08-1999	Hitachi Ltd.		<input type="checkbox"/>
	CT	JP	11-53184	A	02-26-1999	Seta:KK	Corresponds to US 6,018,720	<input checked="" type="checkbox"/>
	CU	WO	98/19237	A1	05-07-1998	Schulumberger Technologies, Inc.		<input type="checkbox"/>
	CV	WO	98/33343		07-30-1998	Sonera OY et al.		<input type="checkbox"/>
	CW	WO	98/37526		08-27-1998	Mondex Int. Ltd.		<input type="checkbox"/>

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials *	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>62</sup>

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	12462263
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	Data Storage and Access Systems
<b>First Named Inventor/Applicant Name:</b>	Patrick Racz
<b>Customer Number:</b>	20350
<b>Filer:</b>	Babak Kusha/William Chinn
<b>Filer Authorized By:</b>	Babak Kusha
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	03-APR-2012
<b>Filing Date:</b>	
<b>Time Stamp:</b>	19:35:32
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Marks_and_Clerks_87790_837 121_Continuation_Application _Transmittals_As_Filed.PDF	4327639  a4098e9c0c2a815d179bde174848606d057 4ed8d	yes	80

<b>Multipart Description/PDF files in .zip description</b>					
<b>Document Description</b>			<b>Start</b>	<b>End</b>	
Transmittal of New Application			1	1	
Application Data Sheet			2	4	
Oath or Declaration filed			5	6	
Power of Attorney			7	7	
Assignee showing of ownership per 37 CFR 3.73(b).			8	8	
Preliminary Amendment			9	9	
Claims			10	11	
Applicant Arguments/Remarks Made in an Amendment			12	12	
Specification			13	49	
Claims			50	62	
Abstract			63	63	
Drawings-only black and white line drawings			64	80	
<b>Warnings:</b>					
<b>Information:</b>					
2		Marks_and_Clerks_87790_837 121_Continuation_IDS.PDF	272790	yes	5
			4c230192e9a9aa23b4444bb88eb18c0951b 31baf		
<b>Multipart Description/PDF files in .zip description</b>					
<b>Document Description</b>			<b>Start</b>	<b>End</b>	
Transmittal Letter			1	2	
Information Disclosure Statement (IDS) Form (SB08)			3	5	
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			4600429		

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

**POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO**

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

Practitioners associated with the Customer Number: 20350

OR

Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b). I further authorize any of the above-identified practitioners to execute a Statement Under 37 CFR 3.73(b) on the undersigned's behalf to certify the chain of title and establish the undersigned's ownership in any and all patent applications in which rights have been assigned to the undersigned.

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

The address associated with Customer Number: 20350

OR

<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		


Assignee Name and Address:

Smartflash Technologies Limited  
1070908 Palm Grove House, P.O. Box 438  
Wickhams' Cay, Road Town  
Tortola  
British Virgin Islands

**A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.**

**SIGNATURE of Assignee of Record**

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	19.01.2011
Name	MAURICE EMERY	Telephone	+41 32 723 2500
Title	a director		

63097047 v1

For and on behalf of Kestrel S.A.,  
acting in its capacity as corporate director  
of Smartflash Technologies Ltd

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**STATEMENT UNDER 37 CFR 3.73(b)**

Applicant/Patent Owner: Smartflash Technologies Limited

Application No./Patent No.: \_\_\_\_\_ Filed/Issue Date: Herewith

Titled: DATA STORAGE AND ACCESS SYSTEMS

Smartflash Technologies Limited, a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

- 1.  the assignee of the entire right, title, and interest in;
- 2.  an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is \_\_\_\_\_ %); or
- 3.  the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A.  An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 013583, Frame 0554, or for which a copy therefore is attached.

OR

B.  A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

2. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

3. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

Additional documents in the chain of title are listed on a supplemental sheet(s).

As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature

08/17/2011  
Date

Jason D. Lohr, Reg. No. 48,163

Attorney Representing Client

Printed or Typed Name

Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on April 3, 2012.

PATENT  
Attorney Docket No. 87790-837121 (000160US)  
Client Ref. No. PN759544USG

KILPATRICK TOWNSEND & STOCKTON LLP

By: William Chinn  
William Chinn

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

PATRICK RACZ, ET AL.

Application No. (not yet assigned)

Filed: (herewith)

For: DATA STORAGE AND ACCESS SYSTEMS

Customer No. 20350

Confirmation No. (not yet assigned)

Examiner: (not yet assigned)

Art Unit: (not yet assigned)

PRELIMINARY AMENDMENT

April 3, 2012  
San Francisco, CA 94111

Mail Stop PCT  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

Prior to examination of the above-referenced application, please enter the following amendments and remarks:

**Amendments to the Claims** are reflected in the listing of the claim which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 4 of this paper.

**Amendments to the Claims:**

This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of Claims:**

Claims 1-39 (canceled):

Claim 40 (new): A handheld multimedia terminal, comprising:

a wireless interface configured to interface with a wireless network for accessing a remote computer system;

non-volatile memory configured to store multimedia content, wherein said multimedia content comprises one or more of music data, video data and computer game data;

a program store storing processor control code;

a processor coupled to said non-volatile memory, said program store, said wireless interface and

a user interface to allow a user to select and play said multimedia content;

a display for displaying one or both of said played multimedia content and data relating to said played multimedia content;

wherein the processor control code comprises:

code to request identifier data identifying one or more items of multimedia content stored in the non-volatile memory;

code to receive said identifier data;

code to present to a user on said display said identified one or more items of multimedia content available from the non-volatile memory;

code to receive a user selection to select at least one of said one or more of said stored items of multimedia content;

code responsive to said user selection of said at least one selected item of multimedia content to transmit payment data relating to payment for said at least one selected item of multimedia content via said wireless interface for validation by a payment validation



system;

code to receive payment validation data via said wireless interface defining if said payment validation system has validated payment for said at least one selected item of multimedia content; and

code to control access to said at least one selected item of multimedia content on said terminal responsive to said payment validation data,

wherein said user interface is operable to enable a user to select said at least one item of multimedia content available from said non-volatile memory; and

wherein said user interface is operable to enable a user to access said at least one selected item of multimedia content responsive to said code to control access permitting access to said at least one selected item of multimedia content.

**REMARKS/ARGUMENTS**

Claims 1-39 from the prior continuation application has been canceled.

Claims 40 is new and is presently pending.

**CONCLUSION**

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,



Babak Kusha  
Reg. No. 51,095

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 415-576-0200  
Fax: 415-576-0300  
Attachments  
BK:wlc  
64088294 v1

**PATENT APPLICATION**

**DATA STORAGE AND ACCESS SYSTEMS**

Inventor(s): Patrick Racz, a citizen of United Kingdom, residing at  
19 Royal Street  
Saint Heller, JE1 4WA Jersey

Hermen-ard Hulst, a citizen of Netherlands, residing at  
Van Tuyll van Serooskerweg 75hs  
Amsterdam, 1076 JG  
Netherlands

Assignee: Smartflash Technologies Limited  
1070908 Palm Grove House, PO Box 438  
Wickhams' Cay, Road Town  
British Virgin Islands

Entity: Small

## DATA STORAGE AND ACCESS SYSTEMS

## CROSS-REFERENCES TO RELATED APPLICATIONS

**[0001]** This application is a continuation of U.S. Patent Application Number 12/943,872, filed  
5 on November 10, 2010; which is a continuation of U.S. Patent Application Number 12/014,558,  
filed on January 15, 2008, now issued U.S. Patent Number 7,942,317; which is a continuation of  
U.S. Patent Application No. 11/336,758, filed on January 19, 2006, now issued U.S. Patent  
Number 7,334,720; which is a continuation of U.S. Patent Application No. 10/111,716, filed on  
10 September 17, 2002, which application is a national stage application under 35 U.S.C. 371,  
claiming the priority of international PCT Application No. GB00104110, filed on October 25,  
2000; which claims priority to UK Application No. 9925227.2, filed on October 25, 1999, each  
of which is incorporated by reference in its entirety for all purposes.

## BACKGROUND OF THE INVENTION

15 **[0002]** This invention is generally concerned with data storage and access systems. More  
particularly, it relates to a portable data carrier for storing and paying for data and to computer  
systems for providing access to data to be stored. The invention also includes corresponding  
methods and computer programs. The invention is particularly useful for managing stored audio  
and video data, but may also be applied to storage and access of text and software, including  
20 games, as well as other types of data.

**[0003]** One problem associated with the increasingly wide use of the internet is the growing  
prevalence of so-called data pirates. Such pirates obtain data either by unauthorized or  
legitimate means and then make this data available essentially world-wide over the internet  
without authorization. Data can be a very valuable commodity, but once it has been published  
25 on the internet it is difficult to police access to and use of it by internet users who may not even  
realize that it is pirated. This is a particular problem with audio recordings, and, once the  
bandwidth becomes available, is also likely to be evident with video.

**[0004]** Over the past three or four years compressed audio sources have become increasingly  
widely available on web pages. One widely used audio data compression format is MP3 (MPEG

- Audio Layer 3 of the MPEG1 compression algorithm), which is an internationally defined standard including a definition of compressed audio information such as speech or music. It relies on psycho-acoustic properties of human hearing to achieve very large data compression factors. It is thus feasible to download usefully long passages of music in a practically convenient short time. Pirate data suppliers have not been slow to realize the potential of this, and many unauthorized websites have sprung up offering popular music, including recent releases by world-famous bands. This has caused the recording industry considerable concern and there is an urgent need to find a way to address the problem of data piracy.

#### SUMMARY OF THE INVENTION

10 [0005] According to the present invention there is therefore provided a method of providing portable data comprising providing a portable data storage device comprising downloaded data storage means and payment validation means; providing a terminal for internet access; coupling the portable data storage device to the terminal; reading payment information from the payment validation means using the terminal; validating the payment information; and downloading data  
15 into the portable storage device from a data supplier.

[0006] Another aspect of the invention provides a corresponding mobile data retrieval device for retrieving and outputting data such as stored music and/or noise from the data storage device.

[0007] The payment validation means is, for example, means to validate payment with an external authority such as a bank or building society. The combination of the payment validation  
20 means with the data storage means allows the access to the downloaded data which is to be stored by the data storage means, to be made conditional upon checked and validated payment being made for the data. Binding the data access and payment together allows the legitimate owners of the data to make the data available themselves over the internet without fear of loss of revenue, thus undermining the position of data pirates.

25 [0008] A further advantage of the system is that it allows users under the age of 18 to make internet purchases. Currently internet users pay for goods and/or services by credit card. Since credit cards cannot legitimately be used by persons under the age of 18 (at least in the UK), a significant fraction of adventurous internet users are excluded from e-commerce, one of the most significant predicted uses of the internet. In one embodiment of the invention, however, the  
30 payment validation means comprises e-cash; that is, the payment validation means stores transaction value information on a cash value of transactions validatable by the data storage

means. In simple terms, the data storage means can be a card which is charged up to a desired cash value (if necessary limited to a maximum value) at a suitable terminal. This might be an internet access terminal but could, more simply, be a device to accept the data storage card and to receive and count money deposited by the user to charge the card, writing update cash value information onto the card. More sophisticated ways of updating the cash value on the card are also possible, such as direct bank transfer. Since, with this type of embodiment, the data storage means is, essentially, precharged with cash rather than acting as a credit card, it can be used by young people without the risk of their incurring large debts.

[0009] In one embodiment the data storage means is powered by the retrieval device when it is connected to the device and retains a memory of the downloaded data when it is unpowered. This can be achieved by the use of Flash RAM or, more generally, any form of programmable read-only memory. Alternatively the data storage means may incorporate a rechargeable cell or capacitor and store information in battery backed-up static RAM.

[0010] The downloaded data may be entered into the data storage device by means of an interface such as a magnetically or capacitatively coupled connection or an optical connection, but preferably the interface comprises contacts for direct electrical connection to the storage means. The payment validation means may likewise have one of a variety of interfaces but again preferably comprises a set of electrical contacts. The payment validation means could, however, comprise a magnetic or holographic data-strip such as is known for use with credit cards and phone cards. The interface to receive the downloaded data may be separate from the interface to the payment validation means, to facilitate separate and simultaneous access to both these systems. In other embodiments a single interface may serve for both data storage and payment. Advantageously the payment validation means includes memory storing information to identify the person who is paying for the downloaded data.

[0011] For additional security the downloaded data may be encrypted. In this case data decryption may be necessary at some stage, either in the data storage means or in the retrieval device or in an information delivering apparatus such as a data access terminal. Alternatively the data decryption function can be shared amongst one or more of these devices. The skilled person will be aware of a range of suitable encryption/decryption techniques, including Pretty Good Privacy (Registered Trade Mark) and PKI (Public Key Infrastructure). Normally, when the downloaded data is encrypted, a decryption key must be supplied. This can be generated

automatically by the data access terminal or data access service provider or it can be entered by the user into the data access terminal or into the mobile data retrieval device.

5 [0012] The data storage means and/or the retrieval device can be provided with access control means to prevent unauthorized access to the downloaded data. Additionally or alternatively, use control means can be provided to stop or provide only limited access of the user to the downloaded data in accordance with the amount paid. These access and use control functions may in some embodiments be combined, permitted use controlling access or permitted access controlling use. Thus, for example, a complete set of data information relating to a particular topic, a particular music track, or a particular software package might be downloaded, although  
10 access to part of the data set might thereafter be controlled by payments made by a user at a later stage. In this way, a user could pay to enable an extra level on a game or to enable further tracks of an album.

15 [0013] In embodiments where the access or use control means is responsive to the payment validation means, access or use control information may be stored with the downloaded data or in a separate storage area, for example in the payment validation means. The user's access to the downloaded data could advantageously be responsive to the payment validation means, for example, by means of a control line coupling the payment validation means with a memory access or decryption control element.

20 [0014] In one embodiment the data storage means comprises an electronic memory card or smart card and the mobile data retrieval device is provided with a slot to receive the card. Preferably the card is a push-fit within the retrieval device, and retention of the card may be effected by pressure from electrical interface connections and/or resilience of the housing, or by using a resilient retaining means. In a preferred embodiment the retrieval device includes an audio output and a display, to play a downloaded track and to show information about the track  
25 and/or an accompanying video.

[0015] To download data onto the data storage means the user can employ a data access terminal coupled to the internet. The terminal can directly validate payment; for example in the case of a smart card charged with electronic cash it can deduct a cash value from the card. Alternatively it can communicate with a bank or other financial services provider to control  
30 payment. In a preferred embodiment, however, the terminal connects to a data access service provider which provides a portal to other sites and which validates payment and then forwards

data from a data supplier to the user's local access terminal. The data access service provider may alternatively forward payment validation information and/or information from the payment validation authority to the data supplier for control by the supplier of the data supplied. Thus, access to the payment validation system and/or data for downloading may be entirely controlled  
5 by the data supplier.

[0016] Data held on the data storage means may advantageously include data relating to the user's or payer's usage of the system. This information may include, for example, information on a user's spending pattern, information on data suppliers used and information on the downloaded data. This information may be accessed by the data supplier and/or data access  
10 service provider and can be used for targeted marketing or loyalty-based incentive schemes such as air miles or the like.

[0017] The data access terminal may be a conventional computer or, alternatively, it may be a mobile phone. Wireless Application Protocol (WAP) and i-mode allow mobile phones to efficiently access the internet and this allows a mobile phone to be used to download data to the  
15 data storage means, advantageously, directly. The data storage means can, if desired, incorporate the functionality of a mobile phone SIM (Subscriber Identity Module) card, which cards already include a user identification means, to allow user billing through the phone network operator.

[0018] In a preferred embodiment the downloaded data is MP3 or other encoded audio data, but the system finds more general application for other data types. For example, download data  
20 can include software, and particularly games, share price information, current news information, transport timetable information, weather information and catalog shopping information. The downloaded information may also include compressed video data. The storage capacity of the data storage means is adaptable to suit the type of data intended to be downloaded; for example, 32 megabytes is sufficient for CD quality music, but for video it is preferable that the data  
25 storage means has a capacity of 128 megabytes or greater.

[0019] In another aspect, the invention provides a portable data carrier comprising an interface for reading and writing data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; non-volatile payment data memory, coupled to the interface, for providing payment data to an external device.



[0020] These features allow the data carrier to store both payment data and content data, thus providing the advantages outlined above. Depending upon the payment system used, the payment data memory may also store code for validating or confirming a payment to an external payment system. The payment data will normally be linked to a card or card holder  
5 identification data for payment by the card holder. The non-volatile memory ensures that stored content and payment data is retained in the data carrier when the data carrier is not receiving power from an external source. Thus "non-volatile" encompasses, for example, low-power memory whose contents are retained by a battery back-up system. In one embodiment the payment data memory comprises EEPROM and the content data memory comprises Flash  
10 memory, but other types of content data memory, such as optical, for example, holographic, data memory can also be used. The data carrier may also be integrated into other apparatus, such as a mobile communications device.

[0021] Preferably, the portable data carrier further comprises a program store for storing code implementable by a processor; and a processor, coupled to the content data memory, the payment  
15 data memory, the interface and to the program store for implementing code in the program store, wherein the code comprises code to output payment data from the payment data memory to the interface and code to provide external access to the data memory.

[0022] Normally, the (content) data memory allows both write and read access for both storing and retrieving data, but in some embodiments the content data memory may be read-only  
20 memory (ROM). In such embodiments, content may be pre-loaded onto the carrier and payment may then be made for permission to access the pre-loaded data.

[0023] Preferably, the data carrier also stores a record of access made to the content data and updates this in response to external access, preferably read access, made to the data memory. The carrier may also store content use rules pertaining to allowed use of stored data items. These  
25 use rules may be linked to payments made from the card to provide payment options such as access to buy content data outright; rental access to content data for a time period or for a specified number of access events; and/or rental/purchase, for example where rental use is provided together with an option to purchase content data at the reduced price after rental access has expired.

[0024] Thus where the data carrier stores, for example, music, the purchase outright option  
30 may be equivalent to the purchase of a compact disc (CD), preferably with some form of content

copy protection such as digital watermarking. In this example, the rental or subscription payment option may be a pay-per-play option, and with this option payment may either be before or after access to the stored data so that the carrier may operate in either a debit or credit payment mode.

5 [0025] The portability of the data carrier potentially allows it to be used to access content or, in the example, play music without the need to be linked to a communications system or to be on-line to the internet. By providing a use record memory on the data carrier, use of the stored data can be tracked while off-line and then any necessary payment can be made when the data carrier is next coupled to a communication system. This allows the data carrier to operate in a credit  
10 mode. In a debit mode, the additional storage of use rules facilitates the regulation of access to content data stored on the carrier without the need for further exchange of payment/use data with an external system to validate the use.

[0026] By combining digital rights management with content data storage using a single carrier, the stored content data becomes mobile and can be accessed anywhere while retaining  
15 control over the stored data for the data content provider or data copyright owner. Preferably, the data carrier also stores access control data, such as a user ID and a password, as the stored data may be valuable. The access control data may be combined with access control to the payment data, which is typically by means of a PIN (Personal Identification Number) to simplify access to valued content stored on the carrier.

20 [0027] In one embodiment the stored content data is encrypted and a unique password or PIN and/or biometric data is required for decryption. The data carrier may be arranged so that the content is erased after a predetermined number of incorrect access attempts. Additionally or alternatively, a permanently stored flag may be set and/or a hardware modification (such as a fusible link) may be made to prevent the data carrier from functioning for further data  
25 storage/retrieval. Preferably, however, access to any stored value/payment data is nevertheless retained.

[0028] Supplementary data may also be stored on the carrier in association with stored content data. This supplementary data may comprise customer reward management data and/or advertising data. The supplementary data may comprise a pointer to an external data source  
30 from which data is downloaded either to the data carrier or to a data access device or content

player, so that advertising or other data can be displayed when reviewing or accessing the stored content.

5 [0029] Additional data security and/or a mechanism for rewarding operators at different levels in the data supply chain may be provided using a content synthesis function. The content synthesis function combines partial content information from two or more sources to provide content data items for storage and/or output. Thus, for example, a first percentage of a content data item could be provided by a content retailer, while a remaining percentage could be provided by an on-line data supplier. This would provide an incentive for a user to register with a content retailer or distributor as well as with an on-line system owner and so could encourage the use of existing retailers and could provide a mechanism for paying commission to such retailers. The two portions of data combined to provide a content data item could comprise encryption data and a key but preferably comprise separate parts of a complete data item, for example, least significant bits and most significant bits or high frequencies and low frequencies (for audio). This arrangement also facilitates customer reward and loyalty management.

15 [0030] In one embodiment the data carrier further comprises memory for storing data for accessing a mobile communications network, for example to receive content data over the network. For such an embodiment, the data carrier may replace a SIM (Subscriber Identity Module) card in a mobile communications device, thus providing a single card for both network access and valued content retrieval and storage. Additionally or alternatively the card may also store the web address of a data supplier from whom data may be downloaded onto the carrier.

20 [0031] The data memory for storing content data may be optic, magnetic or semiconductor memory, but preferably comprises Flash memory. Preferably, the data memory has a large capacity for storing large data files such as compressed video data. Preferably, the data memory is partitioned for lock access, that is, for read and/or write access to blocks of, for example, 1K, 4K, 16K or 64K databytes for faster data access, particularly where the stored content data will normally be accessed serially, as is normally the case with audio and video data. Preferably the card is configured as an IC card or smart card and has a credit card-type format, although other formats such as the "memory stick" format may also be used. This provides a small and convenient portable format and facilitates removable interfacing with a variety of devices.

25 [0032] The invention also provides a related method of controlling access to data on a data carrier, the data carrier comprising non-volatile data memory and non-volatile parameter

memory storing use status data and use rules, the method comprising receiving a data access request; reading the use status data and use rules from memory; and evaluating the use status data using the use rules to determine whether access to the stored data is permitted.

5 [0033] According to another aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a pointer to a data provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored  
10 code, the code comprising code to receive a request for a data item from the requester; code to receive from the communications interface payment data comprising data relating to payment for the requested data item; code responsive to the request and to the received payment data, to read data for the requested data item from a content provider; and code to transmit the read data to the requester over the communications interface.

15 [0034] The computer system is operated by a data supplier or data supply "system owner" for providing content data to the data carrier described above. The payment data received may either be data relating to an actual payment made to the data supplier, or it may be a record of a payment made to an e-payment system relating either to a payment to the data supplier, or to a payment to a third party. The data from the content provider, preferably without permanent  
20 (local) storage of the forwarded data, improves data security as the content provider retains control over a content data item, and the data supplier, a copy of a data item, is unable to supply data for the item without the content provider's assistance. The computer system may provide temporary storage for a requested data item, for example using a disk cache, but preferably the computer system does not store a complete data item, even temporarily.

25 [0035] Preferably, the computer system includes payment distribution information so that when payment is made for a data item, the payment can be distributed for reimbursing royalties and making other payments. Typically a large fraction of the payment for a data item will be transferred to a copyright owner or "content provider" for the item while smaller payments will go to the artist and/or publisher and/or retailer/distributor. Payment may be made directly by the  
30 computer system to the computer systems of other relevant parties using, for example, a signature-transporting type e-payment system. Alternatively, the computer system can issue

appropriate instructions to a third party e-payment system for making the transfers. The computer system allows automatic distribution of payments either before, during or after content data download, or after content data access by a user. Instructions for distributing the payments may be issued substantially simultaneously, thereby avoiding long delays in the payment of some parties; for example, it can presently take a year or more for an artist generating content to be paid by conventional methods.

**[0036]** Preferably, the computer system also stores content data item access rule data, for downloading in association with a content data item. The rule data may be stored by a content provider but is preferably held by the computer system, and links a content identifier with an access rule, typically based upon a required payment value, as outlined above in the context of the data carrier. Normally, each content data item will have an associated access rule, but a single rule may apply to a large number of data items. The computer system also, preferably, stores requester reward data for customer reward/loyalty management. This data may again comprise one or more rules linking a payment value and/or content data item type to a specified reward, such as a number of air miles or retailer value points. The computer system preferably also keeps a record of an identified user's or data's carriers content item downloads and payments for market research purposes.

**[0037]** The computer system, in one embodiment, also stores access control data, such as an access request identity and password which can be employed, for example, to create an extranet of system users, which again can be linked to stored access record data for marketing purposes. When further linked to content item type data, such an arrangement can be used to construct a club of users of content data items of a particular type, for example country and western or rock and roll music. As described in connection with the portable data carrier, the computer system may also comprise content synthesis code for additional data security and for more secure management of payment distributions.

**[0038]** The invention also provides a related method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; reading the requested data from a content provider responsive to the received payment data; and transmitting the read data to the requester.

**[0039]** According to a further aspect of the present invention, there is provided a data access terminal for retrieving data from a data supplier and providing the retrieved data to a data carrier, the terminal comprising a first interface for communicating with the data supplier; a data carrier interface for interfacing with the data carrier; a program store storing code implementable by a processor; and a processor, coupled to the first interface, to the data carrier interface and to the program store for implementing the stored code, the code comprising: code to read payment data from the data carrier and to forward the payment data to a payment validation system; code to receive payment validation data from the payment validation system; code responsive to the payment validation data to retrieve data from the data supplier and to write the retrieved data into the data carrier.

**[0040]** This terminal can be used for retrieving data from the above-described computer system and for downloading the retrieved data to the above-described portable data carrier. As with the data supply computer system, it is preferable that there is no (local) storage of content item data forwarded from the data supplier to the data carrier. The data access terminal is not restricted to use with the above-described status supplier and could, for example, retrieve data for downloading to the data carrier from a local data source, such as a CD (Compact Disc) or DVD (Digital Versatile Disc), or from a third party such as a cable TV company.

**[0041]** The terminal reads payment data from the data carrier and transmits this to a payment validation system for validating the data and authorizing the payment. This may be part of the data supplier's computer system or it may be a separate system such as an e-payment system. Thus, the terminal operates with a data carrier storing payment (validation) data and, in some embodiments, additional payment validation code for validating payment to the payment validation system. Again, the terminal is preferably configured to provide a data item use rule to the carrier in conjunction with a data item. As before, the data item use rule will normally be dependent upon payment value information embodied in the payment data read from the data carrier. The terminal is preferably also configured for user input of access control data. This access control data may be forwarded to the data carrier for access permission verification and/or it may be passed to the data supplier computer system for a similar purpose. The terminal may be configured to warn a user of content access or data carrier function inhibition after a predetermined number of access requests have been refused. The terminal may also incorporate content synthesis code as described above.

**[0042]** The terminal may comprise code to output supplementary data when downloading data to the data carrier. Identity data on the data carrier can be used to retrieve the supplementary data, or a pointer to the supplementary data, from the data supplier computer system, or the supplementary data or a pointer thereto can be retrieved directly from the data carrier.

5 Preferably, however, identification data on the card is used to retrieve characterizing data such as card user preference data from the data supplier computer system, and this characterizing data is then used by the terminal to retrieve and output supplementary data to a terminal user. When the terminal is associated with a contact distributor or retailer, the supplementary data may be retrieved over a network associated with the retailer/distributor such as a local area network  
10 (LAN), wide area network (WAN) or extranet.

**[0043]** The invention also provides a method of providing data from a data supplier to a data carrier, the method comprising reading payment data from the data carrier; forwarding the payment data to a payment validation system; retrieving data from the data supplier; and writing the retrieved data into the data carrier.

15 **[0044]** The payment validation system may be part of the data supplier's computer systems or it may be a separate e-payment system. In one embodiment the method further comprises receiving payment validation data from the payment validation system; and transmitting at least a portion of the payment validation data to the data supplier. Alternatively the payment validation system may comprise a payment processor at the data supplier or at a destination  
20 retrieved from the data supplier. The payment processor may also provide payment distribution data for distributing a payment represented by the payment data.

**[0045]** In a further aspect, the invention provides a data access device for retrieving stored data from a data carrier, the device comprising a user interface; a data carrier interface; a program store storing code implementable by a processor; and a processor coupled to the user interface, to  
25 the data carrier interface and to the program store for implementing the stored code, the code comprising code to retrieve use status data indicating a use status of data stored on the carrier, and use rules data indicating permissible use of data stored on the carrier; code to evaluate the use status data using the use rules data to determine whether access is permitted to the stored data; and code to access the stored data when access is permitted.

30 **[0046]** The data access device uses the use status data and use rules to determine what access is permitted to data stored on the data carrier. As described above, the use rules will normally be

dependent upon payments made for data stored on the data carrier, but may also comprise access control employing a user identification and password. Since a single data carrier may have more than one user, the use status and use rules may be selected dependent upon a user identity. The data access device may also be configured to present supplementary data when presenting the content data, retrieved as described above, from the card, from a remote computer system or from some other source such as a cable TV network or off-air.

**[0047]** The invention also provides a related method of controlling access to data from a data carrier, comprising retrieving use status data from the data carrier indicating past use of the stored data; retrieving use rules from the data carrier; evaluating the use status data using the use rules to determine whether access to data stored on the carrier is permitted; and permitting access to the data on the data carrier dependent on the result of said evaluating.

**[0048]** According to a further aspect of the invention there is provided a data access system comprising a data supply computer system for forwarding data from a data provider to a data access terminal; an electronic payment system for confirming an electronic payment; a data access terminal for communicating with the data supply system to write data from the data supply system onto a data carrier; and a data carrier for storing data from the data supply system and payment data; wherein data is forwarded from the data provider to the data carrier on validation of payment data provided from the data carrier to the electronic payment system.

**[0049]** In a further aspect of the invention, there is provided a portable data carrier comprising an interface for sending and receiving data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; and a digital rights management processor for controlling access to the stored data.

**[0050]** In a further aspect of the invention, there is provided a portable data carrier comprising an interface for sending and receiving data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; and an access control processor; wherein the data memory is partitioned as data blocks and the access control processor controls external access to the data blocks.

**[0051]** In a further aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data



item description and a resource locator; a data provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item; code, responsive to the request and to the received payment data, to output the item data to the requester over the communication interface; wherein said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a requester.

**[0052]** In a further aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a printer location data identifying an electronic address for a provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item; code responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein the data access data store further comprises data item access rule data for output to the requester with a data item; and further comprising code to select access rule data for output with a data item in response to the payment data.

**[0053]** In a yet further aspect of the invention, there is provided a method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; transmitting the requested data to the requester; reading payment distribution information from a data store; and outputting payment data to a payment system for distributing the payment for the requested data.

**[0054]** In a still further aspect of the invention, there is provided a method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; transmitting the

requested data to the requester; and transmitting data access rule data to the requester with the read data.

[0055] These and other aspects of the invention will now be further described, by way of example only, with reference to the accompanying figures.

## 5 BRIEF DESCRIPTION OF THE DRAWINGS

[0056] Figure 1 shows a data access device a) from the top; b) from the front; and c) from the side;

[0057] Figure 2 shows, conceptually, a portable data carrier;

[0058] Figures 3a and b show exemplary data access terminals;

10 [0059] Figures 4a and b show, respectively, a logical signal path between elements of a conceptual data access system; and a physical representation of a conceptual data access system;

[0060] Figure 5 shows a content provision system;

[0061] Figure 6 shows a data supply computer system;

[0062] Figure 7 shows a variety of data access terminals;

15 [0063] Figure 8 shows a schematic diagram of components of a data access terminal;

[0064] Figure 9 shows a schematic diagram of components of a data carrier;

[0065] Figure 10 shows a schematic diagram of components of a data access device;

[0066] Figures 11a and 11b are flow diagrams of a data carrier registration process;

20 [0067] Figures 12a-c and 12d-e show, respectively, a flow diagram of data access using a data access terminal; and a flow diagram of data supply using a data supply computer system; and

[0068] Figure 13 shows a flow diagram of data retrieval using a data access device.

## DETAILED DESCRIPTION

[0069] Referring to Figure 1, this shows a data access device for playing MP3 audio (10) with operator controls (12) and LCD display (14). The outline of a smart card data storage device is shown at (16). The operator controls allow a user to select and play tracks, while track information and still or video images are provided on display (14). A slot (18) is provided in the front of the device to receive a smart card-type data storage means. This smart card occupies

space (20) and interfaces with resilient contacts (24); it is held in the data retrieval device against the contacts, by resilient housing element (22).

[0070] Referring now to Figure 2, this shows a portable data carrier (30) suitable for use with the device of Figure 1. The data storage means is based on a standard smart card; it is plastic, about the size of a standard credit card, and has some flexibility. On the card (30) are two sets of contacts, contacts (32) for interfacing with the payment validation means and contacts (34) for interfacing with the memory for storing downloaded data (although in other embodiments, a single set of contacts may be used for both). The surface of the card can be embellished with suitable graphics.

10 [0071] In one embodiment the smart card retains all its useable functionality as specified for standard Electronics Point of Sale Systems (EPOSS) and, if desired, the memory for storing the downloaded data can be electrically separate from this. However, it may be preferable to provide interaction between the standard smart card device and the data memory in order to accomplish the access control/decryption functions described above.

15 [0072] Referring now to Figure 3, an example of a data access terminal is shown at (40). This has a screen (42) and a slot (44) to receive the data carrier (30). Alternatively the data carrier may interface to the terminal via the data access device (10) and an interface (46) to the terminal (40). In Figure 3b a dedicated terminal (50) has a slot (52) to receive the data carrier, a display (54) and controls (56). Coins can be inserted into the terminal at (58) and notes at (60) to charge  
20 the data carrier with cash.

[0073] Referring now to Figure 4a, this illustrates conceptually the logical connections and data flow between data processing systems involved in payment validation, and data download to the carrier (30). A user connects the data carrier (30) to terminal (40) and logs on to a data web page of data supply service provider (60). Either terminal (40) or service provider (60) then  
25 communicates via data paths (62) with a payment validation authority (70) to check and authorize the user's or payer's payment. In the case of electronic cash the terminal (40) may immediately validate the payment information, updating the service provider and/or payment validation authority (70) at a later stage. The logical connection (64) between the terminal and the service provider is preferably made over the internet.

[0074] The service provider may provide a direct portal to data providers (80) or may collect information from data suppliers (80) and provide a “front end” to present data from the suppliers to the terminal user. Alternatively, data supply service provider (60) may regulate direct access between terminal (40) and data providers (80), as shown by links (66), by communicating with the terminal and the data providers to provide communication regulation information to, for example, instruct data suppliers about what information the user of terminal (40) should have access to.

[0075] In a preferred embodiment, service provider (60) pays royalties at an agreed rate - for example, 10 pence per track or 10 pence per minute - to a computer system owned by a company or entity in the recording industry, such as a content provider or copyright owner, a content publisher or a content creator, and the user of terminal (40) effectively pays the service provider. Billing can also be regulated by bandwidth and/or data download time.

[0076] Preferably the service provider (60) monitors the user’s access to the system and either stores or forwards to data providers (80), or downloads to the data carrier (30), usage information. In a preferred embodiment the service provider sends information via terminal (40) to data carrier (30) which can be used to determine incentives to be provided to users of the system.

[0077] Figure 4b shows a conceptual physical configuration of the system of Figure 4a in which a plurality of terminals (40), a plurality of service providers (60) and a plurality of data providers (80) all interact via the internet. The physical embodiment of the system is not critical and a skilled person will understand that the terminals, data processing systems and the like can all take a variety of forms.

[0078] Referring now to Figure 5, this shows a conceptual illustration of a content provision system 100. Content creators 104a, b generate or receive content data from artist terminals 102a-d and store content data in databases 106a, b. The content data stored in databases 106a, b may comprise audio data, such as music, video data, such as films or TV programs, text, such as literary works, software, such as games software, or other data. Content creators 104a, b are coupled to communications network 101 for communicating created content data over the network. Also coupled to communications network 101 are content publishers 110a and 110b, each of which is coupled to an associated stored content database, 112a and 112b respectively. The content publishers make their stored content available for controlled access using

communications network 101. In some instances, for example where the content data comprises computer games, the functions of content creator and content publisher may be provided by a single entity. Also although conceptually illustrated as blocks in Figure 5, the content creator and content publisher typically each comprise a client server computer network.

5 [0079] The communications network 101 is typically a private communications network, such as an extranet, with security controlled access to entities connected to the network. Physically the network may comprise an internet protocol network or it may comprise, or consist of, dedicated point-to-point links. Thus, for example, a content creator 104 may be directly linked to a content publisher 110 and/or to other entities shown in Figure 5 such as a content provider or  
10 content distributor.

[0080] The content provision system includes a plurality of content providers 108a-e, each coupled to the communications network 101. In the illustrated system, the content providers own copyright in stored content data accessible over communications network 101 and may, in practice, also perform a content publication function. Five content providers own the copyright  
15 in over 80% of all world-wide music sales. The content providers are coupled to stored content databases 106 and 112 via communications network 101, for supplying stored content data.

[0081] A gateway server 114 is also coupled to communications network 101 to link the communications network to other networks such as the internet and/or mobile communications networks. Gateway server 114 provides security and access control functions and firewalls. A  
20 second gateway, content distributor WAN gateway 116, is also shown attached to communications network 101. This provides similar security and firewall functions and coupled communications network 101 to distributor WAN (wide area network) 117. Gateway 116 has logical access to one or more of a content creator, content publisher and content provider for accessing stored content data. Content distributor gateway 116 may be owned by a chain of  
25 record stores and provide content access terminals 118, coupled to WAN 117, in separate retail outlets. Content access terminals 118 have access, via gateway 116, to stored content accessible over communications network 101.

[0082] Referring now to Figure 6, this shows a data supply computer system 120. In this embodiment, three content access terminals 118a-c, e-payment systems 121a, b, and content  
30 access web server 124 are all coupled to internet 142. Data supply system 120 is coupled to the content provision system 100 illustrated in Figure 5. Where communications network 101 of

Figure 5 is an extranet, this extranet physically operates over internet 142; where communications network 101 does not partly operate via internet 142, a connection to internet 142 is established via gateway server 114 as shown in Figure 5. In this way content access terminals 118a-c are provided with controlled access to the stored content data of content provision system 100.

**[0083]** E-payment systems 121a and 121b are coupled to banks 122a, b and c, d respectively. These provide an e-payment system according to, for example, MONDEX, Proton, and/or Visa cash compliant standards. Preferably at least one of e-payment systems 121a, b operates a so-called "open purse" system in which the value is stored as a publicly verifiable digital signature issued by the e-payment system. In such a signature-transporting arrangement, payment data may be validated using public keys and thus payment authentication need not be performed by the e-payment system but may instead be performed by, for example, a data access terminal or data supply system computer, using payment management code. The authenticated signatures, which in effect perform a similar role to checks, are submitted to the relevant e-payment system after authentication for verification and reimbursement or transfer of monetary value. With such a system payments may be made anonymously and thus payer identification is not essential. Data carriers, such as data cards, may be issued with stored value or without value, in which latter case value (that is, a publicly verifiable digital signature) may be written onto the card during an on-line transaction.

**[0084]** In alternative embodiments, a data carrier such as the smart Flash card described below may be used to create value bearing digital signatures as is well-known to those familiar with e-money.

**[0085]** Content access web server 124 is also coupled to internet 142 for providing content access terminals 118a-c with access to content data. Content access web server 124 is typically owned by a content data supply "system owner" who acts as an intermediary between a content access terminal user and a content provider, forwarding content data provided (directly or indirectly) by a content provider to a content access terminal and then to a stored content data carrier. Web server 124 is coupled to web server code storage 126 storing Java code for generating web pages for interpretation by web browsers on content access terminals 111a-c. The web pages provide the content download, value add, CRM (customer reward management) value check/spend and website link functions described below.

[0086] Web server 124 is coupled to payment processor 128, Digital Rights Management (DRM) processor 130, access control processor 132, and content distribution processor 134. Payment processor 128 includes payment management code storage 128a and is coupled to payment record data store 136. Access control processor 132 includes access control code storage 132a and is coupled to access control data store 138. DRM processor 130 includes DRM code storage 130a and is coupled to content access and DRM data store 140. Content distribution processor 134 includes CRM (customer reward management) and payment distribution management code storage 134a and is also coupled to content access and DRM data store 140. As shown in Figure 6, processors 128-134 are all in communication with one another.

10 [0087] Processors 128, 130, 132 and 134 may comprise separate application programs or a single computer program and may operate on a single physical computer, on which web server 124 may also be provided, or may operate on separate computers. Likewise data stores 136, 138 and 140 may comprise a single physical data store or may be distributed over a plurality of physical devices and may even be at locations physically remote from processors 128-134 and  
15 coupled to these processors via internet 142.

[0088] Web server 124 communicates with processors 128-134 by means of a CGI (common gateway interface) script and the code associated with processors 128-134 may be written in any conventional computer language such as C, C++, or Perl. However, in other embodiments one or more of the processors may be coupled to web server 124 via internet 142 and owned and  
20 operated by a separate entity, such as a financial institution. In this case conventional secure web-based communications may be operated between web server 124 and the relevant processor. In particular, payment processor 128 may be operated by one of the e-payment system providers 128a, b.

[0089] Payment management code 128a issues and authenticates payment data and stores an  
25 audit record in payment record data store 136. Access control code 132a stores identification data (of a user or card) together with registration data provided by a user when registering with the system owner. This data comprises a user password for accessing stored content and/or payment data; user characterizing data, for example characterizing user preferences, for marketing purposes; data indicating an e-payment system to use; and in some embodiments,  
30 further general user related data such as card level data for identifying the provision of "gold" level services to selected users. A copy of the password is stored with the content data on the

portable data carrier, as described further below. Alternatively, one or both of the access control data store and portable data carrier may simply store data for verifying a user-entered password.

5 [0090] Content access and DRM data store 140 stores data related to content access and content use, but does not itself store content data items; these are instead provided via content provision system 100 described above. Data store 140 stores a plurality of records each comprising a data item identifier, a data item description, a data item type or genre, and location data comprising one or more pointers to a location or locations from where the data item can be downloaded. Associated with a data item is also a table of use rule data comprising a list of values (i.e. content data item prices) and corresponding levels of permitted usage. Thus a value  
10 of £1 might permit ten plays of a music track, while the value of £10 might permit an unlimited number of plays of the track and copying of the track for personal use.

[0091] Also associated with a data item is a table of payment distribution data comprising a list of recipients and corresponding fractions of the data item value each is to receive. Typically, the main recipient will be the copyright owner of the data item and other recipients will be selected  
15 from the content creator, the artist or artists, the system owner, the content publisher, and the retailer/distributor. The payment distribution proportions may be dependent upon the payment value, in which case a plurality of sets of payment distribution figures may be associated with each data item, each set of distribution figures corresponding to a payment value range. The payment data and distribution data is here termed DRM (Digital Rights Management) data.

20 [0092] Further associated with a data item is a table of CRM (Customer Reward Management) data, linked to the user rule data, comprising CRM rules to specify, for one or more data item use levels, a quantity of reward points and one or more recipients for the reward points (the recipients may include the card user and the retailer/distributor).

[0093] The CRM and payment distribution code 134a operates with content access and DRM  
25 data store 140 to inform a system user of the description and value of a data item, to access and download a data item from the content provider system to a content access terminal, to provide content use rules with the data item, and to provide instructions either to payment processor 128 or to e-payment system 121 to distribute payments for the data item to the recipients identified by the data store 140 and to distribute CRM reward points.



[0094] The access control data store 138 holds a secure key, such as a secret "public" key in a public key cryptography system, for the system owner to authenticate its identity to a content provider. This data is held securely with other sensitive data in the access control data store 138. As is described in more detail below, when data supply system 120 receives a request for a content data item from a content access terminal 118, it looks up a location from which the data item is available using content access and DRM data store 140 and then determines the identity of the corresponding content provider. This identity is either stored in content access and DRM data store 140 or, as there are relatively few content providers, it may be hard written in DRM code 130a. DRM code 130 then requests access control processor 132 to provide the secure system owner identifier from access control data store 138 to the relevant content provider and sets up a trusted connection between the content provider and content access web server 124 for downloading the data item to a content access terminal 118 and then to a portable data carrier.

[0095] Referring now to Figure 7, this shows a variety of content access terminals for accessing data supply computer system 120 over internet 142. The terminals are provided with an interface to a portable data carrier or "smart Flash card" (SFC) as generally described with reference to Figure 2 and as described in more detail below. In most embodiments of the terminal the SFC interface allows the smart Flash card data carrier to be inserted into and removed from the terminal, but in some embodiments the data carrier may be integral with the terminal.

[0096] Referring now to the specific embodiments illustrated in Figure 7, a simple content access terminal may comprise a home personal computer 144 with SFC interface 144a. In another embodiment, a mobile communications device 152 is provided with a smart Flash card interface 152a and is coupled to internet 142 via radio tower 150, mobile communications system 148 and mobile communications internet gateway 146.

[0097] In another embodiment, a smart Flash card interface is provided to a so-called "set top box" (STB) 154. The set top box is, in effect, a receiver for television programs received on video input 154b, which may comprise a satellite TV signal, a cable TV signal or an off-air TV signal. The video signal is provided from the set top box to television 156 or to some other home entertainment device such as a personal computer (not shown). In another embodiment, content access terminals 166 and 168 each with respective SFC interfaces 166a and 168a are coupled to a retailer local area network (LAN) 160 connected to internet 142 via retailer LAN server 158.

DVD player 164 is also coupled to LAN 160. In a further embodiment a smart Flash card interface 170a is provided for a CD/DVD player 170.

5 [0098] In these latter three embodiments, content data for storage on the smart Flash card may be retrieved from broadcast video and/or a CD or DVD. In this case, the computer data supply system 120 illustrated in Figure 6 may be used to provide use rule data for the content data stored on the smart Flash card, and to pay for data downloaded onto the card; the content data may be captured before or after the data supply system 120 is accessed to enable use of the stored data, but in a preferred embodiment content data written to the card from a supplier other than the content data supply computer system is not accessible to a user until corresponding use rule data has been downloaded from computer system 120, which will normally be after receiving payment for the downloaded data.

10 [0099] Referring now to Figure 8, this shows a schematic diagram of one embodiment of a data access terminal 170. The terminal comprises a general purpose computer including an audio/visual interface 184, a keyboard 186 and a pointing device 188 for providing an interface to the user. The terminal has an internet interface 176, for example a modem, and optionally a LAN/WAN interface 174 for connecting the terminal to a retailer or distributor LAN or WAN. The terminal also has an optional video input 178 for receiving broadcast video data and a media input device 180, such as a CD or DVD drive. Further communications I/O ports 182 may also be provided. A portable data carrier or smart Flash card interface 190 is provided for interfacing to a smart Flash card. Optionally, a cash input and verification system 192, such as is conventionally used in an automatic teller machine (ATM), may also be incorporated within the content access terminal. The terminal has working memory 194 such as RAM and program memory 196 which can comprise any conventional storage device such as RAM, ROM or a disk drive. Program code in program memory 196 may also be stored on removable disk 198. A processor 200 loads and implements program code stored in program memory 196. All the components of the terminal are linked by a data and communications bus 172.

20 [0100] More specifically, processor 200 loads and implements cash payment management code 200a for managing cash input data from cash input and verification system 192, for adding value to a smart Flash card. Processor 200 also implements a web browser 200b for accessing system owner web pages and data exchange interface 200c for exchanging data between a smart Flash card interface to the terminal and data supply system 120.

[0101] Processor 200 also implements off-line contents retrieval code 200d for retrieving data for storage on a smart Flash card from media input device 180 and/or video input 178 and/or LAN/WAN interface 174. The processor implements a content sampler 200e for outputting small extracts of content data items to a user via audio/visual interface 184. Such data item samples may be stored with the content description data in content access data store 140. The processor also implements a smart Flash card interface driver 200f, user interface code 200g and additional communication drivers 200h for driving LAN/WAN interface 174 and/or comms I/O ports 182.

[0102] Referring now to Figure 9, this shows a schematic diagram of components of a portable data carrier 202, in the embodiment shown a so-called "smart Flash card". In this context, "smart Flash card" refers to an IC card similar in size to a plastic payment card incorporating a processor and Flash data memory, preferably of large capacity. For further details on smart cards, reference may be made to the ISO (International Standards Organization) series of standards, including ISO 7810, ISO 7811, ISO 7812, ISO 7813, ISO 7816, ISO 9992 and ISO 10102, which are hereby incorporated by reference.

[0103] Referring in more detail to Figure 9, a data and communications bus 204 links components of the card which include a processor 210, working memory 212, timing and control logic 208 and an external interface which may have contacts (ISO 7816) or be contactless (ISO 10536) for providing external access to a bus 204 for reading data from and writing data to the card 202. Also coupled to bus 204 are permanent program memory 216, non-volatile data memory 218 and non-volatile (Flash) content data memory 214. Non-volatile data memory 218 may comprise EEPROM and permanent program memory 216 may comprise ROM, for example, mask-programmed ROM. All the components of Figure 9 are mounted on a single substrate, in a preferred embodiment bearing contacts for external interface 206.

[0104] Processor 200 loads and implements program code from permanent program memory 216. This code comprises operating system code for providing the card with a basic operating system for at least external communications; payment management code for supplying payment data from non-volatile data memory 218 to pay for downloaded content; DRM (Digital Rights Management) and security code, including code to implement content data use rules and code for password controlled access to data and program functions; CRM code for implementing CRM-

related rules; and content synthesis code for combining stored content data with additional data provided via external interface 206 for synthesizing complete content item data.

[0105] Non-volatile data memory 218 stores data including card identity data, access control data, including password data for validating a user password, access record data for storing a record of access attempts and their outcomes, and content supply data such as system owner website addresses and retailer/distributor website addresses.

[0106] Data memory 218 further stores card value data comprising e-money such as publicly verifiable digital signatures, and payment data for storing a payment audit trail including payment amounts and data on to whom payments have been made. The memory 218 also stores RFM (Recency Frequency Monetary) data to provide a record of transactions for market research and customer reward purposes, and CRM data storing customer reward points. Data memory 218 also stores an index of content data items stored in Flash memory 214 and associated content use rules, as well as DRM and royalty data for maintaining an audit trail of use history for rights management tracking. Optionally, data memory 218 may also store supply chain data specifying a supply chain route through which data has been obtained from a content provider, which may be used for rewarding supply chain intermediaries, for example on a commission or reward points basis.

[0107] Content data memory 214 preferably comprises at least 100 MB of data storage, partitioned as data blocks of a size selected to match the stored content type. For storing video data, Flash memory 214 preferably comprises > 1 GB data storage and the data blocks into which the data memory is partitioned are larger.

[0108] Referring now to Figure 10, this shows a schematic diagram of a data access device 220, such as a portable audio/video player. The data access device 220 comprises a conventional dedicated computer system including a processor 238, permanent program memory 236, such as ROM, working memory 234, such as RAM, and timing and control logic 226 all coupled by a data and communications bus 222. Also coupled to the bus are an audio interface 228, a display 230 and user controls 232, for providing a user interface. A smart Flash card interface 224 is coupled to bus 222 for interfacing with a smart Flash card for retrieving and playing stored content data.

[0109] Permanent program memory 236 stores program code for implementation by processor 238; this code may also be provided on a data carrier such as a ROM chip or disk 240. Processor 238 implements an SFC interface 238a, a user interface 238b, a content player 238d for retrieving stored content data from a smart Flash card interfaced to the device and for outputting audio and/or video data derived from the retrieved content data (which may comprise compressed audio and/or video data) to a user of the device.

[0110] Processor 238 also implements use control 238c for controlling access to and use of contents stored on the smart Flash card by the content access device user. Use control routine 238c and/or DRM and security code in permanent memory 216 on the smart Flash card may also implement digital watermarking and other Secure Digital Music Initiative (SDMI) content protection code as specified in the SDMI portable device specification, part one, version 1.0 (see [www.sdmi.org](http://www.sdmi.org)) which is hereby incorporated by reference.

[0111] Figures 11a and 11b show a flow diagram of a process for registering a data carrier or smart Flash card with a data supplier or system owner operating a data supply system as illustrated in Figure 6. A smart Flash card may be issued entirely blank, that is, with no prestored content or value, with prestored value but no prestored content, with prestored content but no prestored value (the content being provided free) or with both prestored value and prestored content. Thus, for example, a user may purchase a card with stored value but no stored content over the counter at a retailer. The process of Figures 11a and 11b illustrates the registration of a card with neither prestored content nor prestored value. As illustrated the registration process records user registration data in the access control data store 138 of Figure 6 and writes value data onto the blank card.

[0112] At step S10 a smart Flash card is inserted into a content access terminal smart Flash card interface. The system owner web page is then loaded onto the content access terminal and displayed to the user (step S11). User registration data is then entered into the content access terminal (step S12) and transmitted to the system owner (S13). The user registration data may include a user identity, a preferred e-payment system to use and, optionally, a content access PIN or password, and a service level (for example bronze, silver or gold). The optional password may be a password required by the e-payment system for validation of a payment by the user with the card or it may be a password to protect unauthorized access to content on a smart Flash card to protect stored data in the event, for example, of the card being stolen. A single password

may serve both these functions. The content access terminal web browser is configured so that all sensitive data passing between the terminal and the system owner is securely transmitted, for example by using a conventional encryption system such as PKI (Public Key Infrastructure).

5 [0113] At step S14 a payment request is received from the system owner at the content access terminal and displayed to the user. At step S15 the user enters payment data into the content access terminal and this payment data is transmitted to the system owner, for adding value to the card. This may, for example, be a credit card transaction as is conventionally used for purchase over the internet. Card value data and a card value access code is then received by the content access terminal from the system owner at step S16. The card value corresponds to the payment  
10 made by the user and the value access code may be a password entered by the user at step S12 or may comprise a password or PIN created by payment processor 128 or e-payment system 121 as illustrated in Figure 6. In a preferred embodiment, the user pays the system owner and the system owner then directly provides digital signature data representing value to the content access terminal for writing onto the smart Flash card.

15 [0114] At step S17, card registration data is received from the system owner by the content access terminal and written onto the smart Flash card. This card registration data comprises user identity data, access control data, payment system specifying data, system owner access data, such as a system owner web page address and other dial-up information. At this stage other data may be entered by the user and written onto the card, including, for example, user preference  
20 data, retail outlet and CRM data (alternatively user preference data may be captured at step S12). At step S18 the card value data and card value access code received at step S16 is written onto the card and output to the user visually and, optionally, as a printed record. The card is then available for use, at step S19.

[0115] Figure 11b shows the corresponding registration steps performed by the system owner's  
25 data supply system 120. At step S20, a request for a smart card registration web page is received from a content access device and, at step S21, transmitted to the device. User registration data is then received, at step S22, from the content access terminal and stored in content access control data store 138. The system owner's computer system then transmits, at step S23, a payment request to the content access terminal and receives, at step S24, payment data in reply, this  
30 payment is then authenticated, at step S25, with an e-payment system such as payment system 121 a or b illustrated in Figure 6, and after verification the payment processor 128 of the

computer system transmits, at step S26, value data and a value access code to the content access terminal, for writing onto the smart Flash card. The payment processor then updates the payment record data store 136 with data relating to the transaction (step S27) and, at step S28, retrieves card registration data previously written into the access control data store and transmits this registration data to the content access terminal. At step S29 the transaction is then complete.

[0116] Referring now to Figures 12a-c, these illustrate a flow chart for downloading data to a smart Flash card using a data access terminal. At step S30 the smart Flash card is inserted into the content access terminal and the user then enters, at step S31, their password for gaining access to the functionality of the smart Flash card. At step S32, the content access terminal transmits the password to the smart card for verification and the terminal checks, at step S33, whether access is permitted. If access is not permitted, a warning is displayed by the terminal, at step S34, and an access denied count is implemented. A threshold count is then read from the card together with a count of the total number of times access to the card has been denied (step S35). At step S36 the terminal checks whether the total number of denied accesses is within three of the card threshold, and if it is not, returns to step S31, while if it is, it proceeds to step S37 where the terminal displays a warning that a further denied access is likely to result in erasure of content stored on the card. At step S38 the terminal then checks whether its count of denied accesses is greater than its threshold value, returning to step S31 if not, and displaying an access refused message at step S39 if the total number of permitted accesses has been exceeded. The system then waits at step S39 for removal of the smart Flash card from the content access terminal.

[0117] If access is permitted at step S33, the terminal loads outline CRM data from the card (step S40) and loads retail data, such as targeted advertising, from the retailer LAN/WAN (step S41). At step S42, the terminal then displays a menu of options, retail data such as advertising or CRM-related data and outline CRM data, such as a total number of reward points earned, on the content access terminal. Many options include download content (from a system owner), add monetary value (to the card), check/spend CRM value stored on the card, follow website links, and exit. At step S43, the user inputs a menu option which, in the illustrated flow chart, is the download option. The system thus passes to step S44 and loads the system owner's content access web page onto the content access terminal and displays this to the user.

[0118] At step S45, the user enters a content search request, which is transmitted to the system owner content distributor processor 134. Content search results are received back from the content distribution processor, including a content identifier, a brief description, and content cost data for at least one payment option, and these results are displayed on the user on the content access terminal. The user then selects one or more content items at step S47 and the selection is transmitted to the content distribution processor 134 where further content cost data and purchase option data is retrieved from data store 140. At step S48, this content cost and purchase data (including use rule data) is received from the system owner and displayed to the terminal user. The user then selects, at step S49, a purchase option and confirms a purchase request or, alternatively, selects "exit" to return to the menu display of step S42. After one or more content items have been selected, together with a purchase option, hard value and CRM data is read from the smart Flash card at step S50, and at step S51 a check is made to determine whether the monetary and/or CRM (reward points) value stored on the smart Flash card is sufficient to purchase the selected purchase data items. If the card value is insufficient, a warning is displayed at step S52 and the system returns to the menu display at step S42. If the card value is sufficient, at step S53 the content access terminal transmits a payment request to the smart Flash card.

[0119] Payment for the data item or items requested may either be made directly to the system owner or may be made to an e-payment system such as e-payment systems 121a and 121b of Figure 6, with these systems then forwarding payment confirmation data to the system owner computer system. Alternatively, the content access terminal may transmit data to the card to set up a transaction directly with a content provider who, being the copyright owner, would normally receive the majority of the payment.

[0120] At step S54, payment data for making a payment to the system owner is received from the smart Flash card by the content access terminal and forwarded to an e-payment system such as e-payment system 121 in Figure 6. Payment record data, validating payment by the card to the system owner, is then received back from the e-payment system at step S55 by the content access terminal and forwarded to the card for updating payment data on the card. In alternative embodiments, payment data from the card may be provided directly to the system owner's data supply computer for authentication and, optionally, further validation with an e-payment system by the system owner's computer.



**[0121]** Distribution of the payment received by the system owner from the card is performed by the system owner's computer system, as described elsewhere. Such payment distribution will normally provide a small percentage of the total payment to a "owner" or operator of the content access terminal, such as a retailer, distributor, or in other embodiments, mobile communications network operator or cable TV network operator.

**[0122]** In the presently described embodiment, payment record data received in step S55 is transmitted to the system owner to confirm payment by the card and thus it is the content access terminal, in the described embodiment, which authenticates a payment before confirming that the payment has been made to the system owner.

**[0123]** In step S56, together with the payment record data, purchase request and card registration data is transmitted to the system owner to identify one or more content data items for purchase and to identify the purchaser. Then, at step S57, the content access terminal sets up a transaction between the system owner data supply computer and the smart Flash card for download of the identified content items requested from the data supplier to the smart Flash card.

The download is preferably arranged so that there is no permanent storage of downloaded data on the content access terminal (although temporary storage in a disk cache may be permissible), and there is further preferably no temporary storage on the content access terminal of complete data for a content data item. This provides data security and reassurance to the content providers.

**[0124]** In the same way as with card registration described with regard to Figure 11, a secure and trusted link is set up between the content access terminal and/or the smart Flash card and the data supply computer in a conventional manner as is well known to those skilled in the art (for example, using public key data encryption). The data transaction may be set up directly between the smart Flash card and the data supply computer, in which case the content access terminal has no access to unencrypted content data, or it may be set up between the content access terminal and the data supply computer, in which case unencrypted data is written by the content access terminal to the smart Flash card. Standard transmission protocols are used to ensure complete transmission of a content data item, for example by re-transmitting blocks of data which are not correctly received.

**[0125]** Also at step S57, one or more content access rules are received from the system owner data supply computer and written to the smart Flash card so that each content data item has an

associated use rule to specify under what conditions a user of the smart Flash card is allowed access to the content data item.

5 [0126] At step S58 the content access terminal receives CRM data from the content distribution processor 134 of the system owner, for example specifying a number of reward points earned by downloading the selected content items. This CRM data will normally be written to the smart Flash card (step S59), but may additionally or alternatively be stored in the content access terminal or in a data store of the content access terminal owner so that the reward points are held by the distributor/retailer/cable TV operator. Finally, also at step S59, a complete record of details of the transactions between the smart Flash card and the content access terminal, the smart Flash card and the system owner, the smart Flash card and the e-payment system, and the content access terminal and the e-payment system and/or data supply computer is recorded on the smart Flash card to provide an audit trail. The system then returns to the menu display at step S42.

15 [0127] The add monetary value menu option provided by the menu operates in a similar manner to that described with regard to steps S15 and S16 of Figure 11a and steps S24 to S27 of Figure 11b. In embodiments of the system in which the smart Flash card operates either in a debit (pre-pay) or credit mode, operating mode data may be loaded from the card together with outlying CRM data at step S40. If the card is operating in a credit mode then, at step S41, the content access terminal reads content use data records from the card and proceeds correspondingly to steps S47 and S48 to determine the value of the content accessed and then proceeds according to steps S15 and S16 of Figure 11a and steps S24 to S27 of Figure 11b to retrieve payment for the accessed content from the card owner. Where enhanced access control features are provided, access control data read from the smart Flash card or entered into the content access terminal at step S31 is used, in step S44, to access the system owner content access webpage and, in some embodiments, to set up a secure connection between the content access terminal and system owner data supply computer at step S44.

25 [0128] Referring now to Figures 12d and 12e, these show steps in a process implemented on the system owner's data supply computer for providing content data to a content access terminal and thence to a data carrier such as a smart Flash card. At step S60 the system owner's content access web page is requested by a content access terminal and transmitted to the requesting terminal. A search request for searching for a content data item is received, at step S61, from the

content access terminal, and at step S62 content distribution processor 134 of the content supply system searches content access and DRM data store 140 and transmits the search results to the content access terminal. The search results will normally comprise a content item identifier, a content item description, optionally a content item sample, and at least one content item price, for example for a default payment option. The search results may comprise a set of content data items, either selected by type or artist or comprising some predetermined selection in a similar manner to a compilation of tracks on a CD.

**[0129]** At step S63 content item selection data identifying one or more content items is retrieved from the content access terminal, and at step S64 content item purchase data for the selected content items is retrieved from content access and DRM data store 140. This purchase data will normally include, for each selected content item, one or more prices and purchase options. Purchase option data may simply comprise one of a set of standard options, for example "1" to purchase outright, "2" to rent for a period of time, "3" to rent for a number of plays, and "4" to rent with a final purchase option. The purchase option data may also indicate when a content item is available free.

**[0130]** At step S65 the content purchase data is transmitted to the content access terminal, and at step S66 payment record data, indicating a payment made from the smart Flash card to the system owner, purchase request data, card registration data and, optionally, access control data, is received from the content access terminal. The payment record data confirms a payment for the requested data items, the purchase request data specifies the payment option selected for the selected content items, and the card registration data provides data for keeping records of the transaction and providing reward points; the access control data may be required for additional data security. At step S67 the payment record data, in the described embodiment of the system, is validated with an e-payment system such as e-payment system 121 of Figure 6. As illustrated in the flow chart, the data supply system computer checks with the e-payment system that a payment has in fact been made to the system owner. In other embodiments of the system, payment may be made directly to the system owner, and either concurrently with the content access and download process, or, at some later stage, payment data received from the smart Flash card may be verified with the e-payment system for reimbursement of the system owner.

**[0131]** At step S68, payment distribution data is read from the content access data store 140. This data will indicate how payment made by the card for the data is to be distributed among

recipients. In one embodiment, recipient's payment fractions are specified in general terms in the content access data store, for example copyright owner 0.90, system owner 0.01, retailer/distributor 0.02, publisher 0.02, creator 0.05. Identification of who is the relevant copyright owner is stored in the data store together with the content item identifier, but may be selected from more than one possible content provider for the data item, and identification of who is the relevant retailer/distributor may be determined from, for example, content access identity information received from the content access terminal when the system owner content access web page is accessed at step S60. At step S69, payments are then distributed in accordance with the payment distribution data, either by direct distribution of value-bearing digital signatures to the relevant parties, or by issuing a payment distribution instruction to e-payment system 121. Preferably the data supply system stores records of individual card payments and, at intervals, combines the payment distribution data for a plurality of individual records to output payment data for distributing the total payment received by the data supply system from a batch of individual payments.

**[0132]** At step S70, content access rules for the purchased level of service are read from the content access data store. These rules could, for example, specify that only a predetermined number of accesses to the content are permitted, for example 10 plays. Alternatively, the rules could provide access for, say, one month from the download date. Other rules may provide unlimited plays but only on specified players, for example set top boxes owned by a particular cable TV network (as determined by content access device identification data provided to a smart Flash card from a content access device). A content provider identification for the requested content data is also read from the content access data store at step S70 together with CRM data for issuing reward points.

**[0133]** At step S71, content access rules for the requested content data items are retrieved from data store 140 and transmitted to the content access terminal. Then, at step S72, DRM processor 130 of the data supply system transmits a transaction request and authentication data to the content provider identified in step S70. This request identifies the system owner data supply system to the content provider in a secure manner, either by means of physical security, such as a dedicated connection from the system owner data supply system to the content provider, or by means of an electronically secure connection such as an encryption connection. Then, at step S73, the content access web server 124 receives protected content from the content provider, comprising the data items requested by the content access terminal, and transmits this protected

content to the content access terminal. The content is preferably protected by data encryption but may be protected in other ways, for example, by digital watermarking or simply by the large number of other transactions taking place at any one time over the internet. The data supply system computer, at this point, essentially acts as a transparent data forwarder, forwarding data from the content provider to the content access terminal, which itself is preferably effectively transparent, using data exchange interface 200c to transmit the protected content data directly to the smart Flash card. As described with regard to Figure 12d, the content download protocol includes error protection and transmission retry protocols to ensure substantially error-free data transmission.

10 [0134] Once content has been downloaded to the content access terminal (and, hence, to the smart Flash card) at step S74 a record of the purchase data and content accessed is written to payment record data store 136, to provide an audit trail. Then, at step S75, updated CRM data is written to the content access data store 140, using rules stored in the content access data store, in conjunction with a record of the downloaded data items, to calculate the CRM data (i.e. reward points). The updated CRM data is then also transmitted to the content access terminal, where it can be forwarded to the smart Flash card. Then, at step S76, the process ends.

15 [0135] Referring now to Figure 13, this shows a flow chart for user access of stored data on a smart Flash card using a data access device such as the MP3 player of Figure 1. At step S77 the smart Flash card is inserted into the player and, at step S78, the user enters a password into the player, which is transmitted to the smart Flash card for validation (this step is optional). If access to stored data on the card is permitted, the process proceeds to step S79 where an index of content data items stored on the card is loaded from the card and displayed together with a menu. The menu provides options including access content, check value (stored on the card), check CRM data (such as reward points) stored on the card, and play options (such as no video, repeat play, random play, and the like). If the user wishes to access content data items stored on the smart Flash card, a user selection of such items is entered into the player at step S80, for example using cursor keys or a pointer; additionally or alternatively a default play option may be provided to, for example, play the most recently downloaded data.

25 [0136] At step S81 content use status data for the selected content items is loaded from the smart Flash card together with associated content use rules. Then, at step S82, the use rules and present use status for each selected content item are compared and the result is displayed

together with a content play menu. The content play menu may comprise a simple list of the selected content items with items not available for access highlighted in, for example, red. Alternatively, more detailed content access permission data may be displayed such as the purchased contents use for a content data item, the actual use of the data item made so far, and the available remaining use. Then, at step S83, the player determines whether content use is permitted. If use is not permitted, the process returns to step S79 to re-display the menu; if content use is permitted the system proceeds to step S84.

[0137] At step S84 the selected content data items whose use is permitted are retrieved sequentially from the card, decoded as necessary, and the decoded audio and/or video data is made available to the user, for example, by providing audio output at a headphone socket on the player and displaying video output on the player display. Preferably, the player also retrieves supplementary data stored in association with a content data item, such as advertising data, or for a web-enabled player, hot links to web sites for sale of goods or services, particularly those related to the accessed content data item or those identified to appeal to users accessing the data item (such as pop group merchandizing or Harley Davidson (trade mark) motor bikes for rock music/video).

[0138] Preferably, the player is provided with "pause" and "continue" functions and corresponding user controls. When "pause" is selected the process passes to step S85 and writes a record to the smart Flash card comprising data specifying how much use has been made of the accessed content data item. In the case of music or video data, this may comprise start and end time markers or simply a play duration time (the start time being predetermined, for example at the start of the data item). In the case of a game the partial use data may comprise an elapsed play time or a number of lives left. In the case of a data item providing a service such as access to stock and share prices, or weather information, or a share dealing service, the partial use information may comprise a status record indicating the status of an interrupted transaction. When the "continue" function is selected on the player the process returns to step S84.

[0139] To allow for the smart Flash card being removed from the player between pause and continue events, a check may be made at step S78, by reading a partial use status data from the card, to determine whether a content data item was left in a pause state when the card was last used. If such a pause state is determined to exist for a content data item, the process may then

jump directly to step S85 to allow a user to resume or continue with the content data item and proceed directly to step S84.

5 [0140] Once play is complete the process moves to step S85 where updated content use data is written to the smart Flash card. This updated use data provides a record of the use of a content made in step S84. This record can then be used in steps S81 to S83 to determine, on a subsequent occasion, whether further use of the content data item is permitted. Finally, at step S86, customer reward management reward rules are loaded from the smart Flash card together with CRM data stored on the card. The CRM data is then updated, using the CRM reward rules, to reflect the use of content data items made in step S84 and the updated data is written back to  
10 the smart Flash card.

[0141] In one embodiment the CRM reward rules are determined by the content access terminal owner (retailer/distributor/cable or mobile network operator) and are written onto the card when registering the card. The updated CRM data may then be accessed by a content access terminal for spending or other use when the smart Flash card is next inserted into a  
15 content access terminal. Once the CRM data has been updated, the process returns to step S79 to display the content index and menu.

[0142] The specific embodiments of the invention described above use communication over the internet and web-based technology but this is not essential, and the invention may be implemented using any electronic communications network, such as a wide area network, local  
20 area network, wireless network, or conventional land line network. Likewise, the invention is applicable to the internet, intranets, extranets, and other internet protocol networks.

[0143] The skilled person will understand that many variants to the system are possible and the invention is not limited to the described embodiments but encompasses modifications which lie within the spirit and scope of the present invention.

WHAT IS CLAIMED IS:

1           1.       A handheld multimedia terminal, comprising:  
2           a wireless interface configured to interface with a wireless network for accessing  
3 a remote computer system;  
4           non-volatile memory configured to store multimedia content, wherein said  
5 multimedia content comprises one or more of music data, video data and computer game data;  
6           a program store storing processor control code;  
7           a processor coupled to said non-volatile memory, said program store, said  
8 wireless interface and  
9           a user interface to allow a user to select and play said multimedia content;  
10          a display for displaying one or both of said played multimedia content and data  
11 relating to said played multimedia content;  
12          wherein the processor control code comprises:  
13               code to request identifier data identifying one or more items of multimedia  
14 content stored in the non-volatile memory;  
15               code to receive said identifier data;  
16               code to present to a user on said display said identified one or more items  
17 of multimedia content available from the non-volatile memory;  
18               code to receive a user selection to select at least one of said one or more of  
19 said stored items of multimedia content;  
20               code responsive to said user selection of said at least one selected item of  
21 multimedia content to transmit payment data relating to payment for said at least one  
22 selected item of multimedia content via said wireless interface for validation by a  
23 payment validation system;  
24               code to receive payment validation data via said wireless interface  
25 defining if said payment validation system has validated payment for said at least one  
26 selected item of multimedia content; and  
27               code to control access to said at least one selected item of multimedia  
28 content on said terminal responsive to said payment validation data,  
29          wherein said user interface is operable to enable a user to select said at least one  
30 item of multimedia content available from said non-volatile memory; and



31            wherein said user interface is operable to enable a user to access said at least one  
32 selected item of multimedia content responsive to said code to control access permitting access  
33 to said at least one selected item of multimedia content.

1            2.        A handheld multimedia terminal as claimed in claim 1, wherein the code  
2 to control access to said at least one selected item of multimedia content on said terminal  
3 responsive to said payment validation data comprises code to modify use control data stored in  
4 said non-volatile memory to enable access to said at least one selected item of multimedia  
5 content.

1            3.        A handheld multimedia terminal as claimed in claim 1, further comprising  
2 code to request content cost data via said wireless interface for said identified one or more items  
3 of multimedia content, and further comprising code to receive said requested content cost data  
4 via said wireless interface for said identified one or more items of multimedia content.

1            4.        A handheld multimedia terminal as claimed in claim 1, wherein said code  
2 responsive to said user selection of said at least one selected item of multimedia content to  
3 transmit payment data relating to payment for said at least one selected item of multimedia  
4 content via said wireless interface for validation by a payment validation system comprises  
5 transmitting said payment data to a data access service provider.

1            5.        A handheld multimedia terminal as claimed in claim 1, further comprising  
2 code to retrieve supplementary data via said wireless interface and output said supplementary  
3 data to said user using said display.

1            6.        A handheld multimedia terminal as claimed in claim 1, further  
2 comprising:  
3            code to read use status data and use rules from said non-volatile memory  
4 pertaining to said at least one selected item of multimedia content; and  
5            wherein said code to control access to said selected item of multimedia content  
6 further comprises code to evaluate said use status data and said use rules to determine whether  
7 access is permitted to said at least one selected item of multimedia content.

1           7.       A handheld multimedia terminal as claimed in claim 1, wherein said at  
2 least one selected items of multimedia content comprises additional multimedia content for  
3 another stored item of multimedia content.

1           8.       A data access terminal for controlling access to one or more content data  
2 items stored on a data carrier, the data access terminal comprising:  
3           a user interface;  
4           a data carrier interface;  
5           a program store storing code implementable by a processor; and  
6           a processor coupled to the user interface, to the data carrier interface and to the  
7 program store for implementing the stored code, the code comprising:  
8           code to request identifier data identifying one or more content data items stored  
9 on the data carrier;  
10          code to receive said identifier data;  
11          code to present to a user via said user interface said identified one or more content  
12 data items available from the data carrier;  
13          code to receive a user selection selecting at least one of said one or more of said  
14 stored content data items;  
15          code responsive to said user selection of said selected content data item to  
16 transmit payment data relating to payment for said selected content item for validation by a  
17 payment validation system;  
18          code to receive payment validation data defining if said payment validation  
19 system has validated payment for said content data item; and  
20          code to control access to said selected content data item responsive to the  
21 payment validation data.

1           9.       A data access terminal as claimed in claim 8, wherein said data carrier is  
2 integrated into the data access terminal, and wherein said data carrier comprises flash memory.

1           10.      A data access terminal as claimed in claim 8, wherein said data access  
2 terminal is integrated with a mobile communications device and audio/video player.

1           11.    A data access terminal as claimed in claim 8, wherein said data access  
2 terminal is integrated with a set top box.

1           12.    A data access terminal as claimed in claim 8, wherein the content data  
2 item comprises additional content data for another stored content data item.

1           13.    A data access terminal as claimed in claim 12, wherein the additional  
2 content data comprises a level on a game.

1           14.    A handheld multimedia terminal, comprising:  
2           a wireless interface configured to interface with a wireless network for  
3 communicating with a data supplier;  
4           non-volatile memory configured to store multimedia content, wherein said  
5 multimedia content comprises one or more of music data, video data and computer game data;  
6           a program store storing processor control code;  
7           a processor coupled to said non-volatile memory, said program store, said  
8 wireless interface and a user interface to allow a user to select and play said multimedia content;  
9           a display for displaying one or both of said played multimedia content and data  
10 relating to said played multimedia content;

11           wherein the processor control code comprises:  
12           code to request identifier data identifying one or more items of multimedia  
13 content available for retrieving via said wireless interface;

14           code to receive said identifier data via said wireless interface, said  
15 identifier data identifying said one or more items of multimedia content available for  
16 retrieving via said wireless interface;

17           code to request content information via said wireless interface, wherein  
18 said content information comprises one or more of description data and cost data  
19 pertaining to at least one of said one or more items of multimedia content identified by  
20 said identifier data;

21           code to receive said content information via said wireless interface;

22           code to present said content information pertaining to said identified one  
23 or more items of multimedia content available for retrieving to a user on said display;

24 code to receive a user selection selecting at least one of said one or more  
25 items of multimedia content available for retrieving;  
26 code responsive to said user selection of said selected at least one item of  
27 multimedia content to transmit payment data relating to payment for said selected at least  
28 one item of multimedia content via said wireless interface for validation by a payment  
29 validation system;  
30 code to receive payment validation data via said wireless interface  
31 defining if said payment validation system has validated payment for said selected at  
32 least one item of multimedia content; and  
33 code responsive to said payment validation data to retrieve said selected at  
34 least one item of multimedia content via said wireless interface from a data supplier and  
35 to write said retrieved at least one item of multimedia content into said non-volatile  
36 memory,  
37 wherein said user interface is operable to enable a user to select said selected at  
38 least one item of multimedia content available for retrieving.

1 15. A handheld multimedia terminal as claimed in claim 14, wherein said code  
2 to request content information comprises code to request said content information from a content  
3 access web server.

1 16. A handheld multimedia terminal as claimed in claim 14, wherein said code  
2 to receive said content data item comprises code to retrieve said content data item from a content  
3 provider.

1 17. A handheld multimedia terminal as claimed in claim 14, wherein said  
2 identifier data is retrieved from a data supplier.

1 18. A handheld multimedia terminal as claimed in claim 14, further  
2 comprising code to transmit at least a portion of said payment validation data to a data supplier  
3 or to a destination received from said data supplier.

1 19. A data access terminal for retrieving a content data item from a data  
2 supplier and providing the retrieved data item to a data carrier, the data access terminal  
3 comprising:

4 a first interface for communicating with the data supplier;  
5 a user interface;  
6 a data carrier interface;  
7 a program store storing code implementable by a processor; and  
8 a processor coupled to the user interface, to the data carrier interface and to the  
9 program store for implementing the stored code, the code comprising:  
10 code to request identifier data identifying one or more content data items  
11 available for retrieving;  
12 code to receive said identifier data identifying said one or more content  
13 data items available for retrieving;  
14 code to request content information pertaining to at least one of said one  
15 or more content data items identified by said identified data;  
16 code to receive said content information;  
17 code to present said content information to a user via said user interface  
18 pertaining to said identified one or more content data items available for retrieving;  
19 code to receive a user selection selecting at least one of said one or more  
20 of said content data items available for retrieving;  
21 code responsive to said user selection of said selected at least one content  
22 data item to transmit payment data relating to payment for said selected at least one  
23 content item for validation by a payment validation system;  
24 code to receive payment validation data defining if said payment  
25 validation system has validated payment for said selected at least one content data item;  
26 and  
27 code responsive to the payment validation data to retrieve said selected at  
28 least one content data item from a data supplier and to write said retrieved at least one  
29 content data item into said data carrier.

1 20. A data access terminal as claimed in claim 19, wherein said content  
2 information comprises at least one of a content data item description and content cost data.

1 21. A data access terminal as claimed in claim 19, wherein said data carrier is  
2 integrated into said data access terminal, and wherein said data carrier comprises flash memory.

1           22.    A data access terminal as claimed in claim 19, wherein said data access  
2 terminal is integrated with a mobile communications device and audio/video player.

1           23.    A data access terminal as claimed in claim 19, wherein said data access  
2 terminal is integrated with a set top box.

1           24.    A data access terminal as claimed in claim 19, wherein the content data  
2 item comprises one or more of music, films, TV programs, text, software, or games software.

1           25.    A handheld multimedia terminal for retrieving and accessing protected  
2 multimedia content, comprising:

3                   a wireless interface configured to interface with a wireless network for  
4 communicating with a data supplier;

5                   non-volatile memory configured to store multimedia content, wherein said  
6 multimedia content comprises one or more of music data, video data and computer game data;

7                   a program store storing processor control code;

8                   a processor coupled to said non-volatile memory, said program store, said  
9 wireless interface and

10                  a user interface to allow a user to select and play said multimedia content;

11                  a display for displaying one or both of said played multimedia content and data  
12 relating to said played multimedia content;

13                  wherein the processor control code comprises:

14                   code to request identifier data identifying one or more items of multimedia  
15 content available for retrieving via said wireless interface;

16                   code to receive said identifier data via said wireless interface, said  
17 identifier data identifying said one or more items of multimedia content available for  
18 retrieving via said wireless interface;

19                   code to request content information via said wireless interface, wherein  
20 said content information comprises one or more of description data and cost data  
21 pertaining to at least one of said one or more items of multimedia content identified by  
22 said identifier data;

23                   code to receive said content information via said wireless interface;

24 code to present said content information pertaining to said identified one  
25 or more items of multimedia content available for retrieving to a user on said display;  
26 code to receive a first user selection selecting at least one of said one or  
27 more items of multimedia content available for retrieving;  
28 code responsive to said first user selection of said selected at least one  
29 item of multimedia content to transmit payment data relating to payment for said selected  
30 at least one item of multimedia content via said wireless interface for validation by a  
31 payment validation system;  
32 code to receive payment validation data via said wireless interface  
33 defining if said payment validation system has validated payment for said selected at  
34 least one item of multimedia content; and  
35 code responsive to said payment validation data to retrieve said selected at  
36 least one item of multimedia content via said wireless interface from a data supplier and  
37 to write said retrieved at least one item of multimedia content into said non-volatile  
38 memory,  
39 code to receive a second user selection selecting one or more of said items  
40 of retrieved multimedia content to access;  
41 code to read use status data and use rules from said non-volatile memory  
42 pertaining to said second selected one or more items of retrieved multimedia content; and  
43 code to evaluate said use status data and use rules to determine whether  
44 access is permitted to said second selected one or more items of retrieved multimedia  
45 content,  
46 wherein said user interface is operable to enable a user to make said first user  
47 selection of said selected at least one item of multimedia content available for retrieving,  
48 wherein said user interface is operable to enable a user to make said second user  
49 selection of said one or more items of retrieved multimedia content available for accessing, and  
50 wherein said user interface is operable to enable a user to access said second user  
51 selection of said one or more item of retrieved multimedia content responsive to said code to  
52 control access permitting access to said second selected one or more items of retrieved  
53 multimedia content.

1           26.     A handheld multimedia terminal as claimed in claim 25, further  
2 comprising code to present said second selected one or more items of retrieved multimedia  
3 content to a user via said display if access is permitted.

1           27.     A handheld multimedia terminal as claimed in claim 25, wherein the rules  
2 comprise one or more of purchase rules, rental rules and subscription rules for said second  
3 selected one or more items of retrieved multimedia content.

1           28.     A handheld multimedia terminal as claimed in claim 25, further  
2 comprising code to write updated use status data to said non volatile memory after user access to  
3 the second selected one or more items of retrieved multimedia content.

1           29.     A handheld multimedia as claimed in claim 28, further comprising code to  
2 write partial use status data to said non volatile memory when only part of one of said second  
3 selected one or more items of retrieved multimedia content has been accessed.

1           30.     A data access terminal for controlling access to one or more content data  
2 items stored on a data carrier, the data access terminal comprising:

3                   a user interface;

4                   a data carrier interface;

5                   a program store storing code implementable by a processor; and

6                   a processor coupled to the user interface, to the data carrier interface and to the  
7 program store for implementing the stored code, the code comprising:

8                                 code to request identifier data identifying one or more content data  
9 items available for retrieving;

10                                code to receive said identifier data identifying said one or more  
11 content data items available for retrieving;

12                                code to request content information pertaining to at least one of  
13 said one or more content data items identified by said identified data;

14                                code to receive said content information;

15                                code to present said content information to a user via said user  
16 interface pertaining to said identified one or more content data items available for  
17 retrieving;



18 code to receive a first user selection selecting at least one of said  
19 one or more of said content data items available for retrieving;  
20 code responsive to said first user selection of said selected at least  
21 one content data item to transmit payment data relating to payment for said  
22 selected at least one content item for validation by a payment validation system;  
23 code to receive payment validation data defining if said payment  
24 validation system has validated payment for said selected at least one content data  
25 item;  
26 code responsive to the payment validation data to retrieve said  
27 selected at least one content data item from a data supplier and to write said  
28 retrieved at least one content data item into said data carrier;  
29 code to receive a second user selection selecting one of said one or  
30 more of said retrieved content data items to access;  
31 code to read use status data and use rules from said data carrier  
32 pertaining to said second selected one or more retrieved content data items; and  
33 code to evaluate said use status data and use rules to determine  
34 whether access is permitted to said second selected one or more retrieved content  
35 data items.

1 31. A data access terminal as claimed in claim 30, wherein said data carrier is  
2 integrated into said data access terminal, and wherein said data carrier comprises flash memory.

1 32. A data access terminal as claimed in claim 30, wherein said data access  
2 terminal is integrated with a mobile communications device and audio/video player.

1 33. A data access terminal as claimed in claim 30, wherein said data access  
2 terminal is integrated with a set top box.

1 34. A data access terminal as claimed in claim 30, wherein the content data  
2 item comprises one or more of music, films, TV programs, text, software, or games software.

1 35. A data access terminal for retrieving data from a data supplier and  
2 providing the retrieved data to a data carrier, the terminal comprising:  
3 a first interface for communicating with the data supplier;

4 a data carrier interface for interfacing with the data carrier;  
5 a program store storing code; and  
6 a processor coupled to the first interface, the data carrier interface, and the  
7 program store for implementing the stored code,  
8 the code comprising:  
9 code to read payment data from the data carrier and to forward the  
10 payment data to a payment validation system;  
11 code to receive payment validation data from the payment validation  
12 system;  
13 code responsive to the payment validation data to retrieve data from the  
14 data supplier and to write the retrieved data into the data carrier;  
15 code responsive to the payment validation data to receive at least one  
16 access rule from the data supplier and to write the at least one access rule into the data  
17 carrier, the at least one access rule specifying at least one condition for accessing the  
18 retrieved data written into the data carrier, the at least one condition being dependent  
19 upon the amount of payment associated with the payment data forwarded to the payment  
20 validation system;  
21 code to retrieve from the data supplier and output to a user stored data  
22 identifier data and associated value data and use rule data for a data item available from  
23 the data supplier; and  
24 code to write use rule data for a data item into the data carrier with the  
25 associated data item,  
26 wherein the data access terminal is integrated with a mobile  
27 communication device, a personal computer, an audio/video player, and/or a set top box.

1 36. A data access device for retrieving stored data from a data carrier, the  
2 device comprising:  
3 a user interface;  
4 a data carrier interface;  
5 a program store storing code implementable by a processor; and  
6 a processor coupled to the user interface, to the data carrier interface and to the  
7 program store for implementing the stored code,  
8 the code comprising:

9 code to retrieve use status data indicating a use status of data stored on the  
10 carrier, and use rules data indicating permissible use of data stored on the carrier;  
11 code to evaluate the use status data using the use rules data to determine  
12 whether access is permitted to the stored data;  
13 code to access the stored data when access is permitted; and  
14 code to write partial use status data to the data carrier when only part of a  
15 stored data item has been accessed,  
16 wherein the data access terminal is integrated with a mobile communication  
17 device, a personal computer, an audio/video player, and/or a set top box.

1 37. A portable data carrier, comprising:  
2 an interface for reading and writing data from and to the carrier;  
3 non-volatile data memory, coupled to the interface, for storing data on the carrier;  
4 non-volatile payment data memory, coupled to the interface, for providing  
5 payment  
6 data to an external device; and  
7 non-volatile communications parameter memory for storing data for accessing a  
8 communications network to receive data from the communications network for storage in the  
9 data memory.

1 38. A portable data carrier, comprising:  
2 an interface for reading and writing data from and to the carrier;  
3 non-volatile data memory, coupled to the interface, for storing data on the carrier;  
4 and  
5 non-volatile payment data memory, coupled to the interface, for providing  
6 payment data to an external device,  
7 wherein the data memory is partitioned for access on a block-by-block basis, each  
8 block comprising a plurality of data bytes read or written as a set.

1 39. A portable data carrier, comprising:  
2 an interface for reading and writing data from and to the carrier;  
3 non-volatile data memory, coupled to the interface, for storing data on the carrier;  
4 and

5 non-volatile payment data memory, coupled to the interface, for providing  
6 payment data to an external device,  
7 wherein said data memory has a capacity of greater than 1 MByte, more  
8 preferably greater than 100 Mbytes, and most preferably greater than 1GByte.

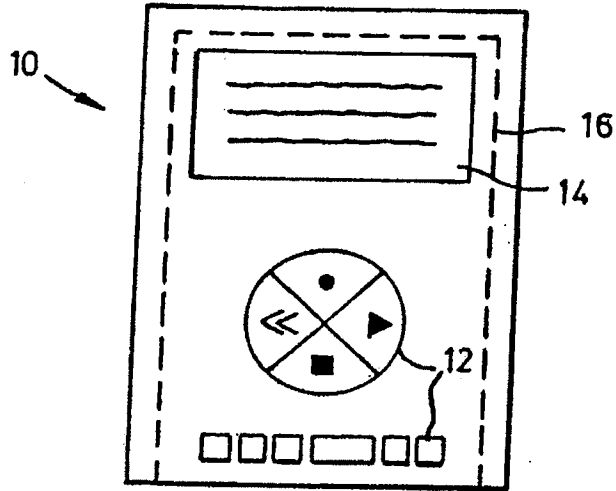
ABSTRACT OF THE DISCLOSURE

Data storage and access systems enable downloading and paying for data such as audio and video data, text, software, games and other types of data. A portable data carrier has an interface for sending and receiving data, data memory for storing received content data, and payment validation memory for providing payment validation data to an external device. The carrier may also store a record of access made to the stored content, and content use rules for controlling access to the stored content. Embodiments store further access control data and supplementary data such as hot links to web sites and/or advertising data. A complementary data access terminal, data supply computer system, and data access device are also described. The combination of payment data and stored content data and use rule data helps reduce the risk of unauthorized access to data such as compressed music and video data, especially over the Internet.

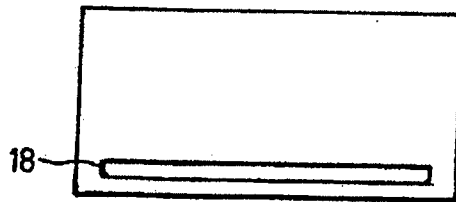
63664751 v1

Fig. 1

A



B



C

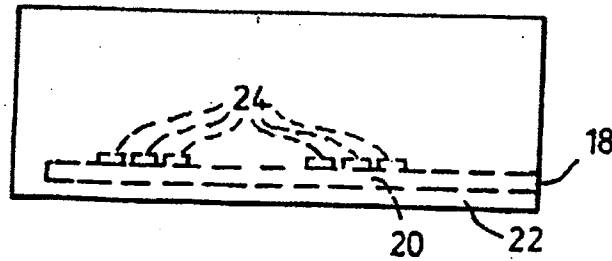


Fig. 2

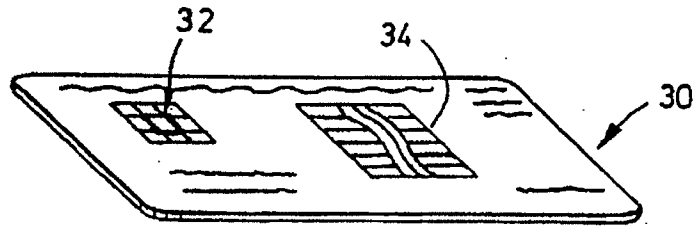


Fig. 3

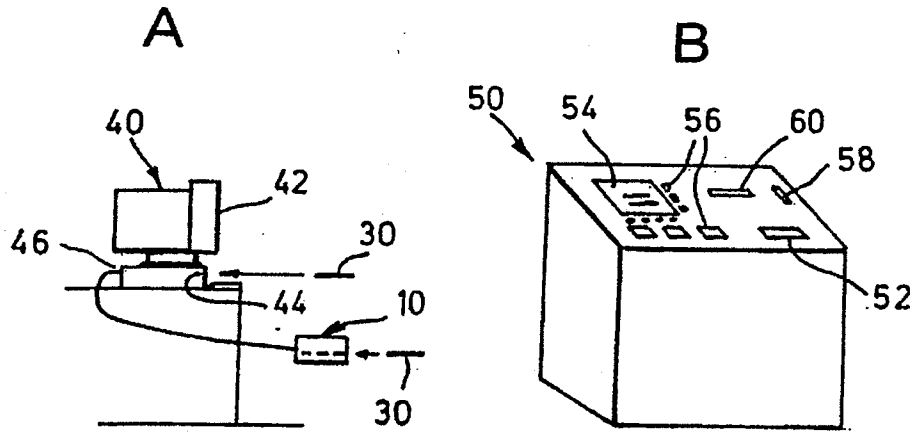
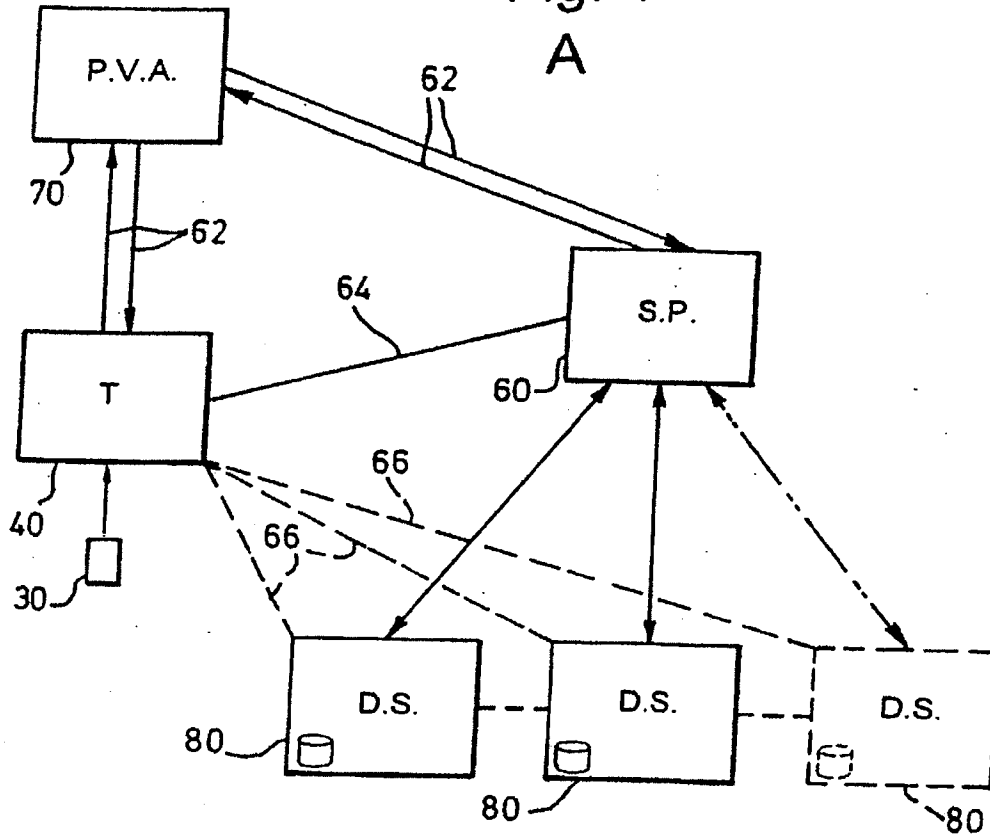
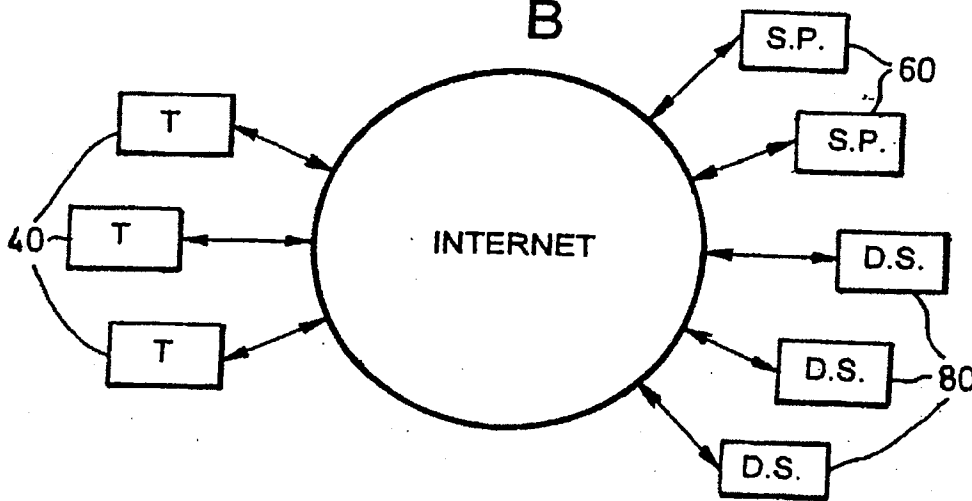


Fig. 4  
A



B





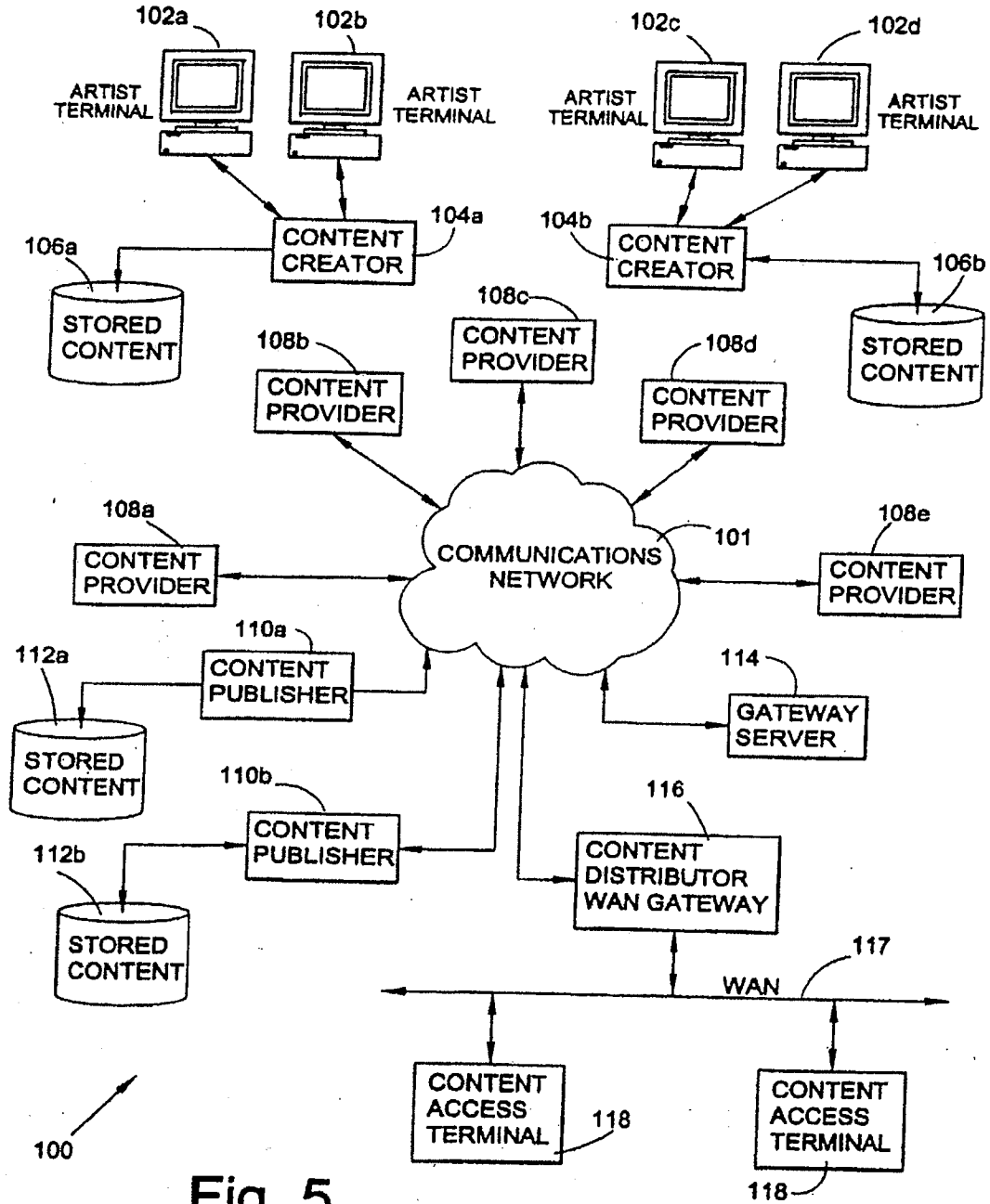


Fig. 5

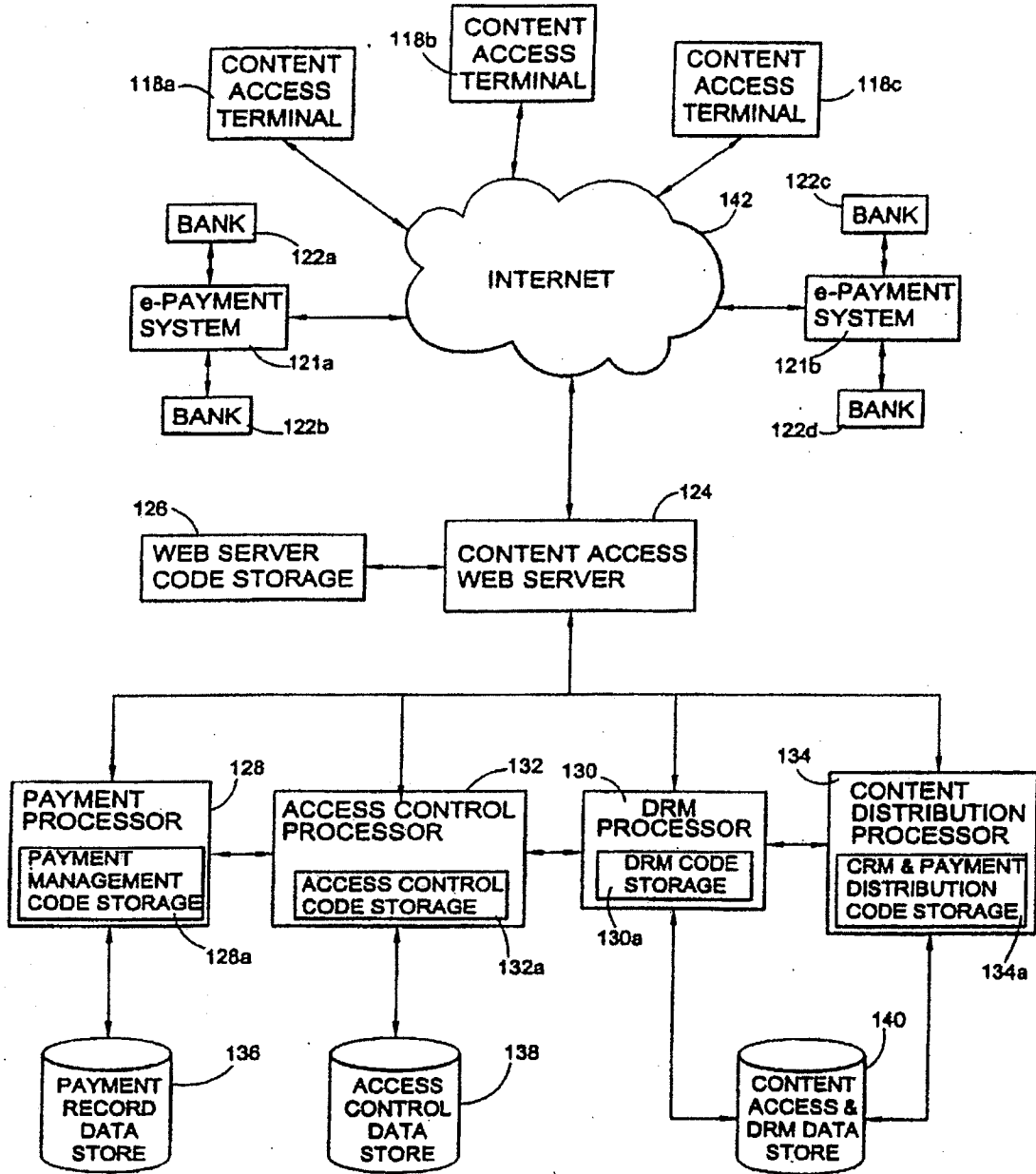


Fig.6

120

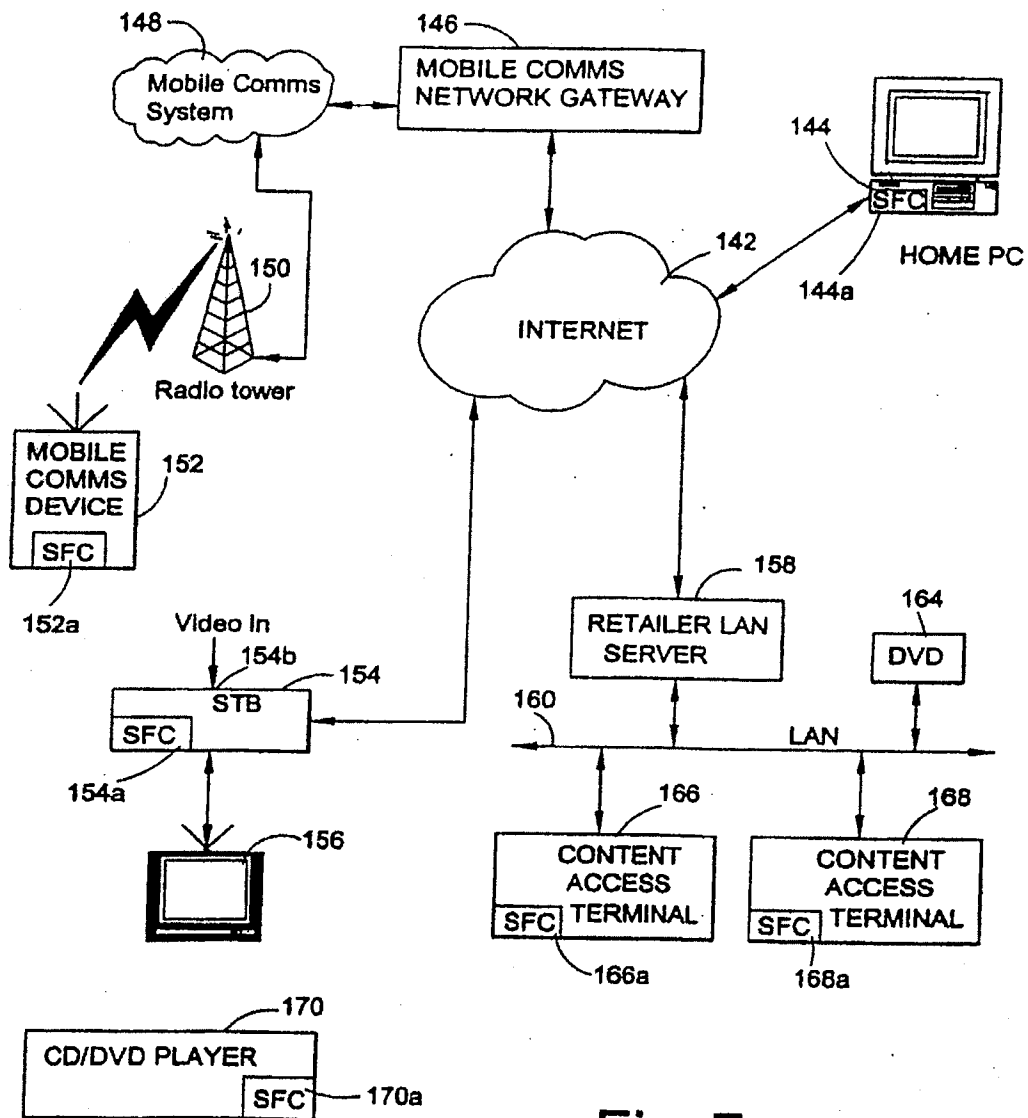


Fig. 7

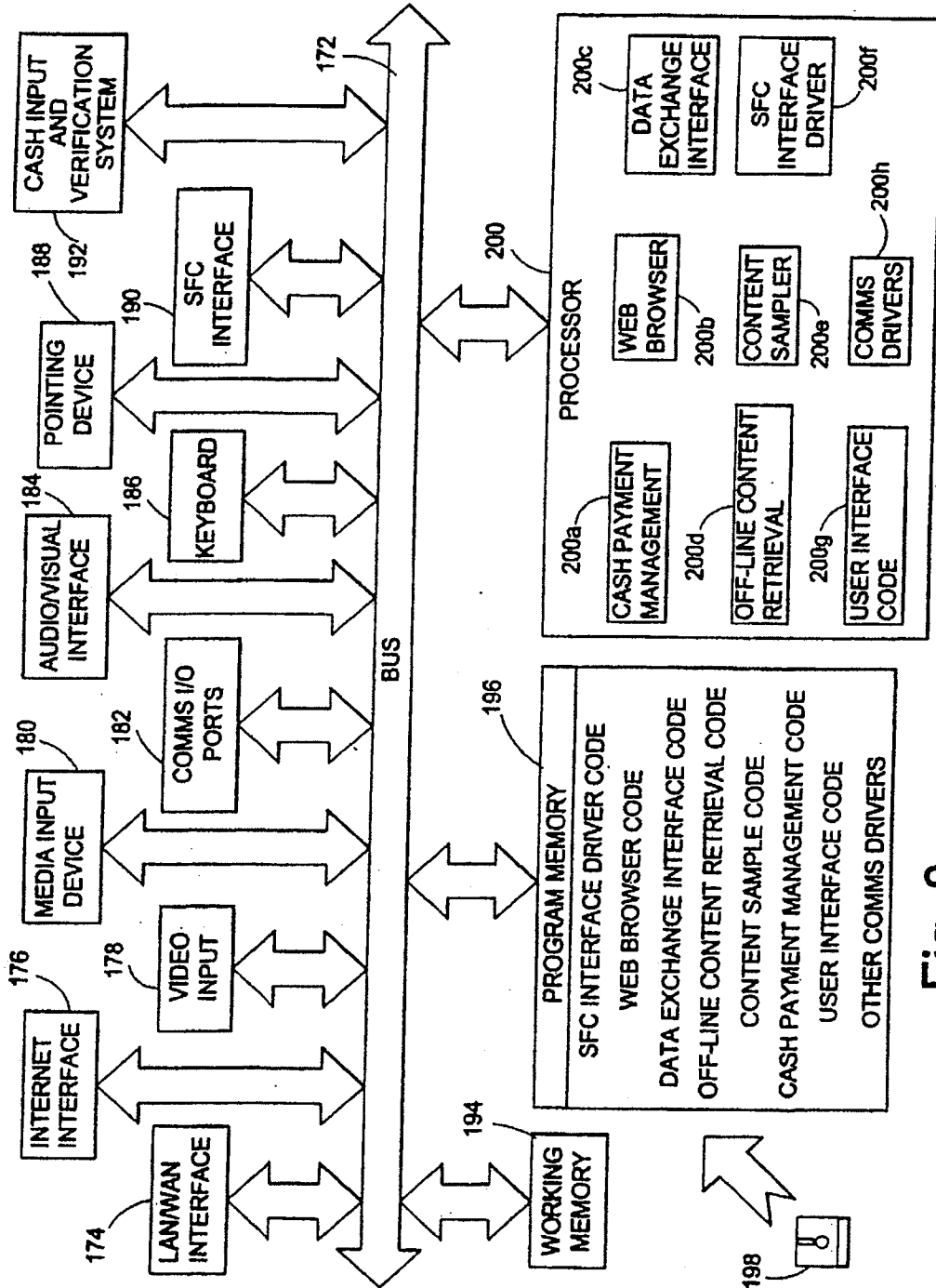


Fig. 8

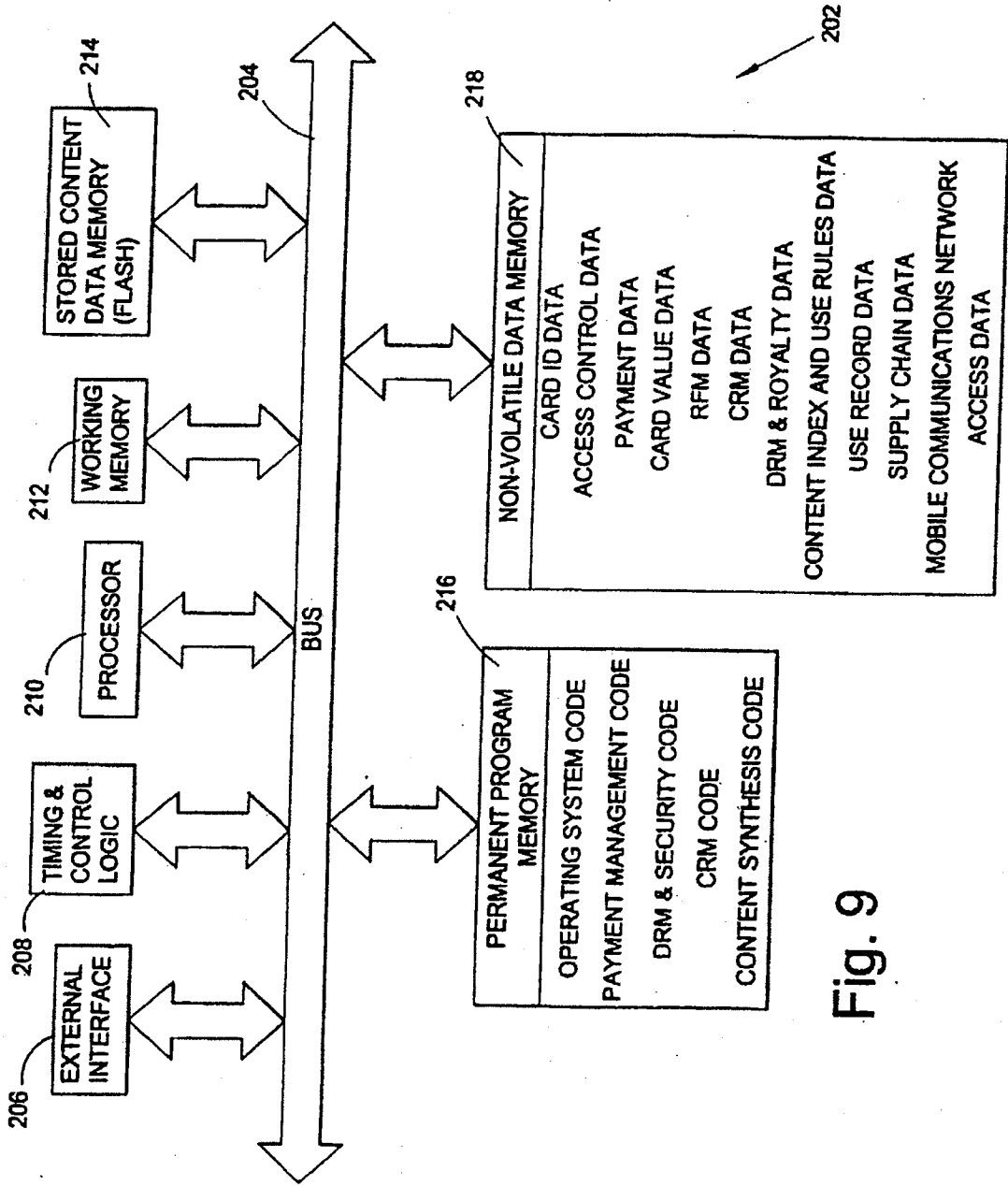


Fig. 9

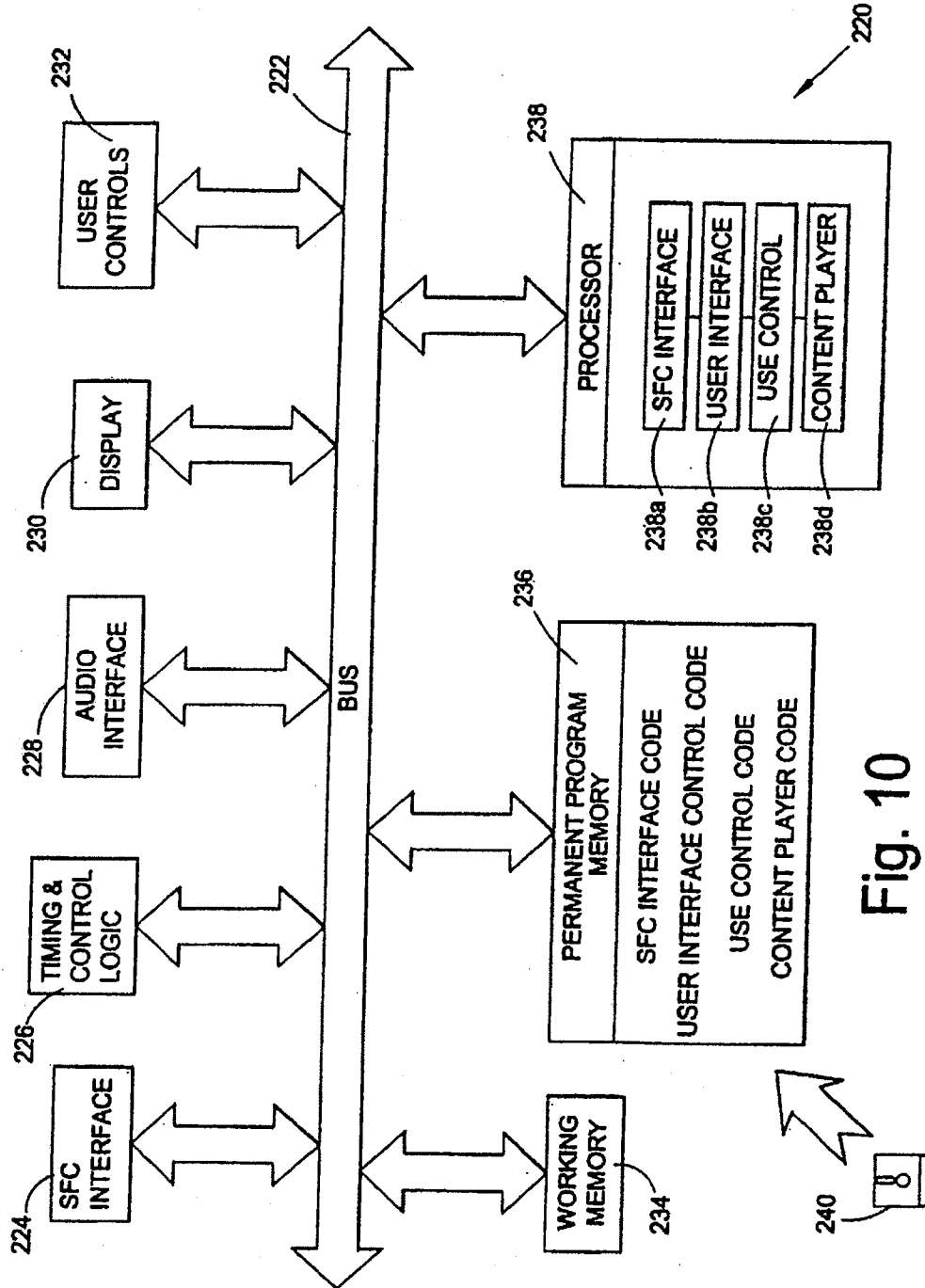


Fig. 10

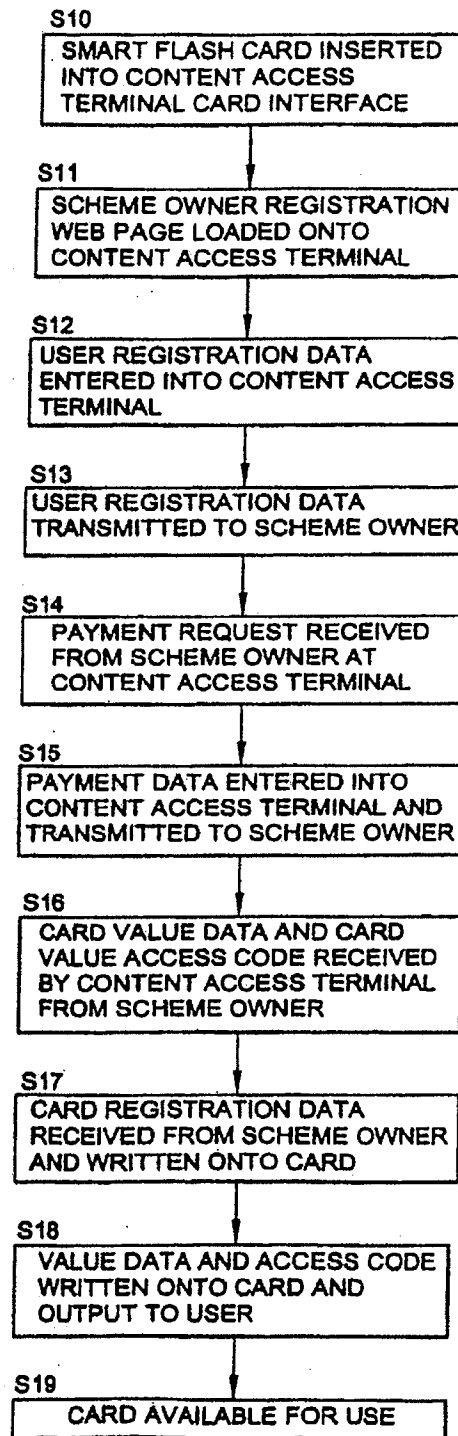


Fig 11a

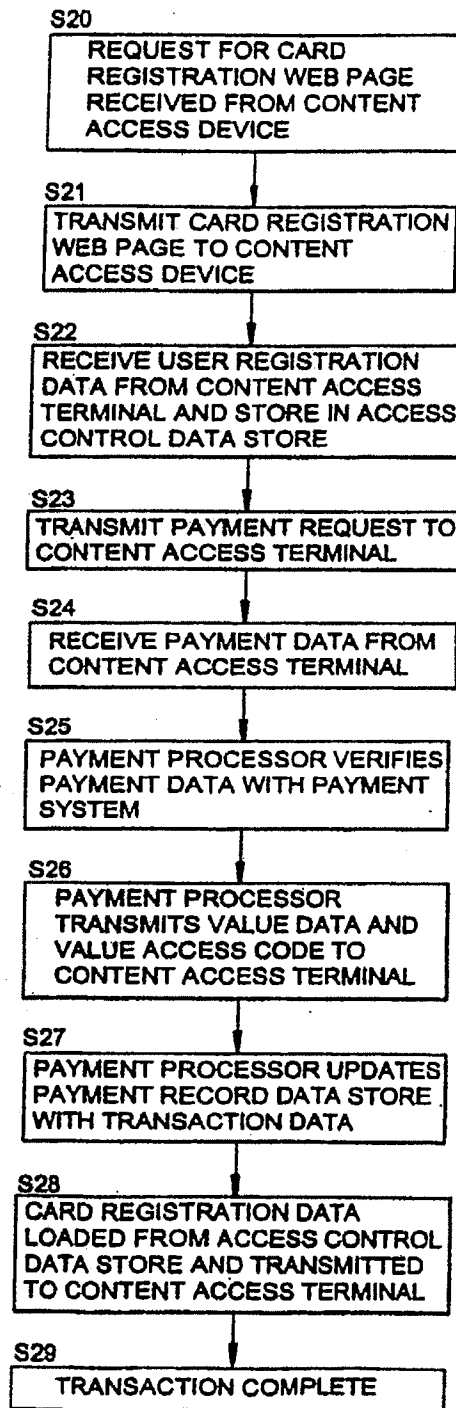


Fig.11b



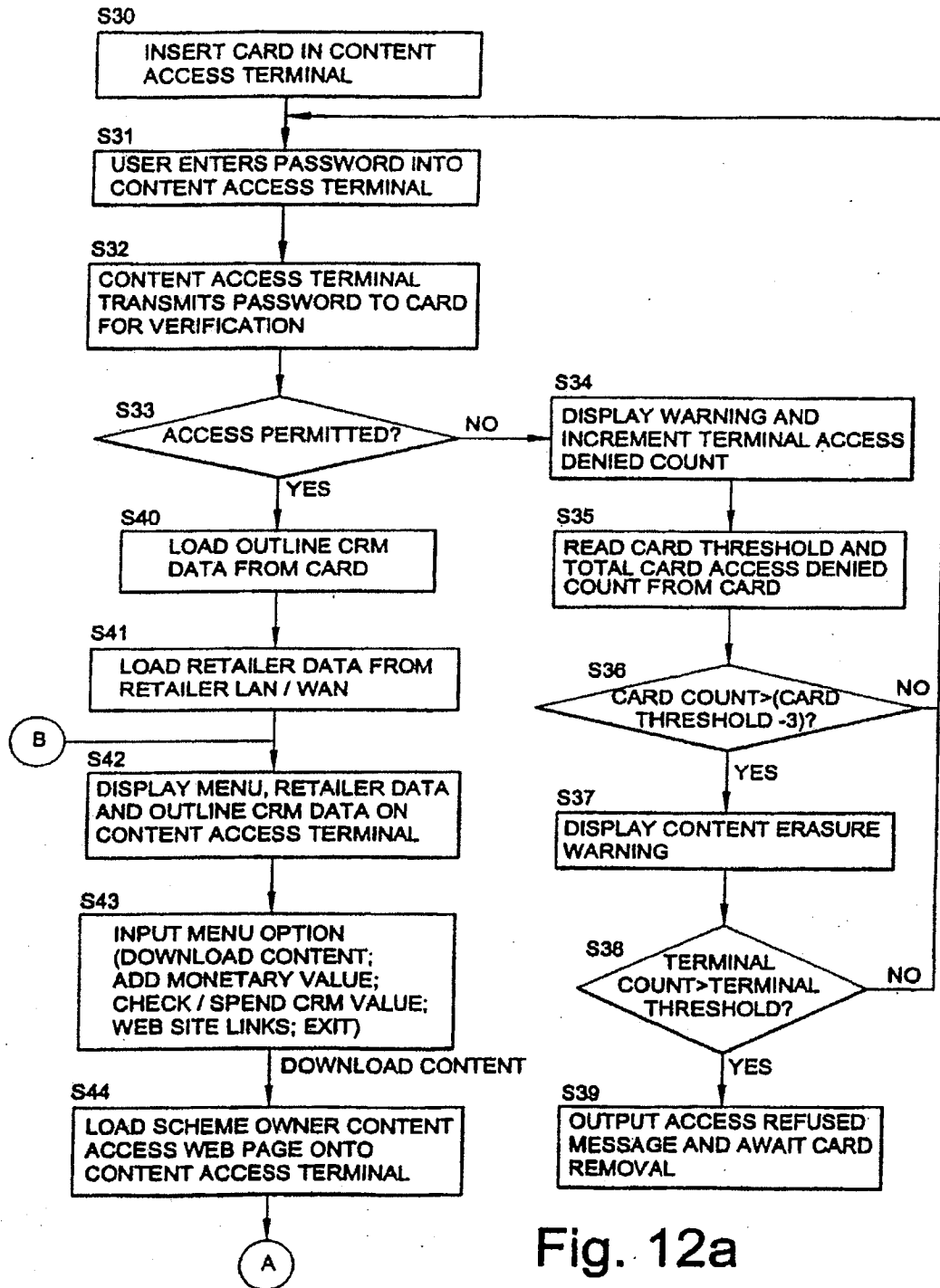
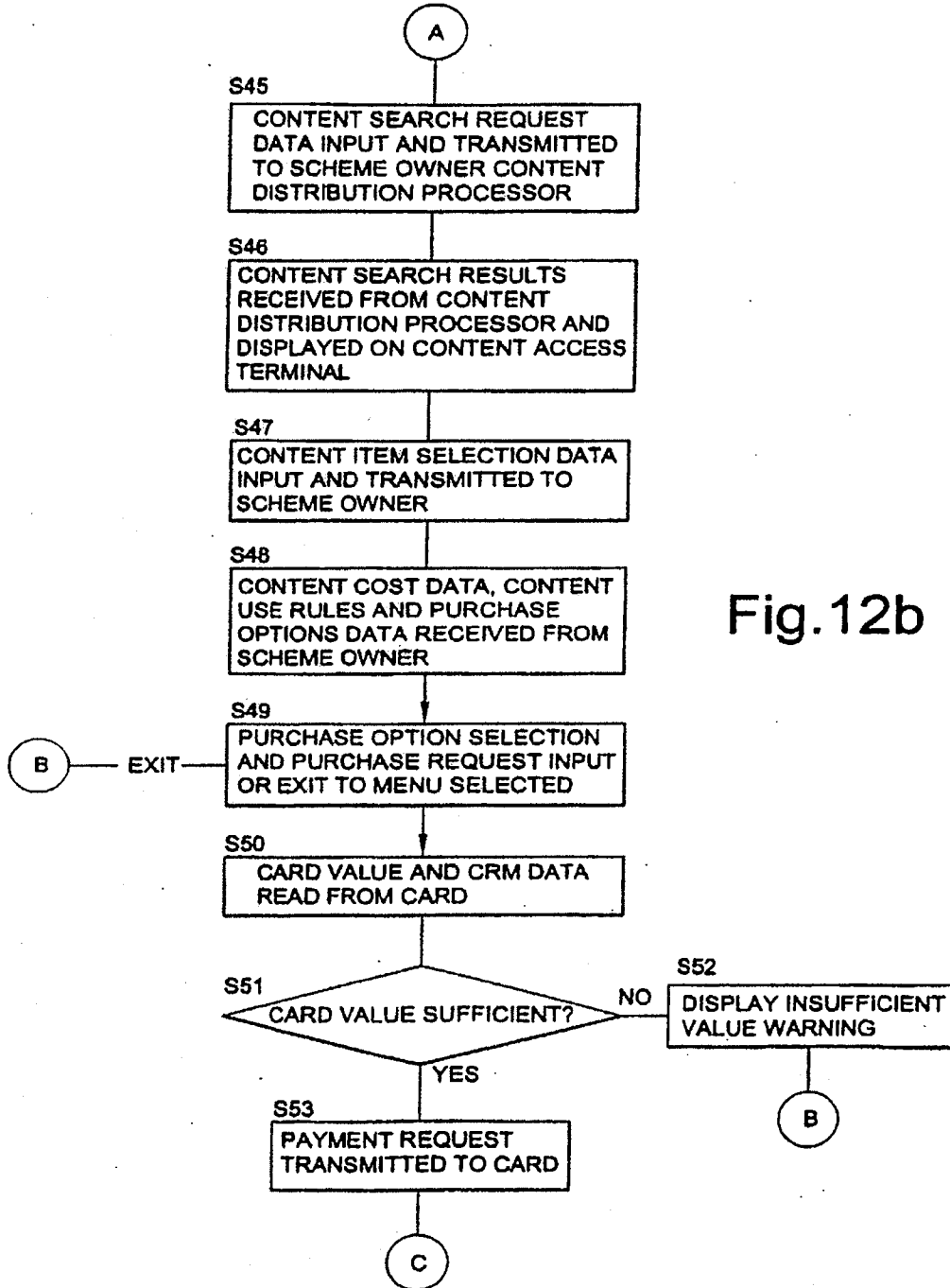


Fig. 12a



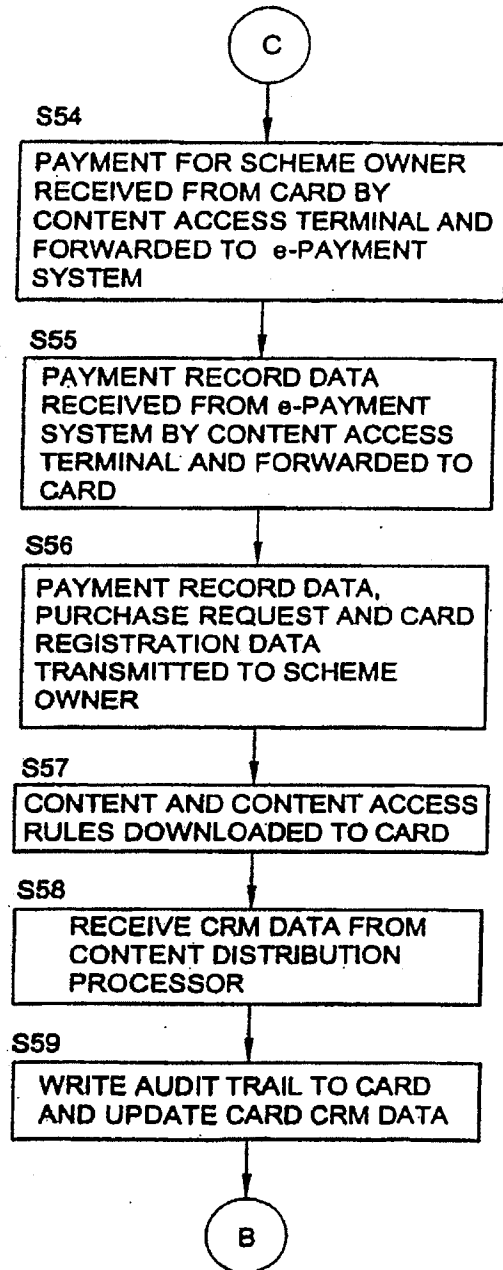


Fig.12c

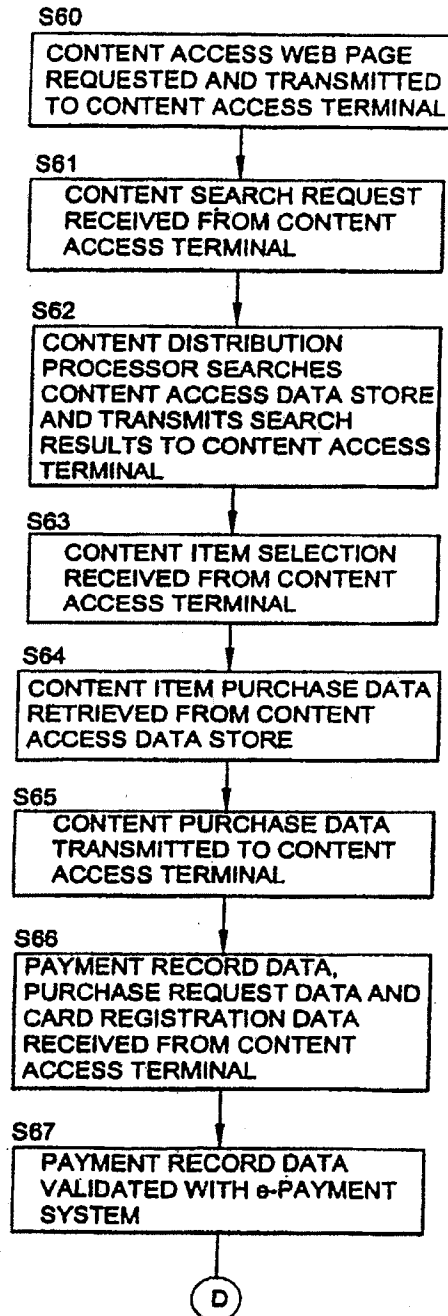


Fig. 12d

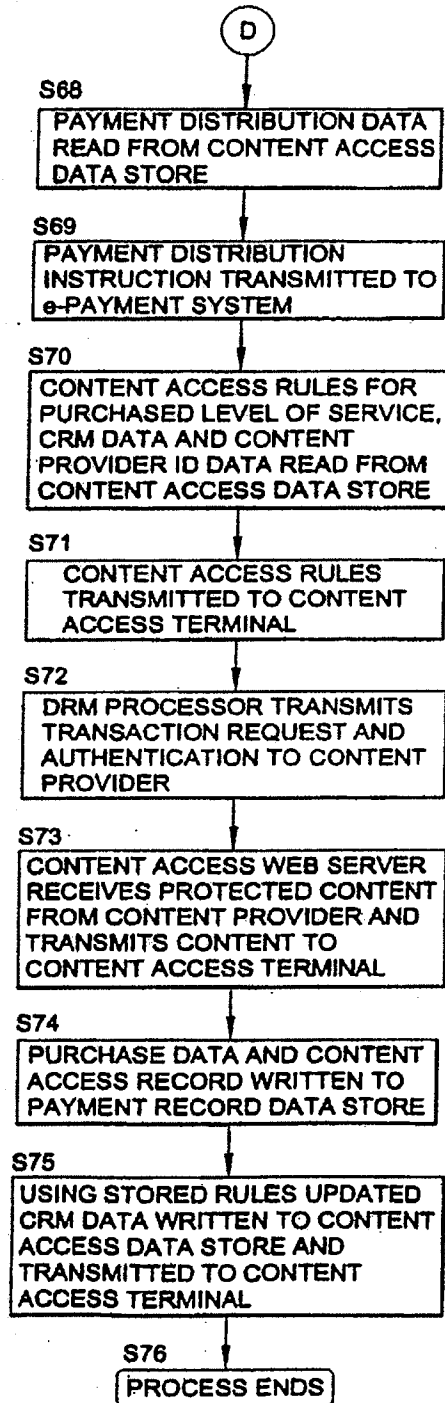


Fig. 12e

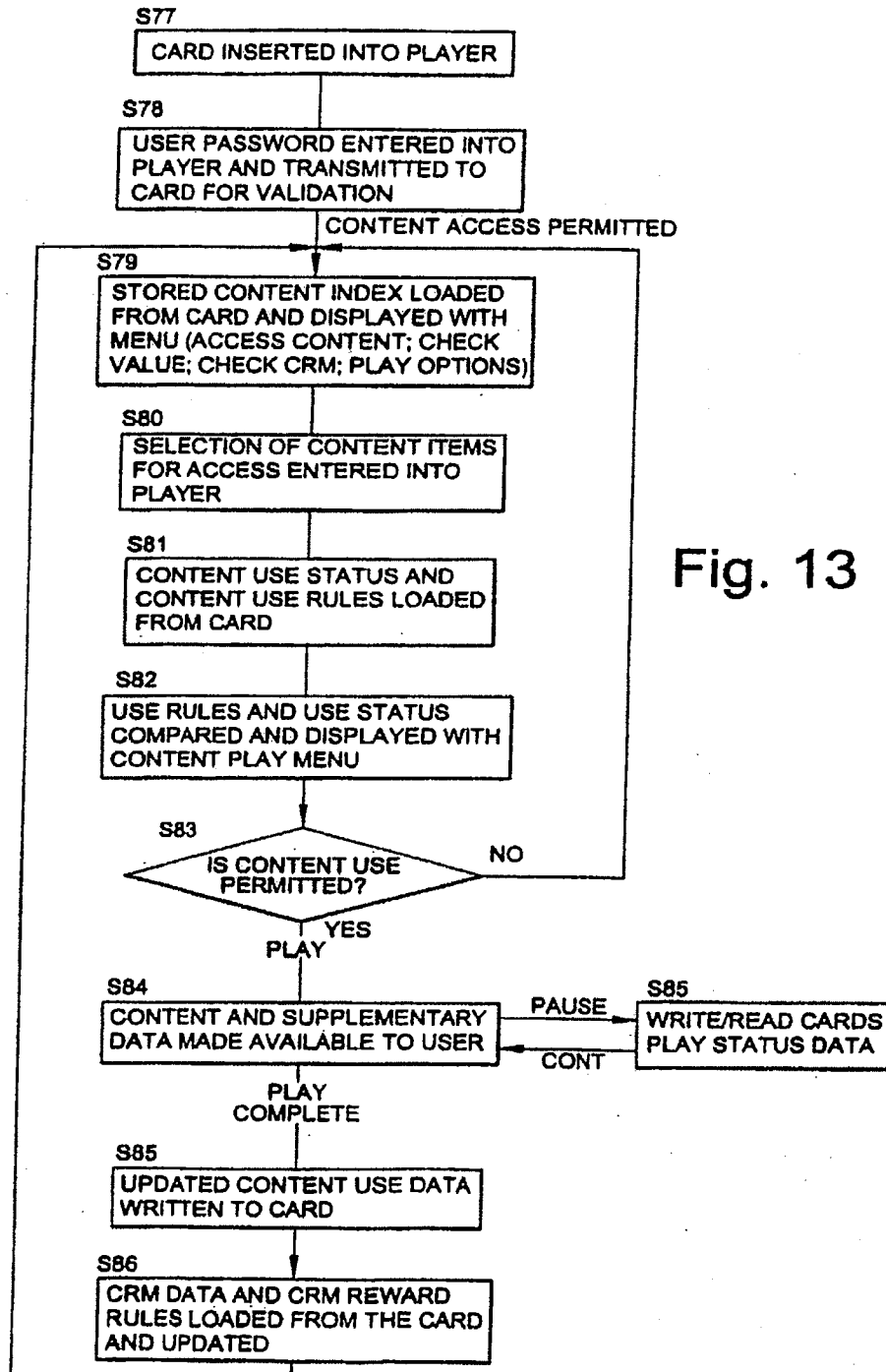


Fig. 13

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on April 3, 2012

PATENT  
Attorney Docket No. 87790-837121 (000160US)  
Client Reference No. PN759544USG

KILPATRICK TOWNSEND & STOCKTON LLP

By:   
William Chinn

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

PATRICK RACZ, ET AL.

Application No. (not yet assigned)

Filed: (herewith)

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No. 20350

Confirmation No.

Examiner:

Art Unit:

INFORMATION DISCLOSURE  
STATEMENT UNDER 37 CFR §1.97 and  
§1.98

San Francisco, CA 94111  
April 3, 2012

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

The references cited on attached form PTO/SB/08A&08B are being called to the attention of the Examiner. In accordance with 37 CFR §1.98(d), copies of the references can be found in related Application No. 13/212,047, filed August 17, 2011 (Attorney Docket No. 87790-818158 (000150US)); Application No. 12/943,872, filed November 10, 2010 (Attorney Docket No. 87790-794402 (000120US)); Application No. 12/014,558, filed January 15, 2008 (Attorney Docket No. 87790-743055 (000110US)); and Application No. 11/336,758, filed January 19, 2006 (Attorney Docket No. 87790-707431 (000100US)). It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and

the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR §1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement.

Respectfully submitted,



Babak Kusha  
Reg. No. 51,095

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 415-576-0200  
Fax: 415-576-0300  
BK:wlc  
64087940 v1



**PATENT APPLICATION FEE DETERMINATION RECORD**

Substitute for Form PTO-875

Application or Docket Number  
13/438,754

**APPLICATION AS FILED - PART I**

(Column 1) (Column 2)

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A
TOTAL CLAIMS (37 CFR 1.16(j))	1 minus 20 = *	*
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 = *	*
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		

\* If the difference in column 1 is less than zero, enter "0" in column 2.

**SMALL ENTITY**

RATE(\$)	FEE(\$)
N/A	95
N/A	310
N/A	125
x 30 =	0.00
x 125 =	0.00
	0.00
	0.00
<b>TOTAL</b>	<b>530</b>

**OR OTHER THAN SMALL ENTITY**

RATE(\$)	FEE(\$)
N/A	
N/A	
N/A	
<b>TOTAL</b>	

**APPLICATION AS AMENDED - PART II**

(Column 1) (Column 2) (Column 3)

AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(j))	*	Minus	**	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=
	Application Size Fee (37 CFR 1.16(s))				
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					

**SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

**OR OTHER THAN SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

(Column 1) (Column 2) (Column 3)

AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(j))	*	Minus	**	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=
	Application Size Fee (37 CFR 1.16(s))				
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					

**SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

**OR OTHER THAN SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 4 columns: APPLICATION NUMBER (13/438,754), FILING OR 371(C) DATE (04/03/2012), FIRST NAMED APPLICANT (Hermen-ard Hulst), ATTY. DOCKET NO./TITLE (87790-837121 (000160US))

CONFIRMATION NO. 3525

FORMALITIES LETTER



20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

Date Mailed: 04/19/2012

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing. Applicant must submit \$95 to complete the basic filing fee for a small entity.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$65 for a small entity in compliance with 37 CFR 1.27, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within TWO MONTHS from the date of this Notice is \$595 for a small entity

- \$95 Statutory basic filing fee.
\$65 Surcharge.
The application search fee has not been paid. Applicant must submit \$310 to complete the search fee.
The application examination fee has not been paid. Applicant must submit \$125 to complete the examination fee for a small entity in compliance with 37 CFR 1.27.

Replies should be mailed to:

Mail Stop Missing Parts  
Commissioner for Patents  
P.O. Box 1450  
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.  
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

*/megga/*

---

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/438,754, 04/03/2012, 2827, 0.00, 87790-837121 (000160US), 1, 1

CONFIRMATION NO. 3525

20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

FILING RECEIPT



Date Mailed: 04/19/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Hermen-ard Hulst, Amsterdam, NETHERLANDS;
Patrick Sandor Racz, Saint Heller, NJ;

Assignment For Published Patent Application

Smartflash Technologies Limited, Wickhams' Cay, VIRGIN ISLANDS, BRITISH

Power of Attorney: The patent practitioners associated with Customer Number 20350

Domestic Priority data as claimed by applicant

This application is a CON of 13/212,047 08/17/2011
which is a CON of 12/943,872 11/10/2010 PAT 8118221
which is a CON of 12/014,558 01/15/2008 PAT 7942317
which is a CON of 11/336,758 01/19/2006 PAT 7334720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB2000/104110 10/25/2000

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

UNITED KINGDOM 9925227.2 10/25/1999

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to Retrieve Electronic Priority Application(s) (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

If Required, Foreign Filing License Granted: 04/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/438,754**

**Projected Publication Date:** To Be Determined - pending completion of Missing Parts

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

Data Storage and Access Systems

**Preliminary Class**

365

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](http://SelectUSA.gov).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/438,754	04/03/2012	Hermen-ard Hulst	87790-837121 (000160US)

**CONFIRMATION NO. 3525**

**POA ACCEPTANCE LETTER**

20350  
KILPATRICK TOWNSEND & STOCKTON LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834



Date Mailed: 04/19/2012

**NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 04/03/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/truong/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on May 7, 2012

PATENT

Attorney Docket No.: 87790-000160US-837121

Client Ref. No.: PN759544USG

KILPATRICK TOWNSEND & STOCKTON LLP

By: Leslie Ehrlich  
Leslie Ehrlich

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of: HULST and RACZ	Confirmation No.: 3525
Application No.: 13/438,754	Examiner: Not Yet Assigned
Filed: April 3, 2012	Technology Center/Art Unit: 2827
For: DATA STORAGE ACCESS SYSTEMS	<u>REQUEST FOR CORRECTED FILING RECEIPT</u>
Customer No.: 20350	

Mail Stop Missing Parts  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

Attached hereto is a markup copy of the Official Filing Receipt received from the Patent Office in the above-noted application which shows the requested change in red and for which issuance of a corrected filing receipt is respectfully requested. The typographical error is due to USPTO processing.

The **Applicant(s)** section of the Filing Receipt is incorrect. The residence of inventor Patrick Sandor Racz is incorrect and should read: **Patrick Sandor Racz, Saint Heller, United Kingdom**, not Patrick Sandor Racz, Saint Heller, NJ. Saint Heller is a city in the State of Jersey in the United Kingdom.

A copy of the Application Data Sheet (ADS) as filed on April 3, 2012 is also enclosed.



HULST and RACZ  
Appl. No. 13/438,754

PATENT  
Attorney Docket No.: 87790-000160US-837121  
Client Ref. No.: PN759544USG

Applicants requests that a Corrected Filing Receipt be issued and all U.S. Patent and Trademark Office records be updated to reflect the requested corrections.

Respectfully submitted,



Babak Kusha  
Registration No. 51,095

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 415-576-0200  
Fax: 415-576-0300  
Attachments

LE



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/438,754, 04/03/2012, 2827, 0.00, 87790-837121 (000160US), 1, 1

CONFIRMATION NO. 3525

20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

FILING RECEIPT



Date Mailed: 04/19/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Hermen-ard Hulst, Amsterdam, NETHERLANDS;
Patrick Sandor Racz, Saint Heller ~~UK~~ United Kingdom

Assignment For Published Patent Application

Smartflash Technologies Limited, Wickhams' Cay, VIRGIN ISLANDS, BRITISH

Power of Attorney: The patent practitioners associated with Customer Number 20350

Domestic Priority data as claimed by applicant

This application is a CON of 13/212,047 08/17/2011
which is a CON of 12/943,872 11/10/2010 PAT 8118221
which is a CON of 12/014,558 01/15/2008 PAT 7942317
which is a CON of 11/336,758 01/19/2006 PAT 7334720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB2000/104110 10/25/2000

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

UNITED KINGDOM 9925227.2 10/25/1999

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to Retrieve Electronic Priority Application(s) (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

If Required, Foreign Filing License Granted: 04/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/438,754**

**Projected Publication Date:** To Be Determined - pending completion of Missing Parts

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

Data Storage and Access Systems

**Preliminary Class**

365

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](http://SelectUSA.gov).

## Application Data Sheet

### Application Information

Application number::

Filing Date::

Application Type:: Regular

Subject Matter:: Utility

Suggested classification::

Suggested Group Art Unit::

CD-ROM or CD-R???:

Number of CD disks::

Number of copies of CDs::

Sequence Submission::

Computer Readable Form (CRF)?::

Number of copies of CRF::

Title:: Data Storage and Access Systems

Attorney Docket Number:: 87790-837121 (000160US)

Request for Early Publication:: No

Request for Non-Publication:: No

Suggested Drawing Figure::

Total Drawing Sheets:: 17

Small Entity?:: Yes

Latin name::

Variety denomination name::

Petition included?:: No

Petition Type::

Licensed US Govt. Agency::

Contract or Grant Numbers One::

Secrecy Order in Parent Appl.:: No

## **Applicant Information**

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: United Kingdom  
Status:: Full Capacity  
Given Name:: Patrick  
Middle Name::  
Family Name:: Racz  
Name Suffix::  
City of Residence:: Saint Heller  
State or Province of Residence:: Jersey  
Country of Residence:: United Kingdom  
Street of Mailing Address:: 19 Royal Street  
City of Mailing Address:: Saint Heller  
State or Province of mailing address:: Jersey  
Country of mailing address:: United Kingdom  
Postal or Zip Code of mailing address:: JE1 4WA

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: Netherlands  
Status:: Full Capacity  
Given Name:: Hermen-ard  
Middle Name::  
Family Name:: Hulst  
Name Suffix::  
City of Residence:: Amsterdam  
State or Province of Residence::  
Country of Residence:: Netherlands  
Street of Mailing Address:: Van Tuyll van Serooskerweg 75hs  
City of Mailing Address:: Amsterdam  
State or Province of mailing address::  
Country of mailing address:: Netherlands

Postal or Zip Code of mailing address:: 1076 JG

**Correspondence Information**

Correspondence Customer Number:: 20350

**Representative Information**

Representative Customer Number:: 20350

**Domestic Priority Information**

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application is a	Continuation of	13/212,047	08/17/11
13/212,047	Continuation of	12/943,872	11/10/10
12/943,872	Continuation of	12/014,558	01/15/08
12/014,558	Continuation of	11/336,758	01/19/06
11/336,758	Continuation of	10/111,716	09/17/02

**Foreign Priority Information**

Country::	Application number::	Filing Date::
PCT	GB00104110	10/25/00
United Kingdom	9925227.2	10/25/99

**Assignee Information**

Assignee Name:: Smartflash Technologies Limited  
Street of mailing address:: 1070908 Palm Grove House, P.O. Box 438  
City of mailing address:: Wickhams' Cay, Road Town  
State or Province of mailing address:: Tortola  
Country of mailing address:: British Virgin Islands  
Postal or Zip Code of mailing address::

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	12715348
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	Data Storage and Access Systems
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Customer Number:</b>	20350
<b>Filer:</b>	Babak Kusha/Leslie Ehrlich
<b>Filer Authorized By:</b>	Babak Kusha
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	07-MAY-2012
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	13:02:32
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Corrected Filing Receipt	RequestCorrectedFilingReceipt_87790-001600US-837121.pdf	256546 <small>0b60d172d30704b5cffe6974c092297acebd6c0a</small>	no	5

### Warnings:

### Information:



2	Application Data Sheet	ADS_87790-000160US-837121.pdf	76504 467da0cfb5180df25dae36d50e2226ac81f06fe1	no	3
---	------------------------	-------------------------------	---	----	---

**Warnings:**

**Information:**

This is not an USPTO supplied ADS fillable form

<b>Total Files Size (in bytes):</b>	333050
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/438,754, 04/03/2012, 2827, 0.00, 87790-837121 (000160US), 1, 1

CONFIRMATION NO. 3525

CORRECTED FILING RECEIPT



20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

Date Mailed: 05/16/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Hermen-ard Hulst, Amsterdam, NETHERLANDS;
Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;

Assignment For Published Patent Application

Smartflash Technologies Limited, Wickhams' Cay, VIRGIN ISLANDS, BRITISH

Power of Attorney: The patent practitioners associated with Customer Number 20350

Domestic Priority data as claimed by applicant

This application is a CON of 13/212,047 08/17/2011
which is a CON of 12/943,872 11/10/2010 PAT 8118221
which is a CON of 12/014,558 01/15/2008 PAT 7942317
which is a CON of 11/336,758 01/19/2006 PAT 7334720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB2000/104110 10/25/2000

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

UNITED KINGDOM 9925227.2 10/25/1999

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to Retrieve Electronic Priority Application(s) (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

If Required, Foreign Filing License Granted: 04/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/438,754**

**Projected Publication Date:** To Be Determined - pending completion of Missing Parts

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

Data Storage and Access Systems

**Preliminary Class**

365

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](http://SelectUSA.gov).

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> (Not for submission under 37 CFR 1.99)	<b>Application Number</b>		13/438,754	
	<b>Filing Date</b>		April 3, 2012	
	<b>First Named Inventor</b>		Hermen-ard Hulst	
	<b>Art Unit</b>		2827	
	<b>Examiner Name</b>			
	<b>Attorney Docket Number</b>		87790-837121 000160US	

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	4,590,365		05-1986	Okada	
	2.	5,682,027		10-1997	Bertina et al.	
	3.	6,025,973		02-2000	Mizoshita et al.	
	4.	6,981,179		12-2005	Shigemasa et al.	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup>	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>

EXAMINER SIGNATURE		
Examiner Signature		Date Considered

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	13591550
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	Data Storage and Access Systems
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Annette Valdivia
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	27-AUG-2012
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	12:00:05
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		837121IDS.PDF	136569 e1cf773b28821b4ec35e511497cd8e8305164e01	yes	3

<b>Multipart Description/PDF files in .zip description</b>			
<b>Document Description</b>		<b>Start</b>	<b>End</b>
Transmittal Letter		1	2
Information Disclosure Statement (IDS) Form (SB08)		3	3

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	136569
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on 8/27/2012

PATENT  
Attorney Docket No.: 87790-837121-000160US

KILPATRICK TOWNSEND & STOCKTON LLP

By: Arnette Valdivia

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of:

Hermen-ard Hulst

Application No.: 13/438,754

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No.: 20350

Confirmation No.: 3525

Examiner:

Technology Center/Art Unit: 2827

INFORMATION DISCLOSURE

STATEMENT

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

The references cited on attached form PTO/SB/08A are being called to the attention of the Examiner. If required, copies of some of the references in compliance with the requirements of 37 CFR § 1.98(a)(2) are enclosed. The references cited in this IDS were cited in Office Action dated July 12, 2012 in related U.S. Patent Application No. 13/212,047. Copies of these Office Actions in U.S. Patent Application No. 13/212,047 are available on PAIR and are believed to be readily accessible to the Examiner.


It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.



As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement. However, if any additional fees are due for the submission of this Information Disclosure Statement, please deduct those fees from Deposit Account No. 20-1430.

Respectfully submitted,



Benjamin J. Holt  
Registration No. 67,536

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 415-576-0200  
Fax: 415-576-0300  
Attachments

**IN THE U.S. PATENT AND TRADEMARK OFFICE**

In re Application of: <b>PATRICK RACZ, et al.</b>	)	Confirmation No. 3525
	)	
Application No.: 13/438,754	)	Art Unit: 2827
	)	
Filed: April 3, 2012	)	Examiner:
	)	
For: DATA STORAGE AND ACCESS	)	Docket No: 87790-837121
SYSTEMS	)	(000160US)

**RESPONSE TO NOTICE TO FILE MISSING PARTS – FILING DATE GRANTED**

Attention: Mail Stop Missing Parts  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Transmitted herewith are papers in the above-identified application.

- Formalities Letter – Notice to File Missing Parts of Application – Filing Date Granted.
- Declaration and Power of Attorney.
- Executed Declaration.
- Power of Attorney and Certificate of Assignee under 37 C.F.R. § 3.73(b).
- Petition for Extension of Time Under 37 C.F.R. § 1.136. (4 months)
- Application Data Sheet
- The fee is calculated on the attached PTO/SB/17.
- Applicant claims small entity status.
- Payment in the amount of **\$2,257** is submitted.
- Form PTO-2038 is attached.
- Preliminary Amendment
- The Commissioner is hereby authorized to charge any additional fees required under 37 CFR §1.16, or credit any overpayment, to Account No. 20-1430.

**Certificate of Electronic Filing**

I hereby certify that this correspondence is being electronically filed with The United States Patent Office via EFS Web, on October 19, 2012.

\_\_\_\_\_/Sylvia E. Arnold/

KILPATRICK TOWNSEND &  
STOCKTON LLP  
Two Embarcadero Center  
8<sup>th</sup> Floor  
San Francisco, CA 94111-3834  
Telephone: **925-472-5000**

By: \_\_\_\_\_/Ben Holt/  
Benjamin J. Holt  
Attorney for Applicant  
Reg. No. 67,536

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**FEE TRANSMITTAL***Complete if Known*

Application Number	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Racz et al.
Examiner Name	
Art Unit	2827
Practitioner Docket No.	87790-837121(000160US)

 Applicant claims small entity status. See 37 CFR 1.27**TOTAL AMOUNT OF PAYMENT** (\$) 2,257**METHOD OF PAYMENT** (check all that apply)

- Check  Credit Card  Money Order  None  Other (please identify) : \_\_\_\_\_
- Deposit Account Deposit Account Number: 20-1430 Deposit Account Name: Kilpatrick Townsend & Stockton, LLP
- For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)
- Charge fee(s) indicated below  Charge fee(s) indicated below, **except for the filing fee**
- Charge any additional fee(s) or underpayments of fee(s)  Credit any overpayments
- Under 37 CFR 1.16 and 1.17

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.****FEE CALCULATION****1. BASIC FILING, SEARCH, AND EXAMINATION FEES**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee(\$)	Fee(\$)	Small Entity Fee(\$)	Fee(\$)	Small Entity Fee(\$)	
Utility	380	190 (98)	620	310	250	125	533
Design	250	125	120	60	160	80	_____
Plant	250	125	380	190	200	100	_____
Reissue	380	190	620	310	750	375	_____
Provisional	250	125	0	0	0	0	_____

**2. EXCESS CLAIM FEES**

Fee Description	Small Entity Fee (\$)	Fee (\$)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225
<b>Total Claims</b>	<b>Extra Claims</b>	<b>Fee(\$)</b>
<u>29</u> - 20 or HP= <u>9</u> x <u>31</u> = <u>279</u>		
HP = highest number of total claims paid for, if greater than 20.		
<b>Indep. Claims</b>	<b>Extra Claims</b>	<b>Fee(\$)</b>
<u>6</u> - 3 or HP= <u>3</u> x <u>125</u> = <u>375</u>		
HP = highest number of independent claims paid for, if greater than 3.		

**3. APPLICATION SIZE FEE**

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee (\$)	Fee Paid (\$)
_____ - 100 = _____	/ 50 = _____	(round up to a whole number) x _____	_____ = _____	_____

**4. OTHER FEE(S)**

	Fees Paid (\$)
Non-English Specification, \$130 fee (no small entity discount)	_____
Non-electronic filing fee under 37 CFR 1.16(t) for a utility application, \$400 fee (\$200 small entity)	_____
Other (e.g., late filing surcharge) :	65

**SUBMITTED BY**

Signature	/Ben Holt/	Registration No. (Attorney/Agent)	67,536	Telephone	925-472-5000
Name (Print/Type)	Benjamin J. Holt	Date	October 19, 2012		

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

64597901V.1

If you need assistance in completing this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b>		Docket Number (Optional)																											
Application Number 13/438,754		87790-837121(000160US)																											
For DATA STORAGE AND ACCESS SYSTEMS		Filed April 3, 2012																											
Art Unit 2827		Examiner																											
<p>This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.</p> <p>The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):</p> <table border="0"> <thead> <tr> <th></th> <th style="text-align: center;"><u>Fee</u></th> <th style="text-align: center;"><u>Small Entity Fee</u></th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> One month (37 CFR 1.17(a)(1))</td> <td style="text-align: center;">\$150</td> <td style="text-align: center;">\$75</td> <td style="text-align: center;">\$ _____</td> </tr> <tr> <td><input type="checkbox"/> Two months (37 CFR 1.17(a)(2))</td> <td style="text-align: center;">\$570</td> <td style="text-align: center;">\$285</td> <td style="text-align: center;">\$ _____</td> </tr> <tr> <td><input type="checkbox"/> Three months (37 CFR 1.17(a)(3))</td> <td style="text-align: center;">\$1290</td> <td style="text-align: center;">\$645</td> <td style="text-align: center;">\$ _____</td> </tr> <tr> <td><input checked="" type="checkbox"/> Four months (37 CFR 1.17(a)(4))</td> <td style="text-align: center;">\$2010</td> <td style="text-align: center;">\$1005</td> <td style="text-align: center;">\$<u>1005</u></td> </tr> <tr> <td><input type="checkbox"/> Five months (37 CFR 1.17(a)(5))</td> <td style="text-align: center;">\$2690</td> <td style="text-align: center;">\$1345</td> <td style="text-align: center;">\$ _____</td> </tr> </tbody> </table> <p><input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.</p> <p><input type="checkbox"/> A check in the amount of the fee is enclosed.</p> <p><input checked="" type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.</p> <p><input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number <u>20-1430</u> .</p> <p><b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b></p> <p>I am the <input type="checkbox"/> applicant/inventor.</p> <p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71 Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).</p> <p><input checked="" type="checkbox"/> attorney or agent of record. Registration Number <u>67,536</u></p> <p><input type="checkbox"/> attorney or agent under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____ .</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 50%; text-align: center;"> <u>/Ben Holt/</u>            _____            Signature            Benjamin J. Holt            _____            Typed or printed name         </td> <td style="width: 50%; text-align: center;"> <u>October 19, 2012</u>            _____            Date            925 472 3129            _____            Telephone Number         </td> </tr> </table> <p>NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.</p> <p><input type="checkbox"/> Total of _____ forms are submitted.</p>					<u>Fee</u>	<u>Small Entity Fee</u>		<input type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$150	\$75	\$ _____	<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$570	\$285	\$ _____	<input type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1290	\$645	\$ _____	<input checked="" type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$2010	\$1005	\$ <u>1005</u>	<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$2690	\$1345	\$ _____	<u>/Ben Holt/</u> _____ Signature Benjamin J. Holt _____ Typed or printed name	<u>October 19, 2012</u> _____ Date 925 472 3129 _____ Telephone Number
	<u>Fee</u>	<u>Small Entity Fee</u>																											
<input type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$150	\$75	\$ _____																										
<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$570	\$285	\$ _____																										
<input type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1290	\$645	\$ _____																										
<input checked="" type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$2010	\$1005	\$ <u>1005</u>																										
<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$2690	\$1345	\$ _____																										
<u>/Ben Holt/</u> _____ Signature Benjamin J. Holt _____ Typed or printed name	<u>October 19, 2012</u> _____ Date 925 472 3129 _____ Telephone Number																												

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

64598130V.1

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on October 19, 2012.

PATENT  
Attorney Docket No.: 87790-837121 (000160US)  
Client Ref. No.: PN759544USG

KILPATRICK TOWNSEND & STOCKTON LLP

By: /Sylvia E. Arnold/

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

PATRICK RACZ, ET AL.

Application No. 13/438,754

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No. 20350

Confirmation No.: 3525

Examiner: (not yet assigned)

Art Unit: 2827

SECOND PRELIMINARY AMENDMENT

Mail Stop PCT  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

Prior to examination of the above-referenced application, please enter the  
following amendments and remarks:

**Amendments to the Claims** are reflected in the listing of the claim which begins on page 2 of  
this paper.

**Remarks/Arguments** begin on page 4 of this paper.

**Amendments to the Claims:**

This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of Claims:**

Claims 1-39 (canceled)

- 1           40.   (Previously Presented) A handheld multimedia terminal, comprising:  
2                   a wireless interface configured to interface with a wireless network for accessing  
3 a remote computer system;  
4                   non-volatile memory configured to store multimedia content, wherein said  
5 multimedia content comprises one or more of music data, video data and computer game data;  
6                   a program store storing processor control code;  
7                   a processor coupled to said non-volatile memory, said program store, said  
8 wireless interface and  
9                   a user interface to allow a user to select and play said multimedia content;  
10                  a display for displaying one or both of said played multimedia content and data  
11 relating to said played multimedia content;  
12                  wherein the processor control code comprises:  
13                   code to request identifier data identifying one or more items of multimedia  
14 content stored in the non-volatile memory;  
15                   code to receive said identifier data;  
16                   code to present to a user on said display said identified one or more items of  
17 multimedia content available from the non-volatile memory;  
18                   code to receive a user selection to select at least one of said one or more of said  
19 stored items of multimedia content;  
20                   code responsive to said user selection of said at least one selected item of  
21 multimedia content to transmit payment data relating to payment for said at least one selected  
22 item of multimedia content via said wireless interface for validation by a payment validation  
23 system;

24 code to receive payment validation data via said wireless interface defining if said  
25 payment validation system has validated payment for said at least one selected item of  
26 multimedia content; and

27 code to control access to said at least one selected item of multimedia content on  
28 said terminal responsive to said payment validation data,

29 wherein said user interface is operable to enable a user to select said at least one  
30 item of multimedia content available from said non-volatile memory; and

31 wherein said user interface is operable to enable a user to access said at least one  
32 selected item of multimedia content responsive to said code to control access permitting access  
33 to said at least one selected item of multimedia content.

1 41. (New) A content data supply server for providing an item of multimedia  
2 content to a handheld multimedia terminal, the content data supply server comprising:

3 a communications interface for communicating with the handheld  
4 multimedia terminal;

5 a program store storing code implementable by a processor;

6 a data store for storing identifier data identifying one or more items of multimedia  
7 content available to the handheld multimedia terminal; and

8 a processor coupled to the communications interface, to the program store  
9 and the data store, the code comprising:

10 code to receive a request from the handheld multimedia terminal for the  
11 identifier data identifying the one or items multimedia content available to the handheld  
12 multimedia terminal;

13 code to retrieve the identifier data from the data store;

14 code to transmit the identifier data via the communications interface to the  
15 handheld multimedia terminal;

16 code to receive payment validation data validating a user purchase of an  
17 item of the multimedia content; and

18 code responsive to the payment validation data validating the user purchase to  
19 retrieve the purchased item of multimedia content data from a multimedia content store and

20 transmit the purchased item of multimedia content via the communications interface to the  
21 handheld multimedia terminal.

1 42. (New) A content data supply server as claimed in claim 41, further  
2 comprising code to receive payment record data indicating a payment made by a user for the  
3 item of multimedia content.

1 43. (New) A content data supply server as claimed in claim 42, further  
2 comprising code responsive to receiving the payment record data to request the payment  
3 validation data.

1 44. (New) A content data supply server as claimed in claim 43, wherein the  
2 code to request the payment validation data comprises code to transmit at least a portion of the  
3 payment record data.

1 45. (New) A content data supply server as claimed in claim 41, wherein the  
2 data supply server comprises the multimedia content store.

1 46. (New) A content data supply server as claimed in claim 41, further  
2 comprising:  
3 code to receive a request from the handheld multimedia terminal for content  
4 information pertaining to at least one of the items of multimedia content identified by the  
5 identifier data, wherein the content information comprises one or more of description data and  
6 cost data;  
7 code to retrieve the content information from the data store; and  
8 code to transmit the content information to the handheld multimedia terminal.

1 47. (New) A content data supply server as claimed in claim 41, wherein the  
2 item of multimedia content comprises one or more of music, films, TV programs, text, software,  
3 or games software.

1 48. (New) A content data supply server as claimed in claim 41, further  
2 comprising:



3 code responsive to the payment validation data validating the user purchase to  
4 transmit at least one access rule to the handheld multimedia terminal,  
5 wherein the at least one access rule specifies at least one condition for accessing  
6 the retrieved and purchased item of multimedia content data.

1 49. (New) A content data supply server as claimed in claim 48, wherein the  
2 data store or multimedia content store further stores the at least one access rule, and further  
3 comprising code to read the at least one access rule from the data store or multimedia content  
4 store.

1 50. (New) A method of providing an item of multimedia content to a  
2 handheld multimedia terminal, the method comprising:  
3 receiving a request from the handheld multimedia terminal for identifier  
4 data identifying one or more items of multimedia content data available to the handheld  
5 multimedia terminal;  
6 retrieving the identifier data from a data store;  
7 transmitting the identifier data to the handheld multimedia terminal;  
8 receiving payment validation data validating a user purchase of an item of  
9 multimedia content; and  
10 responsive to the payment validation data validating the user purchase,  
11 retrieving the purchased item of multimedia content data from a multimedia content store and  
12 transmitting the purchased item of multimedia content to the handheld multimedia terminal.

1 51. (New) A method as claimed in claim 50, further comprising receiving  
2 payment record data indicating a payment made by a user for the item of multimedia content.

1 52. (New) A method as claimed in claim 51, further comprising requesting  
2 the payment validation data responsive to receiving the payment record data.

1 53. (New) A method as claimed in claim 52, wherein the requesting the  
2 payment validation data comprises transmitting at least a portion of the payment record data.

1 54. (New) A method as claimed in claim 50, further comprising:

2 receiving a request from the handheld multimedia terminal for content  
3 information pertaining to at least one of the items of multimedia content identified by the  
4 identifier data, wherein the content information comprises one or more of description data and  
5 cost data;

6 retrieving the content information from the data store; and  
7 transmitting the content information to the handheld multimedia terminal.

1 55. (New) A method as claimed in claim 50, further comprising:  
2 responsive to the payment validation data validating the user purchase,  
3 transmitting at least one access rule to the handheld multimedia terminal,  
4 wherein the at least one access rule specifies at least one condition for accessing  
5 the retrieved and purchased item of multimedia content data.

1 56. (New) A method as claimed in claim 55, further comprising reading the at  
2 least one access rule from the data store or multimedia content store.

1 57. (New) A computer system for providing multimedia data items to a  
2 handheld multimedia terminal, the system comprising:  
3 a communications interface;  
4 a data store for storing records of multimedia data items available from the  
5 system, each record comprising a data item description and a pointer to a data provider for the  
6 data item;

7 a program store storing code implementable by a processor;  
8 a processor coupled to the communications interface, to the data store, and to the  
9 program store for implementing the stored code, the code comprising:

10 code to receive a request for a multimedia data item from the handheld  
11 multimedia terminal;

12 code to receive from the communications interface payment validation data  
13 comprising data confirming payment for the requested multimedia data item;

14 code responsive to the request and to the received payment validation data, to read  
15 the requested multimedia data item from a content provider; and

16 code to transmit the read multimedia data item to the handheld multimedia  
17 terminal over the communications interface.

1 58. (New) A computer system as claimed in claim 57, further comprising  
2 code to receive payment record data indicating a payment made by a user for the item of  
3 multimedia content.

1 59. (New) A computer system in claim 58, further comprising code  
2 responsive to the receiving the payment record data to request the payment validation data.

1 60. (New) A computer system as claimed in claim 57, further comprising:  
2 code responsive to the request and to the received payment validation data, to  
3 transmit at least one access rule to the handheld multimedia terminal,  
4 wherein the at least one access rule specifies at least one condition for accessing  
5 the retrieved and purchased item of multimedia content data.

1 61. (New) A portable data carrier, comprising:  
2 an interface for reading and writing data from and to the carrier;  
3 non-volatile data memory, coupled to the interface, for storing data on the  
4 carrier;  
5 non-volatile payment data memory, coupled to the interface, for providing  
6 payment data to an external device; and  
7 non-volatile communications parameter memory for storing data for  
8 accessing a communications network to receive data from the communications network for  
9 storage in the data memory.

1 62. (New) A portable data carrier as claimed in claim 61, wherein the data  
2 memory is partitioned for access on a block-by-block basis, each block comprising a plurality of  
3 data bytes read or written as a set.

1 63. (New) A portable data carrier as claimed in claim 61, wherein the data  
2 memory has a capacity of greater than 1 MByte, more preferably greater than 100 Mbytes, and  
3 most preferably greater than 1GByte.

1           64.   (New) A method of downloading multimedia content from a content data  
2 supply server to a handheld multimedia terminal, the method comprising:  
3           requesting, via a wireless interface on the handheld multimedia terminal,  
4 identifier data identifying one or more items of multimedia content available for retrieving,  
5           receiving the identifier data via the wireless interface,  
6           requesting content information via the wireless interface, wherein the content  
7 information comprises one or more of description data and cost data pertaining to at least one of  
8 the one or more items of multimedia content identified by the identifier data;  
9           receiving the content information via said wireless interface;  
10          presenting the content information pertaining to the identified one or more items  
11 of multimedia content available for retrieving to a user on a display of the handheld multimedia  
12 terminal;  
13          receiving a user selection selecting at least one of the one or more items of  
14 multimedia content available for retrieving;  
15          responsive to the user selection of the at least one item of multimedia  
16 content transmitting payment data relating to payment for the selected at least one item of  
17 multimedia content via the wireless interface for validation by a payment validation system;  
18          receiving payment validation data via the wireless interface defining if the  
19 payment validation system has validated payment for the selected at least one item of multimedia  
20 content; and  
21          responsive to the payment validation data retrieving the selected at least one item  
22 of multimedia content via the wireless interface from a content data supply server, writing the  
23 retrieved at least one item of multimedia content into non-volatile memory on the handheld  
24 multimedia terminal.

1           65.   (New) A method as claimed in claim 64, further comprising:  
2           retrieving at least one access rule from the content data supply server,  
3           wherein the at least one access rule specifies at least one condition for accessing  
4 the retrieved and purchased item of multimedia content data.

1                   66.   (New) A method as claimed in claim 64, wherein the non-volatile  
2 memory comprises flash memory.

1                   67.   (New) A method as claimed in claim 64, wherein the multimedia content  
2 comprises one or more of music, films, TV programs, text, software, or games software.

**REMARKS/ARGUMENTS**

Claims 1-39 from the prior continuation application have been canceled.

Claim 40 is presently pending.

Claims 41-67 are new and are presently pending.

**CONCLUSION**

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 925-472-4741.

Further, the Commissioner is hereby authorized to charge any additional fees or credit any overpayment in connection with this paper to Deposit Account No. 20-1430.

Respectfully submitted,

/Ben Holt/

Benjamin J. Holt  
Registration No. 67,536

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 415-576-0200  
Fax: 415-576-0300  
BJH/sea  
64597529V.1

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754
<b>Filing Date:</b>	03-Apr-2012
<b>Title of Invention:</b>	Data Storage and Access Systems
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Attorney Docket Number:</b>	87790-837121 (000160US)

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
Utility filing Fee (Electronic filing)	4011	1	98	98
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125

### Pages:

### Claims:

Claims in excess of 20	2202	9	31	279
Independent claims in excess of 3	2201	3	125	375

### Miscellaneous-Filing:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Late filing fee for oath or declaration	2051	1	65	65
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
Extension - 4 months with \$0 paid	2254	1	1005	1005
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>2257</b>



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	14034877
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	Data Storage and Access Systems
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	19-OCT-2012
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	18:42:05
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$2257
RAM confirmation Number	5820
Deposit Account	201430
Authorized User	KILPATRICK TOWNSEND & STOCKTON, LLP

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	2012_10_19_RESP_NOMP_87790-837121-000160US.pdf	73549 247548f05ed1797f8ee5edf6253d31bc83fde388	no	1
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (SB06)	2012_10_19_FEE_TRNS_87790-837121-000160US.pdf	134546 ca74746d04ea4b09e133234b607b5208ba1ebfe9	no	1
<b>Warnings:</b>					
<b>Information:</b>					
3	Extension of Time	2012_10_19_EXT_87790-837121-000160US.pdf	119328 cccd31ae4a32c93b815c7bd26a6a865d54835481	no	1
<b>Warnings:</b>					
<b>Information:</b>					
4	Preliminary Amendment	2012_10_19_PRE_AMD_87790-837121-000160US.pdf	88998 3a9bef83b50d924b6b6c86d79b6a761ed47b5ebd	no	10
<b>Warnings:</b>					
<b>Information:</b>					
5	Fee Worksheet (SB06)	fee-info.pdf	41319 d6d223b87a32b1fab178f6ccfb28a4123a0567	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			457740		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	14034877
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
Adjustment date: 11/07/2012 ABALINAN 10/22/2012 INTEFSW 00005820 13438754 04 FC:2202 -279.00 OP  11/07/2012 ABALINAN 00000013 13438754 01 FC:2202 248.00 OP  <b>Title of Invention:</b> Refund Ref: 11/07/2012 0030117897 ----- Credit Card Refund Total: \$31.00  Am Exp.: XXXXXXXXXXXX1003	Data Storage and Access Systems
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	19-OCT-2012
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	18:42:05
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 2257
RAM confirmation Number	5820
Deposit Account	201430
Authorized User	KILPATRICK TOWNSEND & STOCKTON, LLP

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

**PATENT APPLICATION FEE DETERMINATION RECORD**

Substitute for Form PTO-875

Application or Docket Number  
13/438,754

**APPLICATION AS FILED - PART I**

(Column 1) (Column 2)

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A
TOTAL CLAIMS (37 CFR 1.16(j))	28 minus 20 = *	8
INDEPENDENT CLAIMS (37 CFR 1.16(h))	6 minus 3 = *	3
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		

\* If the difference in column 1 is less than zero, enter "0" in column 2.

**SMALL ENTITY**

RATE(\$)	FEE(\$)
N/A	98
N/A	310
N/A	125
x 31 =	248
x 125 =	375
	0.00
	0.00
<b>TOTAL</b>	<b>1156</b>

**OR OTHER THAN SMALL ENTITY**

RATE(\$)	FEE(\$)
N/A	
N/A	
N/A	
<b>TOTAL</b>	

**APPLICATION AS AMENDED - PART II**

(Column 1) (Column 2) (Column 3)

AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(i))	*	Minus	**	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=
	Application Size Fee (37 CFR 1.16(s))				
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))				

**SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

**OR OTHER THAN SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

(Column 1) (Column 2) (Column 3)

AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(i))	*	Minus	**	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=
	Application Size Fee (37 CFR 1.16(s))				
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))				

**SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

**OR OTHER THAN SMALL ENTITY**

RATE(\$)	ADDITIONAL FEE(\$)
x =	
x =	
<b>TOTAL ADD'L FEE</b>	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

\*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/438,754, 04/03/2012, 2827, 1221, 87790-837121 (000160US), 28, 6

CONFIRMATION NO. 3525

UPDATED FILING RECEIPT

20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834



Date Mailed: 11/13/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Inventor(s)

Hermen-ard Hulst, Amsterdam, NETHERLANDS;
Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;

Applicant(s)

Hermen-ard Hulst, Amsterdam, NETHERLANDS;
Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;

Assignment For Published Patent Application

Smartflash Technologies Limited, Wickhams' Cay, VIRGIN ISLANDS, BRITISH

Power of Attorney: The patent practitioners associated with Customer Number 20350

Domestic Priority data as claimed by applicant

This application is a CON of 13/212,047 08/17/2011
which is a CON of 12/943,872 11/10/2010 PAT 8118221
which is a CON of 12/014,558 01/15/2008 PAT 7942317
which is a CON of 11/336,758 01/19/2006 PAT 7334720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB2000/104110 10/25/2000

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

UNITED KINGDOM 9925227.2 10/25/1999

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to

**Retrieve Electronic Priority Application(s)** (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

**If Required, Foreign Filing License Granted:** 04/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/438,754**

**Projected Publication Date:** 02/21/2013

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

Data Storage and Access Systems

**Preliminary Class**

365

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](http://SelectUSA.gov).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
13/438,754 04/03/2012 Hermen-ard Hulst 87790-837121 (000160US) 3525

20350 7590 01/07/2013
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

LE, THIEN MINH

ART UNIT PAPER NUMBER

2887

NOTIFICATION DATE DELIVERY MODE

01/07/2013

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipefiling@kilpatricktownsend.com
jlhice@kilpatrick.foundationip.com



<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	13/438,754	HULST ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Thien M. Le	2887	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 10/19/2012 and 4/3/2012.
- 2a)  This action is **FINAL**.
- 2b)  This action is non-final.
- 3)  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 5)  Claim(s) 41-67 is/are pending in the application.
- 5a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 6)  Claim(s) \_\_\_\_\_ is/are allowed.
- 7)  Claim(s) 41-67 is/are rejected.
- 8)  Claim(s) \_\_\_\_\_ is/are objected to.
- 9)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

\* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).

**Application Papers**

- 10)  The specification is objected to by the Examiner.
- 11)  The drawing(s) filed on 03 April 2012 is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

**Priority under 35 U.S.C. § 119**

- 12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All   b)  Some \* c)  None of:
  - 1.  Certified copies of the priority documents have been received.
  - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - 3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 4/3/2012; 8/27/2012.
- 3)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 4)  Other: \_\_\_\_\_.

### **DETAILED ACTION**

The information disclosure statements filed on 4/3/2012 and 8/27/2012 have been entered. The preliminary amendments filed on 4/3/2012 and 10/19/2012 have been entered. Claims 1-39 have been canceled. Claims 40-67 are presented for examination.

#### ***Double Patenting***

A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

**Claim 40** is rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 1 of prior U.S. Patent No. 8,336,772. This is a double patenting rejection.

#### ***Double Patenting***

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims

Art Unit: 2887

are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 41-60 and 64-67 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims of U.S. Patent No. 8,336,772. Although the conflicting claims are not identical, they are not patentably distinct from each other because they essentially reciting the same limitations.

**Claim 41** is rejected in view of the claim 1 of the '772 patent in that they recite a data server comprising the following features:

i. a communication interface for communicating with a hand-held terminal (claim 1: an interface connecting a handheld terminal and a remote data server)

ii. a program store for storing code implemented by a process (claim 1: the remote server receives user selection request, receiving payment data, having a payment validation system, enabling access and allowing access to the multimedia; claim 19: allowing multimedia to be downloaded to the handheld device; thus, a processor and processor control codes are considered to be included in the remote data server);

iii. processor coupled to the communication interfaces (claims 1 and 19: the processor of the data supplier is coupled to the interface for interacting with user's selection, receiving request, processing multimedia purchase data, allowing access and download from the handheld terminal);

iv. code to receive a request from a handheld terminal (claims 1 and 19: the remote server receives request from the handheld terminal for the identifier data identifying one or more items of multimedia contents);

v. code to retrieve the identifier data (claims 1 and 19: upon receiving request for identifier data, the remote server retrieves identifier data from a store and transmit the identifier data to the handheld terminal);

vi. code to transmit identifier data to the handheld terminal (claims 1 and 19: the handheld terminal received identifier data from the remote server via the wireless interface so that the remote server has code instruction to transmit the identifier data);

vii. code to receive payment validation data (claims 1 and 19: the remote data server receive payment validation data from the handheld terminal, having a payment validation system to verify the payment validation data);

viii. code responsive to the payment validation data allowing access and retrieval of purchased multimedia content (claims 1 and 19: the remote data server receive payment validation data from the handheld terminal, having a payment validation system to verify the payment validation data, enable access and download of multimedia content to the handheld device).

As can be seen, claim 41 of this instant application are the combination of various features that have been recited in claims 1 and 19 of the '772 patent and would have been obvious to an ordinary skilled in the art. Thus, the patent protections have been provided to the earlier filed patent application.

**Claim 50** is rejected in view of claim 1 of the '772 patent in that they recite the following features:

i. receiving a request from the handheld multimedia (claim 1: interface for user to select, display and play multimedia, code to request identifier data);

ii. retrieving identifier data (claim 1: code to receive identifier data);

iii. transmitting identifier data to the handheld multimedia terminal (claim 1: receiving identifier data from a remote computer system);

iv. receiving payment validation data (claim 1: remote computer system receives transmitted payment data for the selected multimedia content from the handheld terminal);

v. allowing access to the multimedia content (claim 1: payment validation using payment validation system, permitting access to the selected multimedia item responsive to payment validation data).

As can be seen, claim 50 of this instant application are the combination of various features that have been recited in claim 1 of the '772 patent and would have been obvious to an ordinary skilled in the art. Thus, the patent protections have been provided to the earlier filed patent application.

**Claim 57** is rejected in view of the claim 1 of the '772 patent in that they recite the following features:

i. a wireless communication interface between a handheld device and a remote computer data supplier (claim 1: wireless communication interface);

ii. a program store for storing multimedia content (claim 1: user interfaces allowing user to display, select, play, presenting and transmitting payment information to the remote data supplier (pointer) and receiving access for selected and paid multimedia content);

iii. a process for storing processor control code (claim 1: processor for storing program control code);

Art Unit: 2887

iv. code to receiving a request for a multimedia item from the handheld terminal (claim 1: code to receive a request for multimedia via user selection);

v. code to responsive to the request and payment validation data, enable access to the selected multimedia content (claim 1: code upon receiving request and payment validation data, enable user to select the multimedia content);

vi. code to allow user to select, access and playing the multimedia (claim 1: claim 1, interfaces allowing user to select the multimedia that has proof of purchased, display and playing the multimedia at the handheld terminal).

As can be seen, claim 57 of this instant application are the combination of various features that have been recited in claim 1 of the '772 patent and would have been obvious to an ordinary skilled in the art. Thus, the patent protections have been provided to the earlier filed patent application.

**Claim 64** is rejected in view of the claim 19 of the '772 patent in that it recites:

19. (Original) A data access terminal for retrieving a content data item from a data supplier and providing the retrieved data item to a data carrier, the data access terminal comprising:

a first interface for communicating with the data supplier;

a user interface;

a data carrier interface;

a program store storing code implementable by a processor; and

a processor coupled to the user interface, to the data carrier interface and to the program store for implementing the stored code, the code comprising:

Art Unit: 2887

code to request identifier data identifying one or more content data items available for retrieving;

code to receive said identifier data identifying said one or more content data items available for retrieving;

code to request content information pertaining to at least one of said one or more content data items identified by said identified data;

code to receive said content information;

code to present said content information to a user via said user interface pertaining to said identified one or more content data items available for retrieving;

code to receive a user selection selecting at least one of said one or more of said content data items available for retrieving;

code responsive to said user selection of said selected at least one content data item to transmit payment data relating to payment for said selected at least one content item for validation by a payment validation system;

code to receive payment validation data defining if said payment validation system has validated payment for said selected at least one content data item; and

code responsive to the payment validation data to retrieve said selected at least one content data item from a data supplier and to write said retrieved at least one content data item into said data carrier.

As can be seen, claim 64 of this instant application are the combination of various features that have been recited in claim 19 of the '772 patent and would have been obvious to an ordinary skilled in the art. Thus, the patent protections have been provided to the earlier filed patent application.

**Claims 42-49, 51-56, 58-60, 65-67** of this instant application are the combination of various features that have been recited in the claims of the '772 patent and would have been obvious to an ordinary skilled in the art. Thus, the patent protections have been provided to the earlier filed patent application.



***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 61-62 are rejected under 35 U.S.C. 102(b) as being anticipated by Bertina et al. (Bertina et al. – 5,682,027; herein after referred to as Bertina).

**Regarding claim 61**, Bertina discloses IC card (IC card 13, figure 1) having a non-volatile memory (EEPROM 19) for containing transaction data and non-volatile memory (ROM 17 – figure 1) for storing instructions for conducting transactions with an external transaction device (figure 2).

**Regarding claim 62**, see the discussions regarding claim 61. The EEPROM is considered to include memory partitions as recited in this claim (also noted that applicant's data memory is also an EEPROM – par. 20, page 6 of the specification).

Claims 61-63 are rejected under 35 U.S.C. 102(e) as being anticipated by Gildea et al. (Gildea et al. – 5,861,841; herein after referred to as Gildea).

**Regarding claims 61-63**, Gildea discloses a GPS smart card device comprising a processor 14, a memory 17 of the processor 14 can contain a combination of different types of memories ROM, EPROM, EEPROM, flash ROM, SRAM, DRAM up to the storage capacity of 64 Mbytes (figure 1t, 1b, 8 and their descriptions) and an additional 64 Mbytes of attribute memory. The GPS smart card device can be used to store transaction information (see background of invention: smart card having keypad, built in CPU, EEPROM and other data memories, interface such as display, I/O port to external devices such as a card reader, payment and transaction data storage).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thien M. Le whose telephone number is (571)272-2396. The examiner can normally be reached on Monday - Friday from 7:30am - 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve S. Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thien M. Le/  
Primary Examiner, Art Unit 2887

<b>Notice of References Cited</b>	Application/Control No. 13/438,754	Applicant(s)/Patent Under Reexamination HULST ET AL.	
	Examiner Thien M. Le	Art Unit 2887	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-5,682,027	10-1997	Bertina et al.	235/380
	B US-			
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012							
	40	✓							
	41	✓							
	42	✓							
	43	✓							
	44	✓							
	45	✓							
	46	✓							
	47	✓							
	48	✓							
	49	✓							
	50	✓							
	51	✓							
	52	✓							
	53	✓							
	54	✓							
	55	✓							
	56	✓							
	57	✓							
	58	✓							
	59	✓							
	60	✓							
	61	✓							
	62	✓							
	63	✓							
	64	✓							
	65	✓							
	66	✓							
	67	✓							
	68								
	69								
	70								
	71								
	72								
	73								
	74								
	75								

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012							
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								
	101								
	102								
	103								
	104								
	105								
	106								

<b>Search Notes</b>  	<b>Application/Control No.</b>  13438754	<b>Applicant(s)/Patent Under Reexamination</b>  HULST ET AL.
	<b>Examiner</b>  THIEN M LE	<b>Art Unit</b>  2887

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
235	380, 382, 492, 451, 486, 487	12/20/2012	LTM

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
EAST, review parent applications for double patenting	12/20/2012	LTM

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

--	--

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> (Not for submission under 37 CFR 1.99)	<b>Application Number</b>		13/438,754	
	<b>Filing Date</b>		April 3, 2012	
	<b>First Named Inventor</b>		Hermen-ard Hulst	
	<b>Art Unit</b>		<del>2827</del> 2887	
	<b>Examiner Name</b>		T. Le	
	<b>Attorney Docket Number</b>		87790-837121 000160US	

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	4,590,365		05-1986	Okada	
	2.	5,682,027		10-1997	Bertina et al.	
	3.	6,025,973		02-2000	Mizoshita et al.	
	4.	6,981,179		12-2005	Shigemasa et al.	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup>	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>

EXAMINER SIGNATURE			
Examiner Signature	/Thien Le/		Date Considered 12/20/2012

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.




**UNITED STATES PATENT AND TRADEMARK OFFICE**

UNITED STATES DEPARTMENT OF COMMERCE  
**United States Patent and Trademark Office**  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

**BIB DATA SHEET**
**CONFIRMATION NO. 3525**

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/438,754	04/03/2012	235	2887	87790-837121 (000160US)		
<b>APPLICANTS</b> Hermen-ard Hulst, Amsterdam, NETHERLANDS; Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;						
<b>** CONTINUING DATA *****</b> This application is a CON of 13/212,047 08/17/2011 PAT 8,336,772 which is a CON of 12/943,872 11/10/2010 PAT 8,118,221 which is a CON of 12/014,558 01/15/2008 PAT 7,942,317 which is a CON of 11/336,758 01/19/2006 PAT 7,334,720 which is a CON of 10/111,716 09/17/2002 ABN which is a 371 of PCT/GB2000/104110 10/25/2000						
<b>** FOREIGN APPLICATIONS *****</b> UNITED KINGDOM 9925227.2 10/25/1999						
<b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **</b> 04/16/2012						
Foreign Priority claimed 35 USC 119(a-d) conditions met Verified and Acknowledged	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No /THIEN MINH LE/ Examiner's Signature	<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> NETHERLANDS	<b>SHEETS DRAWINGS</b> 17	<b>TOTAL CLAIMS</b> 28	<b>INDEPENDENT CLAIMS</b> 6
<b>ADDRESS</b> KILPATRICK TOWNSEND & STOCKTON LLP TWO EMBARCADERO CENTER EIGHTH FLOOR SAN FRANCISCO, CA 94111-3834 UNITED STATES						
<b>TITLE</b> Data Storage and Access Systems						
<b>FILING FEE RECEIVED</b> 1221	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit			

Substitute for form 1449/PTO  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)				<b>Complete if Known</b>	
				Application Number	13/438,754
				Filing Date	4/3/2012
				First Named Inventor	Racz, Patrick
				Art Unit	2887
				Examiner Name	T. Le
Sheet	1	of	3	Attorney Docket Number	87790-837121

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. <sup>1</sup>	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number Kind Code <sup>2 (if known)</sup>			
	AA	US 2003/0163594	8/28/2003	Aasheim et al.	
	AB	US 2003/0168515 A1	9/11/2003	Gray	
	AC	US 2006/0179211	8/10/2006	Aasheim et al.	
	AD	US 2006/0249570	11/9/2006	Seifert et al.	
	AE	US 2007/0162300	7/12/2007	Roever et al.	
	AF	US 2008/0041938	2/21/2008	Wise	
	AG	US 2008/0314974	12/25/2008	Hulst et al.	
	AH	US 4,341,951	Jul-82	Benton	
	AI	US 4,341,951	7/27/1982	Benton	
	AJ	US 4,697,073	9/29/1987	Hara	
	AK	US 5,148,432	9/15/1992	Gordon et al.	
	AL	US 5,226,145	7/6/1993	Moronaga et al.	
	AM	US 5,226,145	7/6/1993	Moronaga et al.	
	AN	US 5,367,150	11/22/1994	Kitta et al.	
	AO	US 5,406,619	4/11/1995	Akhteruzzaman et al.	
	AP	US 5,457,746	10/10/1995	Dolphin	
	AQ	US 5,532,466	7/2/1996	Konno et al.	
	AR	US 5,588,146	12/24/1996	Leroux	
	AS	US 5,677,953	10/14/1997	Dolphin	
	AT	US 5,703,951	12/30/1997	Dolphin	
	AU	US 5,740,369	4/14/1998	Yokozawa et al.	
	AV	US 5,744,787	4/28/1998	Teicher	
	AW	US 5,754,654	5/19/1998	Hiroya et al.	
	AX	US 5,794,202	8/11/1998	Kim	
	AY	US 5,809,241	9/15/1998	Hanel et al.	
	AZ	US 5,845,201	12/1/1998	Funke et al.	
	BA	US 5,845,281 A	12/1/1998	Benson et al.	
	BB	US 5,847,372	12/8/1998	Kreft	
	BC	US 5,874,760	2/23/1999	Burns et al.	
	BD	US 5,889,860	3/30/1999	Eller et al.	

Examiner Signature	/Thien Le/	Date Considered	12/20/2012
--------------------	------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

64087940 v1

Substitute for form 1449/PTO  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)				<b>Complete if Known</b>	
				Application Number	
				Filing Date	
				First Named Inventor	Racz, Patrick
				Art Unit	
				Examiner Name	
Sheet	2	of	3	Attorney Docket Number	87790-837121

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. <sup>1</sup>	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number Kind Code <sup>2 (if known)</sup>			
	BE	US 5,901,330	5/4/1999	Sun et al.	
	BF	US 5,918,213	6/29/1999	Bernard et al.	
	BG	US 5,923,884	7/13/1999	Peyret et al.	
	BH	US 5,933,498 A	8/3/1999	Schneck et al.	
	BI	US 5,936,220	8/10/1999	Hoshino et al.	
	BJ	US 6,012,634	1/11/2000	Brogan et al.	
	BK	US 6,018,720 A	1/25/2000	Fujimoto	Corresponds to JP 11-53184
	BL	US 6,078,917	6/20/2000	Paulsen et al.	
	BM	US 6,119,945	9/19/2000	Muller et al.	
	BN	US 6,142,369	Nov-00	Jonstromer	
	BO	US 6,202,056	3/13/2001	Nuttall	
	BP	US 6,385,731	5/7/2002	Ananda	
	BQ	US 6,415,156 B1	7/2/2002	Stadelmann	
	BR	US 6,424,975	7/23/2002	Walter et al.	
	BS	US 6,442,570	8/27/2002	Wu	
	BT	US 6,473,829	10/29/2002	Dahman et al.	
	BU	US 6,510,236	1/21/2003	Crane et al.	
	BV	US 6,553,413	4/22/2003	Leighton et al.	
	BW	US 6,554,192	4/29/2003	Tingl	
	BX	US 6,574,643	6/3/2003	Walter et al.	
	BY	US 6,658,568 B1	12/2/2003	Ginter et al.	
	BZ	US 6,721,749	4/13/2004	Najm et al.	
	CA	US 6,747,930 B1	6/8/2004	Weldon et al.	
	CB	US 6,993,507	1/31/2006	Meyer et al.	
	CC	US 6,999,936	2/14/2006	Sehr	
	CD	US 7,000,836 B2	2/21/2006	Saeki	
	CE	US 7,044,362	5/16/2006	Yu	
	CF	US 7,083,081	8/1/2006	McGee et al.	
	CG	US 7,334,720	2/26/2008	Hulst et al.	
	CH	US 7,677,446	3/16/2010	Wise	

Examiner Signature	/Thien Le/	Date Considered	12/20/2012
--------------------	------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)				<i>Complete if Known</i>			
				Application Number			
				Filing Date			
				First Named Inventor		Racz, Patrick	
				Art Unit			
				Examiner Name			
Sheet	3	of	3	Attorney Docket Number	87790-837121		

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No. <sup>1</sup>	Document Number		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number Kind Code <sup>2</sup> (if known)				
	CI	US 7,942,317		5/17/2011	Racz et al.	

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No. <sup>1</sup>	Foreign Patent Document			Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Country Code <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (if known)				
	CJ	EP	0 195 098		10-03-1990	FPDC, Inc.		<input type="checkbox"/>
	CK	EP	0 542 298		04-22-1998	Hitachi, Ltd.		<input type="checkbox"/>
	CL	EP	0 713 198	A2	05-22-1996	Nederland PTT		<input type="checkbox"/>
	CM	EP	0 823 694	A1	02-11-1998	Citibank NA		<input type="checkbox"/>
	CN	EP	0 843 449	A2	05-07-1998	Sunhawk Corp. Inc.		<input type="checkbox"/>
	CO	EP	0 914 001	A1	05-06-1999	Canal Plus SA		<input type="checkbox"/>
	CP	JP	10-269291	A	10-09-1998	Sony Corp.		<input type="checkbox"/>
	CQ	JP	11-212785	A	08-06-1999	Casio Comput. Co. Ltd.		<input type="checkbox"/>
	CR	JP	11-213010	A	08-06-1999	Planet Computer:KK		<input type="checkbox"/>
	CS	JP	11-272762	A	10-08-1999	Hitachi Ltd.		<input type="checkbox"/>
	CT	JP	11-53184	A	02-26-1999	Seta:KK	Corresponds to US 6,018,720	<input checked="" type="checkbox"/>
	CU	WO	98/19237	A1	05-07-1998	Schulumberger Technologies, Inc.		<input type="checkbox"/>
	CV	WO	98/33343		07-30-1998	Sonera OY et al.		<input type="checkbox"/>
	CW	WO	98/37526		08-27-1998	Mondex Int. Ltd.		<input type="checkbox"/>

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials *	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>62</sup>

Examiner Signature	/Thien Le/	Date Considered	12/20/2012
--------------------	------------	-----------------	------------

<sup>1</sup> EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>2</sup> Applicant's unique citation designation number (optional). <sup>3</sup> See Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>4</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>5</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>6</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>62</sup> Applicant is to place a check mark here if English language Translation is attached.

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/08 14:51
S2	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S3	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S4	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:13
S5	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25
S6	2	S1 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25
S7	0	S1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:33
S8	27343	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S9	1	S8 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S10	35059	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S11	3	S10 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S12	1	S9 and S11	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S13	0	code.clm. same present.clm.	US-PGPUB;	OR	OFF	2012/07/08

			USPAT; EPO; JPO; DERWENT			15:39
S14	3000	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S15	3	S14 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S16	1	S12 and S15	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S17	36126	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:41
S18	1	S16 and S17	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S19	13678	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S20	0	S19 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S21	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 05:52
S22	3	S21 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 05:52
S23	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 07:46
S24	2	S23 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S25	2	S23 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S26	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 09:13
S27	1	S26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S28	0	S27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S29	0	S27 and Mbyte.clm.	US-PGPUB;	OR	OFF	2012/07/09

			USPAT; EPO; JPO; DERWENT			09:13
S30	0	S26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S31	2178	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S32	39	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S33	61	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:35
S34	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:52
S35	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S36	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S37	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S38	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S39	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S40	2	S35 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S41	0	S35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S42	28666	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S43	1	S42 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25

S44	37012	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S45	3	S44 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S46	1	S43 and S45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S48	3161	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S49	3	S48 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S50	1	S46 and S49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S51	37531	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S52	1	S50 and S51	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S53	14209	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S54	0	S53 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S55	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S56	3	S55 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S57	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S58	2	S57 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S59	2	S57 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO;	OR	OFF	2012/10/22 14:25



			JPO; DERWENT			
S60	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S61	1	S60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S62	0	S61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S63	0	S61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S64	0	S60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S65	2322	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S66	40	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S67	69	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S68	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S69	542	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:39
S82	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 08:51
S83	1	S82 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 08:51
S84	3	((("8336772") or ("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 09:27
S85	1	S84 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:39
S86	3	S84 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S87	3	S84 and processor.clm.	US-PGPUB; USPAT; EPO;	OR	OFF	2012/12/20 09:40

			JPO; DERWENT			
S88	0	S84 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S89	1	S84 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S90	1	S85 and S89	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S91	1	S90 and S86 and S87	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S92	0	S84 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S93	3	S84 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:44
S94	1	S91 and S93	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:44
S95	1	S94 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S96	3	S84 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S97	3	S84 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S98	1	S95 and S95	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S99	1	S95 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S100	1	S95 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S101	0	S95 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52

S102	1	S95 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S103	1	S102 and S100	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S104	3	S84 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S105	0	S84 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S106	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 11:53
S107	0	S106 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 11:53
S108	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 15:00
S109	2	S108 and supplier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:01

## EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S70	29199	code.clm. same request.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S71	3300	code.clm. same payment.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S72	14468	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:35
S73	2284	memory same network same parameter\$1 same card	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S74	73	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S77	21580	(235/375,380,382,492,383,486,487).CCLS.	US-	OR	OFF	2012/10/22

			PGPUB; USPAT; UPAD			14:39
S78	212	S72 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S79	469	S70 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S80	404	S71 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S81	19	S74 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40

12/ 21/ 2012 7:40:48 AM

C:\Users\tle4\Documents\EAST\Workspaces\13438754.wsp



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 4 columns: APPLICATION NUMBER (13/438,754), FILING OR 371(C) DATE (04/03/2012), FIRST NAMED APPLICANT (Hermen-ard Hulst), ATTY. DOCKET NO./TITLE (87790-837121 (000160US))

CONFIRMATION NO. 3525

PUBLICATION NOTICE

20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834



Title:Data Storage and Access Systems

Publication No.US-2013-0046658-A1

Publication Date:02/21/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on March 21, 2013.

PATENT  
Attorney Docket No.: 87790-837121 (000160US)  
Client Ref. No. PN759544USG:

KILPATRICK TOWNSEND & STOCKTON LLP

By: /Sylvia E. Arnold/

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Hermen-ard Hulst et al.

Application No.: 13/438,754

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No.: 20350

Confirmation No.: 3525

Examiner: Thien Minh Le

Technology Center/Art Unit: 2887

AMENDMENT

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

In response to the Office Action mailed January 7, 2013, please enter the following amendments and remarks:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 10 of this paper.

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

Claims 1-39 (canceled)

1           40.   (Currently Amended) A handheld multimedia terminal, comprising:  
2           a wireless interface configured to interface with a wireless network for accessing  
3 a remote computer system;  
4           non-volatile memory configured to store multimedia content, wherein said  
5 multimedia content comprises one or more of music data, video data and computer game data;  
6           a program store storing processor control code;  
7           a processor coupled to said non-volatile memory, said program store, said  
8 wireless interface and  
9           a user interface to allow a user to select and play said multimedia content;  
10          a display for displaying one or both of said played multimedia content and data  
11 relating to said played multimedia content;  
12          wherein the processor control code comprises:  
13           code to request identifier data identifying one or more items of multimedia  
14 content stored in the non-volatile memory;  
15           code to receive said identifier data;  
16           code to present to a user on said display said identified one or more items  
17 of multimedia content available from the non-volatile memory;  
18           code to receive a user selection to select at least one of said one or more of  
19 said stored items of multimedia content;  
20           code responsive to said user selection of said at least one selected item of  
21 multimedia content to transmit payment data relating to payment for said at least one  
22 selected item of multimedia content via said wireless interface for validation by a  
23 payment validation system, wherein said payment data comprises user identification data  
24 identifying said user to said payment validation system;

25 code to receive payment validation data via said wireless interface  
26 defining if said payment validation system has validated payment for said at least one  
27 selected item of multimedia content; and  
28 code to control access to said at least one selected item of multimedia  
29 content on said terminal responsive to said payment validation data,  
30 wherein said user interface is operable to enable a user to select said at least one  
31 item of multimedia content available from said non-volatile memory; and  
32 wherein said user interface is operable to enable a user to access said at least one  
33 selected item of multimedia content responsive to said code to control access permitting access  
34 to said at least one selected item of multimedia content.

1 41. (Previously Presented) A content data supply server for providing an item  
2 of multimedia content to a handheld multimedia terminal, the content data supply server  
3 comprising:  
4 a communications interface for communicating with the handheld  
5 multimedia terminal;  
6 a program store storing code implementable by a processor;  
7 a data store for storing identifier data identifying one or more items of multimedia  
8 content available to the handheld multimedia terminal; and  
9 a processor coupled to the communications interface, to the program store  
10 and the data store, the code comprising:  
11 code to receive a request from the handheld multimedia terminal for the  
12 identifier data identifying the one or items multimedia content available to the handheld  
13 multimedia terminal;  
14 code to retrieve the identifier data from the data store;  
15 code to transmit the identifier data via the communications interface to the  
16 handheld multimedia terminal;  
17 code to receive payment validation data validating a user purchase of an  
18 item of the multimedia content; and



19 code responsive to the payment validation data validating the user purchase to  
20 retrieve the purchased item of multimedia content data from a multimedia content store and  
21 transmit the purchased item of multimedia content via the communications interface to the  
22 handheld multimedia terminal.

1 42. (Previously Presented) A content data supply server as claimed in claim  
2 41, further comprising code to receive payment record data indicating a payment made by a user  
3 for the item of multimedia content.

1 43. (Previously Presented) A content data supply server as claimed in claim  
2 42, further comprising code responsive to receiving the payment record data to request the  
3 payment validation data.

1 44. (Previously Presented) A content data supply server as claimed in claim  
2 43, wherein the code to request the payment validation data comprises code to transmit at least a  
3 portion of the payment record data.

1 45. (Previously Presented) A content data supply server as claimed in claim  
2 41, wherein the data supply server comprises the multimedia content store.

1 46. (Previously Presented) A content data supply server as claimed in claim  
2 41, further comprising:

3 code to receive a request from the handheld multimedia terminal for content  
4 information pertaining to at least one of the items of multimedia content identified by the  
5 identifier data, wherein the content information comprises one or more of description data and  
6 cost data;

7 code to retrieve the content information from the data store; and

8 code to transmit the content information to the handheld multimedia terminal.

1 47. (Previously Presented) A content data supply server as claimed in claim  
2 41, wherein the item of multimedia content comprises one or more of music, films, TV  
3 programs, text, software, or games software.

1           48.   (Previously Presented) A content data supply server as claimed in claim  
2 41, further comprising:  
3           code responsive to the payment validation data validating the user purchase to  
4 transmit at least one access rule to the handheld multimedia terminal,  
5           wherein the at least one access rule specifies at least one condition for accessing  
6 the retrieved and purchased item of multimedia content data.

1           49.   (Previously Presented) A content data supply server as claimed in claim  
2 48, wherein the data store or multimedia content store further stores the at least one access rule,  
3 and further comprising code to read the at least one access rule from the data store or multimedia  
4 content store.

1           50.   (Previously Presented) A method of providing an item of multimedia  
2 content to a handheld multimedia terminal, the method comprising:  
3           receiving a request from the handheld multimedia terminal for identifier  
4 data identifying one or more items of multimedia content data available to the handheld  
5 multimedia terminal;  
6           retrieving the identifier data from a data store;  
7           transmitting the identifier data to the handheld multimedia terminal;  
8           receiving payment validation data validating a user purchase of an item of  
9 multimedia content; and  
10           responsive to the payment validation data validating the user purchase,  
11 retrieving the purchased item of multimedia content data from a multimedia content store and  
12 transmitting the purchased item of multimedia content to the handheld multimedia terminal.

1           51.   (Previously Presented) A method as claimed in claim 50, further  
2 comprising receiving payment record data indicating a payment made by a user for the item of  
3 multimedia content.

1                   52.     (Previously Presented) A method as claimed in claim 51, further  
2 comprising requesting the payment validation data responsive to receiving the payment record  
3 data.

1                   53.     (Previously Presented) A method as claimed in claim 52, wherein the  
2 requesting the payment validation data comprises transmitting at least a portion of the payment  
3 record data.

1                   54.     (Previously Presented) A method as claimed in claim 50, further  
2 comprising:  
3                   receiving a request from the handheld multimedia terminal for content  
4 information pertaining to at least one of the items of multimedia content identified by the  
5 identifier data, wherein the content information comprises one or more of description data and  
6 cost data;  
7                   retrieving the content information from the data store; and  
8                   transmitting the content information to the handheld multimedia terminal.

1                   55.     (Previously Presented) A method as claimed in claim 50, further  
2 comprising:  
3                   responsive to the payment validation data validating the user purchase,  
4 transmitting at least one access rule to the handheld multimedia terminal,  
5                   wherein the at least one access rule specifies at least one condition for accessing  
6 the retrieved and purchased item of multimedia content data.

1                   56.     (Previously Presented) A method as claimed in claim 55, further  
2 comprising reading the at least one access rule from the data store or multimedia content store.

1                   57.     (Previously Presented) A computer system for providing multimedia data  
2 items to a handheld multimedia terminal, the system comprising:  
3                   a communications interface;

4                   a data store for storing records of multimedia data items available from the  
5 system, each record comprising a data item description and a pointer to a data provider for the  
6 data item;

7                   a program store storing code implementable by a processor;  
8                   a processor coupled to the communications interface, to the data store, and to the  
9 program store for implementing the stored code, the code comprising:

10                   code to receive a request for a multimedia data item from the handheld  
11 multimedia terminal;

12                   code to receive from the communications interface payment validation data  
13 comprising data confirming payment for the requested multimedia data item;

14                   code responsive to the request and to the received payment validation data, to read  
15 the requested multimedia data item from a content provider; and

16                   code to transmit the read multimedia data item to the handheld multimedia  
17 terminal over the communications interface.

1                   58.     (Previously Presented) A computer system as claimed in claim 57, further  
2 comprising code to receive payment record data indicating a payment made by a user for the  
3 item of multimedia content.

1                   59.     (Previously Presented) A computer system in claim 58, further  
2 comprising code responsive to the receiving the payment record data to request the payment  
3 validation data.

1                   60.   (Previously Presented) A computer system as claimed in claim 57, further  
2 comprising:  
3                   code responsive to the request and to the received payment validation data, to  
4 transmit at least one access rule to the handheld multimedia terminal,  
5                   wherein the at least one access rule specifies at least one condition for accessing  
6 the retrieved and purchased item of multimedia content data.

1                   61-63. (Canceled)

1                   64.   (Previously Presented) A method of downloading multimedia content  
2 from a content data supply server to a handheld multimedia terminal, the method comprising:  
3                   requesting, via a wireless interface on the handheld multimedia terminal,  
4 identifier data identifying one or more items of multimedia content available for retrieving,  
5                   receiving the identifier data via the wireless interface,  
6                   requesting content information via the wireless interface, wherein the content  
7 information comprises one or more of description data and cost data pertaining to at least one of  
8 the one or more items of multimedia content identified by the identifier data;  
9                   receiving the content information via said wireless interface;  
10                  presenting the content information pertaining to the identified one or more items  
11 of multimedia content available for retrieving to a user on a display of the handheld multimedia  
12 terminal;  
13                  receiving a user selection selecting at least one of the one or more items of  
14 multimedia content available for retrieving;  
15                  responsive to the user selection of the at least one item of multimedia  
16 content transmitting payment data relating to payment for the selected at least one item of  
17 multimedia content via the wireless interface for validation by a payment validation system;  
18                  receiving payment validation data via the wireless interface defining if the  
19 payment validation system has validated payment for the selected at least one item of multimedia  
20 content; and  
21                  responsive to the payment validation data retrieving the selected at least one item  
22 of multimedia content via the wireless interface from a content data supply server, writing the

23 retrieved at least one item of multimedia content into non-volatile memory on the handheld  
24 multimedia terminal.

1                   65.     (Previously Presented) A method as claimed in claim 64, further  
2 comprising:  
3                   retrieving at least one access rule from the content data supply server,  
4                   wherein the at least one access rule specifies at least one condition for accessing  
5 the retrieved and purchased item of multimedia content data.

1                   66.     (Previously Presented) A method as claimed in claim 64, wherein the  
2 non-volatile memory comprises flash memory.

1                   67.     (Previously Presented) A method as claimed in claim 64, wherein the  
2 multimedia content comprises one or more of music, films, TV programs, text, software, or  
3 games software.

1                   68.     (New) A handheld multimedia terminal as claimed in claim 40, further  
2 comprising code to retrieve supplementary data via said wireless interface and output said  
3 supplementary data to said user using said display.

1                   69.     (New) A handheld multimedia terminal as claimed in claim 68, wherein  
2 said supplementary data comprises advertising data.

1                   70.     (New) A handheld multimedia terminal as claimed in claim 69, wherein  
2 said processor further comprises code to display said advertising data when presenting said  
3 identified one or more items of multimedia content available from the non-volatile memory  
4 and/or accessing said at least one selected item of multimedia content.

### **REMARKS/ARGUMENTS**

This Amendment is in response to the Office Action mailed January 7, 2013. Before this Amendment, claims 40-67 were pending. Claims 40-67 are rejected. Claim 40 stands rejected under 35 U.S.C. § 101 for statutory type double patenting over claim 1 of U.S. Pat. 8,336,772. Claims 41-60 and 64-57 were rejected under 35 U.S.C. § 101 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims of U.S. Patent No. 8,336,772. Claims 61-62 were rejected under 35 U.S.C. § 102(b) as being anticipated by Bertina et al. (US 5,682,027) (hereinafter "Bertina"). Claims 61-63 were rejected under 35 U.S.C. § 102(e) as being anticipated by Gildea et al. (US 5,861,841) (hereinafter "Gildea").

In this Amendment, claims 61-63 have been cancelled. Claim 40 has been amended. Claims 68-70 are new and are supported by the specification, including paragraphs 28 and 137. After entry of this Amendment, which is respectfully requested, claims 41-60 and 64-70 will be pending. Support for all amended claims can be found in the specification, and no new matter has been added by these amendments. A terminal disclaimer with regard to U.S. Pat. 8,336,772 is concurrently filed with this response. Reconsideration of the remaining rejected claims is hereby requested.

#### **I. Statutory-Type Double Patenting Rejection**

The Office Action rejects claim 40 on the ground of statutory type double patenting as being unpatentable over claim 1 of U.S. Patent No. 8,336,772. Claim 40 has been amended and therefore Applicant submits that this rejection is moot.

#### **II. Nonstatutory Double Patenting Rejection**

The Office Action rejects claims 41-60 and 64-67 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over the claims of U.S. Patent No. 8,336,772. A terminal disclaimer is concurrently submitted with this response. It is Applicant's understanding that this will place claims 41-60 and 64-57 in condition for allowance.

#### **III. Rejections Under 35 U.S.C. § 102**

The Office Action rejected claims 61-62 under 35 U.S.C. 102(b) as being anticipated by Bertina (US 5,682,027) (hereinafter "Bertina"). Claims 61-62 have been cancelled and therefore Applicant submits that this rejection is moot.

Claims 61-63 were also rejected under 35 U.S.C. § 102(e) as being anticipated by Gildea. Claims 61-63 have been cancelled and therefore Applicant submits that this rejection is moot.

#### **IV. Amendment to the Claims**

New claims 68-70 depend from claim 40 and are supported by the specification. No new matter has been added. The claims recite limitations that are not disclosed by Bertina and Gildea for reasons including at least some of those set forth above, such that these claims should be allowable over the references. Applicant, therefore, respectfully submits that claims 68-70 are allowable and request consideration and allowance of the claim.

#### **V. Amendment to the Claims**

Unless otherwise specified or addressed in the remarks section, amendments to the claims are made for purposes of clarity, and are not intended to alter the scope of the claims or limit any equivalents thereof. The amendments are supported by the specification and do not add new matter. In addition, by focusing on specific claims and claim elements in the discussion above, Applicant does not imply that other claim elements are disclosed or suggested by the references. In addition, any characterizations of claims and/or cited art are being made to facilitate expeditious prosecution of this application. Applicant reserves the right to pursue at a later date any other broader or narrower claims that capture any subject matter supported by the present disclosure, including subject matter found to be specifically disclaimed herein or by another prosecution. Accordingly, reviewers of this or any child or related prosecution history shall not reasonably infer that Applicant has made any disclaimers or disavowals of any subject matter supported by the present disclosure.



**CONCLUSION**

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

Further, the Commissioner is hereby authorized to charge any additional fees or credit any overpayment in connection with this paper to Deposit Account No. 20-1430.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 925-472-5000.

Respectfully submitted,

/Ben Holt/

Benjamin J. Holt

Registration No. 67,536

KILPATRICK TOWNSEND & STOCKTON LLP

Two Embarcadero Center, Eighth Floor

San Francisco, California 94111-3834

Tel: 415 576 0200

Fax: 415 576 0300

BJH/sea

64860885V.1

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBTAIN A DOUBLE PATENTING  
REJECTION OVER A "PRIOR" PATENT**

Docket Number (Optional)  
87790-837121 (000160US)

In re Application of: Hermen-ard Hulst et al.

Application No. 13/438,754 Conf.: 3525

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS SYSTEMS

The owner\*, Smartflash Technologies Limited, of 100% percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 8,336,772 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney of record. Reg. No. 67,536

/Ben Holt/ 03/21/2013

---

Signature Date

Benjamin J. Holt

---

Typed or printed name

925-472-4741

---

Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).  
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754			
<b>Filing Date:</b>	03-Apr-2012			
<b>Title of Invention:</b>	Data Storage and Access Systems			
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst			
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold			
<b>Attorney Docket Number:</b>	87790-837121 (000160US)			
Filed as Large Entity				
<b>Utility under 35 USC 111(a) Filing Fees</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Statutory or Terminal Disclaimer	1814	1	160	160
<b>Total in USD (\$)</b>				<b>160</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	15325244
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	Data Storage and Access Systems
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	21-MAR-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	17:34:05
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$160
RAM confirmation Number	4505
Deposit Account	201430
Authorized User	KILPATRICK TOWNSEND & STOCKTON, LLP

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

<b>File Listing:</b>					
<b>Document Number</b>	<b>Document Description</b>	<b>File Name</b>	<b>File Size(Bytes)/ Message Digest</b>	<b>Multi Part /.zip</b>	<b>Pages (if appl.)</b>
1	Amendment/Req. Reconsideration-After Non-Final Reject	2013_03_21_AMEND_87790-837121-000160US.pdf	99844 c8238b7dd54791a2fd2aba92b619e7a6e9fbc9fa	no	12
<b>Warnings:</b>					
<b>Information:</b>					
2	Statutory disclaimers per MPEP 1490.	2013_03_21_TD_87790-837121-000160US.pdf	70661 585b787448182844d3591ccc0d0e68df62c9aaa5	no	1
<b>Warnings:</b>					
<b>Information:</b>					
3	Fee Worksheet (SB06)	fee-info.pdf	29867 40beef61df22e4128fa968b329061f5f573e1a65	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			200372		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>13/438,754</b>	Filing Date <b>04/03/2012</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		OR	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		OR	N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		OR	N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		OR	X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				OR		
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>					OR		
			TOTAL		OR	TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	<b>03/21/2013</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 28	Minus ** 28	= 0	X \$40 =	0	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 5	Minus *** 6	= 0	X \$210 =	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR		
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE	<b>0</b>	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR		
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	


\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /eugenia v. hardy/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

<b>Application Number</b> 	<b>Application/Control No.</b> 13/438,754	<b>Applicant(s)/Patent under Reexamination</b> HULST ET AL.	

<b>Document Code - DISQ</b>	<b>Internal Document – DO NOT MAIL</b>
-----------------------------	--

<b>TERMINAL DISCLAIMER</b>	<input checked="" type="checkbox"/> <b>APPROVED</b>	<input type="checkbox"/> <b>DISAPPROVED</b>
Date Filed : 03/21/13	<b>This patent is subject to a Terminal Disclaimer</b>	

<b>Approved/Disapproved by:</b>
---------------------------------

Angie Walker
--------------





NOTICE OF ALLOWANCE AND FEE(S) DUE

20350 7590 04/04/2013
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

Table with 2 columns: EXAMINER (LE, THIEN MINH), ART UNIT (2887), PAPER NUMBER (3525)

DATE MAILED: 04/04/2013

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies. If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above. If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)". For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

20350 7590 04/04/2013  
**KILPATRICK TOWNSEND & STOCKTON LLP**  
 TWO EMBARCADERO CENTER  
 EIGHTH FLOOR  
 SAN FRANCISCO, CA 94111-3834

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	04/03/2012	Hermen-ard Hulst	87790-837121 (000160US)	3525

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$890	\$300	\$0	\$1190	07/05/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, THIEN MINH	2887	235-380000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____</p> <p>3 _____</p>
---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

5. **Change in Entity Status** (from status indicated above)

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

---

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

---

Authorized Signature \_\_\_\_\_

Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_

Registration No. \_\_\_\_\_

---

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

---



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
13/438,754 04/03/2012 Hermen-ard Hulst 87790-837121 (000160US) 3525

20350 7590 04/04/2013
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

LE, THIEN MINH

ART UNIT PAPER NUMBER

2887

DATE MAILED: 04/04/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

## Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**Notice of Allowability**

**Application No.**

13/438,754

**Examiner**

Thien M. Le

**Applicant(s)**

HULST ET AL.

**Art Unit**

2887

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

- 1.  This communication is responsive to an amendment filed on 3/25/2013.
- 2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 3.  The allowed claim(s) is/are 40-60 and 64-70. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
- 4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All    b)  Some\*    c)  None    of the:
  - 1.  Certified copies of the priority documents have been received.
  - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - 3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

- 5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.

**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
- 6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- 1.  Notice of References Cited (PTO-892)
- 2.  Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
- 3.  Examiner's Comment Regarding Requirement for Deposit of Biological Material
- 4.  Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
- 5.  Examiner's Amendment/Comment
- 6.  Examiner's Statement of Reasons for Allowance
- 7.  Other \_\_\_\_\_.

### **DETAILED ACTION**

The Terminal Disclaimer filed on 3/25/2013 has been approved. Claims 1-39 and 61-63 have been canceled. Claims 40-60 and 64-70 are presented for examination.

### ***Allowable Subject Matter***

Claims 40-60 and 64-70 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to disclose a handheld multimedia terminal comprising: a wireless interface, a non-volatile memory, a program store, a processor, a user interface, a display, and having the processor control codes as recited in claims 40. Claim 41 recites a data supply server having similar limitations as recited in claim 40. The prior art also fails to disclose a computer system and a method of providing and downloading multimedia contents having limitations as recited in claims 50, 57 and 64.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thien M. Le whose telephone number is (571)272-2396. The examiner can normally be reached on Monday - Friday from 7:30am - 4:00pm.


Art Unit: 2887

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve S. Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thien M. Le/  
Primary Examiner, Art Unit 2887



<b>Index of Claims</b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013						
1	40	✓	=						
5	41	✓	=						
6	42	✓	=						
7	43	✓	=						
8	44	✓	=						
9	45	✓	=						
10	46	✓	=						
11	47	✓	=						
12	48	✓	=						
13	49	✓	=						
14	50	✓	=						
15	51	✓	=						
16	52	✓	=						
17	53	✓	=						
18	54	✓	=						
19	55	✓	=						
20	56	✓	=						
21	57	✓	=						
22	58	✓	=						
23	59	✓	=						
24	60	✓	=						
	61	✓	-						
	62	✓	-						
	63	✓	-						
25	64	✓	=						
26	65	✓	=						
27	66	✓	=						
28	67	✓	=						
2	68		=						
3	69		=						
4	70		=						
	71								
	72								
	73								
	74								
	75								

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013						
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								
	101								
	102								
	103								
	104								
	105								
	106								


<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

CPC		
Symbol	Type	Version


CPC Combination Sets				
Symbol	Type	Set	Ranking	Version

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION							
CLASS	SUBCLASS	CLAIMED				NON-CLAIMED			
235	380	G	0	6	K	5 / 00 (2006.01.01)			
<b>CROSS REFERENCE(S)</b>									
<b>CLASS</b>	<b>SUBCLASS (ONE SUBCLASS PER BLOCK)</b>								
235	382								

NONE		<b>Total Claims Allowed:</b>	
(Assistant Examiner)		28	
/THIEN M LE/ Primary Examiner. Art Unit 2887		04/01/2013	
(Primary Examiner)		O.G. Print Claim(s)	O.G. Print Figure
		1	5


<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.	
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887	


NONE		<b>Total Claims Allowed:</b>	
(Assistant Examiner)		28	
(Date)		<b>O.G. Print Claim(s)</b>	<b>O.G. Print Figure</b>
/THIEN M LE/ Primary Examiner. Art Unit 2887	04/01/2013	1	5
(Primary Examiner)	(Date)		

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant																<input type="checkbox"/> CPA		<input checked="" type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original						
1	40	20	56																		
5	41	21	57																		
6	42	22	58																		
7	43	23	59																		
8	44	24	60																		
9	45	25	64																		
10	46	26	65																		
11	47	27	66																		
12	48	28	67																		
13	49	2	68																		
14	50	3	69																		
15	51	4	70																		
16	52																				
17	53																				
18	54																				
19	55																				

NONE		<b>Total Claims Allowed:</b>	
		28	
(Assistant Examiner)	(Date)	O.G. Print Claim(s)	O.G. Print Figure
/THIEN M LE/ Primary Examiner. Art Unit 2887	04/01/2013	1	5
(Primary Examiner)	(Date)		

<b>Search Notes</b>  	<b>Application/Control No.</b>  13438754	<b>Applicant(s)/Patent Under Reexamination</b>  HULST ET AL.
	<b>Examiner</b>  THIEN M LE	<b>Art Unit</b>  2887

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	380, 382, 492, 451, 486, 487	12/20/2012	LTM
updated	same as above	4/1/2013	LTM

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, review parent applications for double patenting	12/20/2012	LTM
EAST	4/1/2013	LTM

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
235	380,382	4/1/2013	LTM

--	--

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L2	1	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L3	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L4	1	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L5	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L6	2	L1 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L7	0	L1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L8	30643	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L9	1	L8 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L10	40009	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L11	3	L10 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L12	1	L9 and L11	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L13	0	code.clm. same present.clm.	US-PGPUB;	OR	OFF	2013/04/01

			USPAT; EPO; JPO; DERWENT			09:39
L14	3421	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L15	3	L14 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L16	1	L12 and L15	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L17	39665	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L18	1	L16 and L17	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L19	15054	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L20	0	L19 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L21	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L22	3	L21 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L23	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L24	2	L23 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L25	2	L23 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L26	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L27	1	L26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L28	0	L27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L29	0	L27 and Mbyte.clm.	US-PGPUB;	OR	OFF	2013/04/01



			USPAT; EPO; JPO; DERWENT			09:39
L30	0	L26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L31	2561	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L32	48	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L33	78	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L34	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L35	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L36	1	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L37	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L38	1	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L39	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L40	2	L35 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L41	0	L35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L42	30643	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L43	1	L42 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L44	40009	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L45	3	L44 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L46	1	L43 and L45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L48	3421	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L49	3	L48 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L50	1	L46 and L49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L51	39665	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L52	1	L50 and L51	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L53	15054	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L54	0	L53 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L55	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L56	3	L55 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L57	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L58	2	L57 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L59	2	L57 and status.clm. and mobile.clm.	US-PGPUB; USPAT;	OR	OFF	2013/04/01 09:39

			EPO; JPO; DERWENT			
L60	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L61	1	L60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L62	0	L61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L63	0	L61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L64	0	L60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L65	2561	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L66	48	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L67	78	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L68	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L69	550	"l37" and "l42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L81	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L82	1	L81 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L83	4	((("8336772") or ("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L84	2	L83 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L85	4	L83 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L86	4	L83 and processor.clm.	US-PGPUB; USPAT;	OR	OFF	2013/04/01 09:39

			EPO; JPO; DERWENT			
L87	1	L83 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L88	2	L83 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L89	2	L84 and L88	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L90	2	L89 and L85 and L86	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L91	1	L83 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L92	4	L83 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L93	2	L90 and L92	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L94	2	L93 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L95	4	L83 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L96	4	L83 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L97	2	L94 and L94	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L98	2	L94 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L99	2	L94 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L100	1	L94 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L101	2	L94 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L102	2	L101 and L99	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L103	4	L83 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L104	1	L83 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L105	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L106	0	L105 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L107	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L108	2	L107 and supplier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L109	2	((("6688789") or ("20070176003")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L110	6162	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L111	17444	light adj4 control adj4 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L112	574	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L113	1	L110 and L112	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L114	304	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L115	0	L114 and L110	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L116	0	L114 and 235/462.\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L117	0	L114 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L118	8923	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L119	63	L118 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L120	453	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L121	2	L120 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L122	19	L120 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L123	1874	(light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L124	1973	(illumination or light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L125	40	L124 and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L126	949	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L127	949	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L128	61	L126 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L129	64	((light or illumination) adj40 decreas\$4 adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L130	7	L126 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L131	1042	pulse\$4 adj20 decreas\$4 adj20 zero	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/04/01 09:39

			DERWENT			
L132	9	L131 and flick\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L133	8	L131 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L134	102	(pulse\$4 adj20 decreas\$4 adj20 zero) and patient	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L135	1	L129 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L136	27	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L137	961	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L138	11	L137 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L139	191877	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L140	47	L137 and L139	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L141	4159	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L142	4577	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L143	283	L142 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L144	0	L143 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L145	12	((flicker\$4 near30 gradual\$4 near30 zero))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L146	2387	((light or illumination) near20 pulse\$1	US-PGPUB;	OR	OFF	2013/04/01

		near20 zero)	USPAT; EPO; JPO; DERWENT			09:39
L147	24	L146 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L148	3694	((light or illumination) near20 control near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L149	109	L148 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L150	4610	((light or illumination) near20 (width or control) near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L151	117	L150 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L152	1	L150 and "236"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L153	164	((light or illumination) near30 "off" near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L154	33	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L155	7603	(decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L156	9	L155 and (barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L157	482	light same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L158	496	(illumination or light) same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L159	109	L149 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L160	374	(illumination or light) same (decreas\$4 adj20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39



L161	14	L160 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L162	6332	((illumination or light) near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L163	86	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L164	4	L163 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L165	171	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L166	486192	l61and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L167	3	L165 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L168	482	((pulse\$1) near10 zero) same (scanner or reader)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L169	47	((pulse\$1) near10 zero) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L170	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L171	22	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L172	856	((light or illumination) adj20 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L173	717	((light or illumination) adj10 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L174	62	((light or illumination) adj10 (zero)) same strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L175	6	((light or illumination) adj10 (zero)) same strobe same power	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/04/01 09:39

			DERWENT			
L176	0	((zero near20 pulse\$4 near20 ("off")) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L177	1059	((zero near20 pulse\$4 near20 ("off")) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L178	53	((zero near20 pulse\$4 near20 ("off")) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L179	118	((zero near20 pulse\$4 near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L180	61	((zero near20 (light or illumination) near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L181	526	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L182	268	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L183	0	L182 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L184	39	L182 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L185	743	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L186	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L187	39	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L188	18	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L189	179	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L190	3	(pulse\$1 near20 (down or saving)	US-PGPUB;	OR	OFF	2013/04/01

		near20 (flick\$4 or flash)) and (scanner or barcode)	USPAT; EPO; JPO; DERWENT			09:39
L191	81	(pulse\$1 near20 (power) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L192	318	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L193	10	L192 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L194	12896	light near20 control\$4 near20 decrea\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L195	132	light near20 control\$4 near20 decrea\$4 near20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L196	818	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L197	4	L195 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L198	4331	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L199	13	L198 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L200	569	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L201	212	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L202	0	L201 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L203	30	L201 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L204	53	L112 and ((power or sleep) same zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L205	8155	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L206	8538	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L207	11	L206 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L208	1	("8302866").PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L209	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L210	2	L209 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L211	2	L209 and retrieving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L212	3	L209 and transmitting.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L213	3	L209 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L214	1012	(portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L215	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S1	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/08 14:51
S2	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S3	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S4	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:13
S5	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25

		same request.clm.				
S6	2	S1 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25
S7	0	S1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:33
S8	27343	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S9	1	S8 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S10	35059	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S11	3	S10 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S12	1	S9 and S11	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S13	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S14	3000	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S15	3	S14 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S16	1	S12 and S15	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S17	36126	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:41
S18	1	S16 and S17	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S19	13678	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S20	0	S19 and S1	US-PGPUB;	OR	OFF	2012/07/08

			USPAT; EPO; JPO; DERWENT			15:42
S21	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 05:52
S22	3	S21 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 05:52
S23	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 07:46
S24	2	S23 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S25	2	S23 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S26	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 09:13
S27	1	S26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S28	0	S27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S29	0	S27 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S30	0	S26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S31	2178	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S32	39	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S33	61	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:35
S34	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:52
S35	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S36	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/10/22 14:25

		validation.clm.	DERWENT			
S37	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S38	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S39	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S40	2	S35 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S41	0	S35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S42	28666	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S43	1	S42 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S44	37012	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S45	3	S44 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S46	1	S43 and S45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S48	3161	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S49	3	S48 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S50	1	S46 and S49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25

S51	37531	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S52	1	S50 and S51	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S53	14209	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S54	0	S53 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S55	3	(("8118221" or ("7942317" or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S56	3	S55 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S57	3	(("8118221" or ("7942317" or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S58	2	S57 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S59	2	S57 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S60	3	(("8118221" or ("7942317" or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S61	1	S60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S62	0	S61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S63	0	S61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S64	0	S60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S65	2322	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S66	40	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25



S67	69	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S68	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S69	542	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:39
S82	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 08:51
S83	1	S82 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 08:51
S84	3	((("8336772") or ("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 09:27
S85	1	S84 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:39
S86	3	S84 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S87	3	S84 and processor.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S88	0	S84 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S89	1	S84 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S90	1	S85 and S89	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S91	1	S90 and S86 and S87	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S92	0	S84 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S93	3	S84 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:44
S94	1	S91 and S93	US-PGPUB; USPAT;	OR	OFF	2012/12/20 09:44

			EPO; JPO; DERWENT			
S95	1	S94 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S96	3	S84 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S97	3	S84 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S98	1	S95 and S95	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S99	1	S95 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S100	1	S95 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S101	0	S95 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S102	1	S95 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S103	1	S102 and S100	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S104	3	S84 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S105	0	S84 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S106	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 11:53
S107	0	S106 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 11:53
S108	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 15:00
S109	2	S108 and supplier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:01

S110	2	((("6688789") or ("20070176003")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 15:30
S111	6083	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S112	17020	light adj4 control adj4 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S113	559	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S114	1	S111 and S113	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S115	301	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S116	0	S115 and S111	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S117	0	S115 and 235/462.\$ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S118	0	S115 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S119	8726	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S120	62	S119 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S121	441	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:37
S122	2	S121 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:37
S123	18	S121 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:38
S124	1836	(light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40

S125	1930	(illumination or light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40
S126	40	S125 and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40
S127	923	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:43
S128	923	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:43
S129	60	S127 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:44
S130	63	((light or illumination) adj40 decreas\$4 adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:44
S131	7	S127 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:47
S132	1029	pulse\$4 adj20 decreas\$4 adj20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:48
S133	9	S132 and flick\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:49
S134	8	S132 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:51
S135	99	(pulse\$4 adj20 decreas\$4 adj20 zero) and patient	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:53
S136	1	S130 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:57
S137	25	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:57
S138	945	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:58
S139	11	S138 and barcode\$1	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/12/20 15:58

			DERWENT			
S140	187291	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:00
S141	47	S138 and S140	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:00
S142	4072	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S143	4474	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S144	261	S143 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S145	0	S144 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S146	12	((flicker\$4 near30 gradual\$4 near30 zero))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:04
S147	2343	((light or illumination) near20 pulse\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:06
S148	24	S147 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:06
S149	3615	((light or illumination) near20 control near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:08
S150	109	S149 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:08
S151	4507	((light or illumination) near20 (width or control) near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S152	117	S151 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S153	1	S151 and "236"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S154	162	((light or illumination) near30 "off"	US-PGPUB;	OR	OFF	2012/12/20

		near30 zero near30 (pulse\$4)	USPAT; EPO; JPO; DERWENT			16:11
S155	31	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:12
S156	7416	(decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:43
S157	8	S156 and (barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:43
S158	472	light same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S159	483	(illumination or light) same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S160	109	S150 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S161	365	(illumination or light) same (decreas\$4 adj20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:45
S162	14	S161 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:46
S163	6180	((illumination or light) near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:48
S164	86	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:49
S165	4	S164 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:49
S166	168	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50
S167	474725	S166 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50
S168	3	S166 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50

S169	480	((pulse\$1) near10 zero) same (scanner or reader)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:51
S170	47	((pulse\$1) near10 zero) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:51
S171	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:55
S172	22	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:03
S173	842	((light or illumination) adj20 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S174	706	((light or illumination) adj10 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S175	61	((light or illumination) adj10 (zero)) same strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S176	5	((light or illumination) adj10 (zero)) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S177	0	((zero) near20 pulse\$4 near20 ("off")) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:07
S178	1039	((zero) near20 pulse\$4 near20 ("off")) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:08
S179	53	((zero) near20 pulse\$4 near20 ("off")) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:08
S180	116	((zero) near20 pulse\$4 near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:10
S181	59	((zero) near20 (light or illumination) near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:13
S182	511	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:14
S183	260	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/12/20 17:14

			DERWENT			
S184	0	S183 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:14
S185	37	S183 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:15
S186	716	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:16
S187	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:16
S188	39	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:17
S189	18	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:18
S190	177	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S191	3	(pulse\$1 near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S192	80	(pulse\$1 near20 (power) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S193	304	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:21
S194	10	S193 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:21
S195	12573	light near20 control\$4 near20 decrea\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S196	131	light near20 control\$4 near20 decrea\$4 near20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S197	790	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S198	4	S196 and (barcode\$1 or scanner)	US-PGPUB;	OR	OFF	2012/12/20



			USPAT; EPO; JPO; DERWENT			17:23
S199	4145	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:26
S200	13	S199 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:26
S201	551	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:28
S202	207	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S203	0	S202 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S204	30	S202 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S205	52	S113 and ((power or sleep) same zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:33
S206	7915	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S207	8295	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S208	11	S207 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S209	1	("8302866").PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 17:44
S210	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/21 06:10
S211	2	S210 and request.dlm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:11
S212	2	S210 and retrieving.dlm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:11
S213	3	S210 and transmitting.dlm.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/12/21 06:11

			DERWENT			
S214	3	S210 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:12
S215	913	((portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 07:44
S216	16	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 07:46

## EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L70	31139	code.clm. same request.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L71	3558	code.clm. same payment.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L72	15293	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L73	2521	memory same network same parameter\$1 same card	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L74	82	memory same storing same card same ((payment or transaction) near10 data) same instructions	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L76	22443	(235/375,380,382,492,383,486,487).CCLS.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L77	222	L72 and L76	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L78	499	L70 and L76	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L79	437	L71 and L76	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39

L80	19	L74 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L216	0	"L26" and portable.clm. and carrier.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
L217	783	"S113" and ((power or sleep) same zero)	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
L218	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
L219	787	(portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
L220	8880	(235/380,382).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
L221	92	l219 and l220	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
S70	29199	code.clm. same request.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S71	3300	code.clm. same payment.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S72	14468	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:35
S73	2284	memory same network same parameter\$1 same card	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S74	73	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S77	21580	(235/375,380,382,492,383,486,487).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:39
S78	212	S72 and S77	US-PGPUB; USPAT;	OR	OFF	2012/10/22 14:40

			UPAD			
S79	469	S70 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S80	404	S71 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S81	19	S74 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40

4/ 1/ 2013 10:27:06 AM

C:\Users\tle4\Documents\EAST\Workspaces\13438754.wsp


**UNITED STATES PATENT AND TRADEMARK OFFICE**

UNITED STATES DEPARTMENT OF COMMERCE  
**United States Patent and Trademark Office**  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

**BIB DATA SHEET**
**CONFIRMATION NO. 3525**

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/438,754	04/03/2012	235	2887	87790-837121 (000160US)		
<b>APPLICANTS</b>						
Hermen-ard Hulst, Amsterdam, NETHERLANDS; Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;						
<b>** CONTINUING DATA *****</b>						
This application is a CON of 13/212,047 08/17/2011 PAT 8336772 which is a CON of 12/943,872 11/10/2010 PAT 8118221 which is a CON of 12/014,558 01/15/2008 PAT 7942317 which is a CON of 11/336,758 01/19/2006 PAT 7334720 which is a CON of 10/111,716 09/17/2002 ABN which is a 371 of PCT/GB2000/104110 10/25/2000						
<b>** FOREIGN APPLICATIONS *****</b>						
UNITED KINGDOM 9925227.2 10/25/1999						
<b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **</b>						
04/16/2012						
Foreign Priority claimed 35 USC 119(a-d) conditions met Verified and Acknowledged	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No /THIEN MINH LE/ Examiner's Signature	<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> NETHERLANDS	<b>SHEETS DRAWINGS</b> 17	<b>TOTAL CLAIMS</b> 28	<b>INDEPENDENT CLAIMS</b> 6
<b>ADDRESS</b>						
KILPATRICK TOWNSEND & STOCKTON LLP TWO EMBARCADERO CENTER EIGHTH FLOOR SAN FRANCISCO, CA 94111-3834 UNITED STATES						
<b>TITLE</b>						
Data Storage and Access Systems						
<b>FILING FEE RECEIVED</b> 1221	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L2	1	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L3	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L4	1	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L5	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L6	2	L1 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L7	0	L1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L8	30643	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L9	1	L8 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L10	40009	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L11	3	L10 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L12	1	L9 and L11	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L13	0	code.clm. same present.clm.	US-PGPUB;	OR	OFF	2013/04/01

			USPAT; EPO; JPO; DERWENT			09:39
L14	3421	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L15	3	L14 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L16	1	L12 and L15	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L17	39665	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L18	1	L16 and L17	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L19	15054	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L20	0	L19 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L21	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L22	3	L21 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L23	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L24	2	L23 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L25	2	L23 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L26	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L27	1	L26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L28	0	L27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L29	0	L27 and Mbyte.clm.	US-PGPUB;	OR	OFF	2013/04/01

			USPAT; EPO; JPO; DERWENT			09:39
L30	0	L26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L31	2561	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L32	48	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L33	78	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L34	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L35	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L36	1	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L37	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L38	1	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L39	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L40	2	L35 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L41	0	L35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L42	30643	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L43	1	L42 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39



L44	40009	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L45	3	L44 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L46	1	L43 and L45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L48	3421	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L49	3	L48 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L50	1	L46 and L49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L51	39665	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L52	1	L50 and L51	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L53	15054	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L54	0	L53 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L55	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L56	3	L55 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L57	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L58	2	L57 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L59	2	L57 and status.clm. and mobile.clm.	US-PGPUB; USPAT;	OR	OFF	2013/04/01 09:39

			EPO; JPO; DERWENT			
L60	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L61	1	L60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L62	0	L61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L63	0	L61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L64	0	L60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L65	2561	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L66	48	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L67	78	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L68	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L69	550	"l37" and "l42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L81	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L82	1	L81 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L83	4	((("8336772") or ("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L84	2	L83 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L85	4	L83 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L86	4	L83 and processor.clm.	US-PGPUB; USPAT;	OR	OFF	2013/04/01 09:39

			EPO; JPO; DERWENT			
L87	1	L83 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L88	2	L83 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L89	2	L84 and L88	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L90	2	L89 and L85 and L86	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L91	1	L83 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L92	4	L83 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L93	2	L90 and L92	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L94	2	L93 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L95	4	L83 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L96	4	L83 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L97	2	L94 and L94	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L98	2	L94 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L99	2	L94 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L100	1	L94 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L101	2	L94 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L102	2	L101 and L99	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L103	4	L83 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L104	1	L83 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L105	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L106	0	L105 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L107	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L108	2	L107 and supplier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L109	2	((("6688789") or ("20070176003")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L110	6162	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L111	17444	light adj4 control adj4 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L112	574	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L113	1	L110 and L112	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L114	304	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L115	0	L114 and L110	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L116	0	L114 and 235/462.\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L117	0	L114 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L118	8923	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L119	63	L118 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L120	453	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L121	2	L120 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L122	19	L120 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L123	1874	(light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L124	1973	(illumination or light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L125	40	L124 and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L126	949	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L127	949	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L128	61	L126 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L129	64	((light or illumination) adj40 decreas\$4 adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L130	7	L126 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L131	1042	pulse\$4 adj20 decreas\$4 adj20 zero	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/04/01 09:39

			DERWENT			
L132	9	L131 and flick\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L133	8	L131 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L134	102	(pulse\$4 adj20 decreas\$4 adj20 zero) and patient	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L135	1	L129 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L136	27	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L137	961	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L138	11	L137 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L139	191877	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L140	47	L137 and L139	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L141	4159	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L142	4577	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L143	283	L142 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L144	0	L143 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L145	12	((flicker\$4 near30 gradual\$4 near30 zero))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L146	2387	((light or illumination) near20 pulse\$1	US-PGPUB;	OR	OFF	2013/04/01

		near20 zero)	USPAT; EPO; JPO; DERWENT			09:39
L147	24	L146 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L148	3694	((light or illumination) near20 control near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L149	109	L148 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L150	4610	((light or illumination) near20 (width or control) near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L151	117	L150 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L152	1	L150 and "236"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L153	164	((light or illumination) near30 "off" near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L154	33	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L155	7603	(decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L156	9	L155 and (barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L157	482	light same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L158	496	(illumination or light) same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L159	109	L149 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L160	374	(illumination or light) same (decreas\$4 adj20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L161	14	L160 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L162	6332	((illumination or light) near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L163	86	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L164	4	L163 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L165	171	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L166	486192	l61and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L167	3	L165 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L168	482	((pulse\$1) near10 zero) same (scanner or reader)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L169	47	((pulse\$1) near10 zero) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L170	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L171	22	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L172	856	((light or illumination) adj20 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L173	717	((light or illumination) adj10 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L174	62	((light or illumination) adj10 (zero)) same strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L175	6	((light or illumination) adj10 (zero)) same strobe same power	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/04/01 09:39



			DERWENT			
L176	0	((zero near20 pulse\$4 near20 ("off")) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L177	1059	((zero near20 pulse\$4 near20 ("off")) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L178	53	((zero near20 pulse\$4 near20 ("off")) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L179	118	((zero near20 pulse\$4 near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L180	61	((zero near20 (light or illumination) near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L181	526	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L182	268	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L183	0	L182 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L184	39	L182 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L185	743	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L186	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L187	39	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L188	18	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L189	179	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L190	3	(pulse\$1 near20 (down or saving)	US-PGPUB;	OR	OFF	2013/04/01

		near20 (flick\$4 or flash)) and (scanner or barcode)	USPAT; EPO; JPO; DERWENT			09:39
L191	81	(pulse\$1 near20 (power) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L192	318	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L193	10	L192 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L194	12896	light near20 control\$4 near20 decrea\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L195	132	light near20 control\$4 near20 decrea\$4 near20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L196	818	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L197	4	L195 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L198	4331	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L199	13	L198 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L200	569	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L201	212	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L202	0	L201 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L203	30	L201 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L204	53	L112 and ((power or sleep) same zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

L205	8155	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L206	8538	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L207	11	L206 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L208	1	("8302866").PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L209	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
L210	2	L209 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L211	2	L209 and retrieving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L212	3	L209 and transmitting.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L213	3	L209 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L214	1012	(portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
L215	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S1	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/08 14:51
S2	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S3	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S4	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:13
S5	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25

		same request.clm.				
S6	2	S1 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25
S7	0	S1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:33
S8	27343	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S9	1	S8 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S10	35059	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S11	3	S10 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S12	1	S9 and S11	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S13	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S14	3000	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S15	3	S14 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S16	1	S12 and S15	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S17	36126	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:41
S18	1	S16 and S17	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S19	13678	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S20	0	S19 and S1	US-PGPUB;	OR	OFF	2012/07/08

			USPAT; EPO; JPO; DERWENT			15:42
S21	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 05:52
S22	3	S21 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 05:52
S23	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 07:46
S24	2	S23 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S25	2	S23 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S26	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 09:13
S27	1	S26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S28	0	S27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S29	0	S27 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S30	0	S26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S31	2178	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S32	39	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S33	61	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:35
S34	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:52
S35	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S36	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/10/22 14:25

		validation.clm.	DERWENT			
S37	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S38	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S39	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S40	2	S35 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S41	0	S35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S42	28666	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S43	1	S42 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S44	37012	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S45	3	S44 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S46	1	S43 and S45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S48	3161	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S49	3	S48 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S50	1	S46 and S49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25

S51	37531	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S52	1	S50 and S51	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S53	14209	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S54	0	S53 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S55	3	(("8118221" or ("7942317" or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S56	3	S55 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S57	3	(("8118221" or ("7942317" or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S58	2	S57 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S59	2	S57 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S60	3	(("8118221" or ("7942317" or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S61	1	S60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S62	0	S61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S63	0	S61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S64	0	S60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S65	2322	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S66	40	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25

S67	69	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S68	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S69	542	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:39
S82	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 08:51
S83	1	S82 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 08:51
S84	3	((("8336772") or ("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 09:27
S85	1	S84 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:39
S86	3	S84 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S87	3	S84 and processor.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S88	0	S84 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S89	1	S84 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S90	1	S85 and S89	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S91	1	S90 and S86 and S87	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S92	0	S84 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S93	3	S84 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:44
S94	1	S91 and S93	US-PGPUB; USPAT;	OR	OFF	2012/12/20 09:44



			EPO; JPO; DERWENT			
S95	1	S94 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S96	3	S84 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S97	3	S84 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S98	1	S95 and S95	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S99	1	S95 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S100	1	S95 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S101	0	S95 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S102	1	S95 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S103	1	S102 and S100	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S104	3	S84 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S105	0	S84 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S106	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 11:53
S107	0	S106 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 11:53
S108	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 15:00
S109	2	S108 and supplier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:01

S110	2	((("6688789") or ("20070176003")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 15:30
S111	6083	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S112	17020	light adj4 control adj4 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S113	559	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S114	1	S111 and S113	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S115	301	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S116	0	S115 and S111	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S117	0	S115 and 235/462.\$ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S118	0	S115 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S119	8726	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S120	62	S119 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S121	441	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:37
S122	2	S121 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:37
S123	18	S121 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:38
S124	1836	(light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40

S125	1930	(illumination or light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40
S126	40	S125 and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40
S127	923	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:43
S128	923	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:43
S129	60	S127 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:44
S130	63	((light or illumination) adj40 decreas\$4 adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:44
S131	7	S127 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:47
S132	1029	pulse\$4 adj20 decreas\$4 adj20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:48
S133	9	S132 and flick\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:49
S134	8	S132 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:51
S135	99	(pulse\$4 adj20 decreas\$4 adj20 zero) and patient	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:53
S136	1	S130 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:57
S137	25	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:57
S138	945	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:58
S139	11	S138 and barcode\$1	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/12/20 15:58

			DERWENT			
S140	187291	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:00
S141	47	S138 and S140	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:00
S142	4072	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S143	4474	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S144	261	S143 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S145	0	S144 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S146	12	((flicker\$4 near30 gradual\$4 near30 zero))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:04
S147	2343	((light or illumination) near20 pulse\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:06
S148	24	S147 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:06
S149	3615	((light or illumination) near20 control near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:08
S150	109	S149 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:08
S151	4507	((light or illumination) near20 (width or control) near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S152	117	S151 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S153	1	S151 and "236"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S154	162	((light or illumination) near30 "off"	US-PGPUB;	OR	OFF	2012/12/20

		near30 zero near30 (pulse\$4)	USPAT; EPO; JPO; DERWENT			16:11
S155	31	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:12
S156	7416	(decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:43
S157	8	S156 and (barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:43
S158	472	light same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S159	483	(illumination or light) same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S160	109	S150 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S161	365	(illumination or light) same (decreas\$4 adj20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:45
S162	14	S161 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:46
S163	6180	((illumination or light) near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:48
S164	86	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:49
S165	4	S164 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:49
S166	168	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50
S167	474725	S166 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50
S168	3	S166 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50

S169	480	((pulse\$1) near10 zero) same (scanner or reader)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:51
S170	47	((pulse\$1) near10 zero) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:51
S171	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:55
S172	22	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:03
S173	842	((light or illumination) adj20 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S174	706	((light or illumination) adj10 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S175	61	((light or illumination) adj10 (zero)) same strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S176	5	((light or illumination) adj10 (zero)) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S177	0	((zero) near20 pulse\$4 near20 ("off")) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:07
S178	1039	((zero) near20 pulse\$4 near20 ("off")) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:08
S179	53	((zero) near20 pulse\$4 near20 ("off")) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:08
S180	116	((zero) near20 pulse\$4 near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:10
S181	59	((zero) near20 (light or illumination) near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:13
S182	511	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:14
S183	260	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/12/20 17:14

			DERWENT			
S184	0	S183 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:14
S185	37	S183 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:15
S186	716	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:16
S187	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:16
S188	39	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:17
S189	18	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:18
S190	177	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S191	3	(pulse\$1 near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S192	80	(pulse\$1 near20 (power) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S193	304	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:21
S194	10	S193 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:21
S195	12573	light near20 control\$4 near20 decrea\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S196	131	light near20 control\$4 near20 decrea\$4 near20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S197	790	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S198	4	S196 and (barcode\$1 or scanner)	US-PGPUB;	OR	OFF	2012/12/20

			USPAT; EPO; JPO; DERWENT			17:23
S199	4145	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:26
S200	13	S199 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:26
S201	551	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:28
S202	207	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S203	0	S202 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S204	30	S202 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S205	52	S113 and ((power or sleep) same zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:33
S206	7915	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S207	8295	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S208	11	S207 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S209	1	("8302866").PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 17:44
S210	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/21 06:10
S211	2	S210 and request.dlm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:11
S212	2	S210 and retrieving.dlm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:11
S213	3	S210 and transmitting.dlm.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/12/21 06:11



			DERWENT			
S214	3	S210 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:12
S215	913	((portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 07:44
S216	16	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 07:46

**EAST Search History (Interference)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L70	31139	code.clm. same request.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L71	3558	code.clm. same payment.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L72	15293	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L73	2521	memory same network same parameter\$1 same card	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L74	82	memory same storing same card same ((payment or transaction) near10 data) same instructions	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L76	22443	(235/375,380,382,492,383,486,487).CCLS.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L77	222	L72 and L76	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L78	499	L70 and L76	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L79	437	L71 and L76	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39

L80	19	L74 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
L216	0	"L26" and portable.clm. and carrier.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
L217	783	"S113" and ((power or sleep) same zero)	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
L218	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
L219	787	(portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
L220	8880	(235/380,382).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
L221	92	l219 and l220	US-PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
S70	29199	code.clm. same request.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S71	3300	code.clm. same payment.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S72	14468	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:35
S73	2284	memory same network same parameter\$1 same card	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S74	73	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S77	21580	(235/375,380,382,492,383,486,487).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:39
S78	212	S72 and S77	US-PGPUB; USPAT;	OR	OFF	2012/10/22 14:40

			UPAD			
S79	469	S70 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S80	404	S71 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S81	19	S74 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40

4/ 1/ 2013 10:28:02 AM

C:\Users\tle4\Documents\EAST\Workspaces\13438754.wsp

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on April 24, 2013.

PATENT  
Attorney Docket No.: 87790-837121 (000160US)  
Client Ref. No.: PN759544USG

KILPATRICK TOWNSEND & STOCKTON LLP

By: /Sylvia E. Arnold/

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Hermen-ard HULST, et al.

Application No.: 13/438,754

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No.: 20350

Confirmation No.: 3525

Examiner: Le, Thien Minh

Art Unit: 2887

PETITION TO CHANGE ORDER OF  
NAMES OF JOINT INVENTORS IN  
THE HEADING OF THE PATENT  
APPLICATION UNDER 37 CFR 1.48

Mail Stop Petition  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

Applicants respectfully request under 37 CFR 1.48 that the order of names of joint inventors in the above-captioned patent application be changed to reflect inventor Patrick Racz as the first-named inventor. Both inventors are listed on the most recent filing receipt and, based on the pending claims, should be listed as inventors in the present application. Only the order of the inventors should be changed. The corrected order of inventor names is listed below:

**Patrick S. Racz**, a citizen of the United Kingdom, residing at  
19 Royal Street  
Saint Heller, JE1 4WA Jersey

**Hermen-ard Hulst**, a citizen of Netherlands, residing at  
Van Tuyll van Serooskerweg 75hs  
Amsterdam, 1076 JG Netherlands

It is respectfully requested that this change be reflected on all subsequent correspondence from the United States Patent and Trademark Office directed to this application and that any patent issuing from this application, or a continuation thereof, names the inventors in the order listed above.

The Commissioner is hereby authorized to deduct the required fee of \$140 from the undersigned's Deposit Account No. 20-1430. Pleased deduct any additional fees from, or credit any overpayment to, the above-noted deposit account.

If it is believed that a telephone conference would be helpful, please telephone the undersigned at 925-472-4741.

Respectfully submitted,

/Ben Holt/

Benjamin J. Holt  
Reg. No. 67,536

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 925-472-5000  
Fax: 415-576-0300  
BJH/sea  
65346124V.1

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754
<b>Filing Date:</b>	03-Apr-2012
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Attorney Docket Number:</b>	87790-837121 (000160US)

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
Petition Fee-37CFR 1.17(h) (Group II)	2464	1	70	70

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

**Extension-of-Time:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>70</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	15606334
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	24-APR-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	19:27:38
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$70
RAM confirmation Number	6012
Deposit Account	201430
Authorized User	KILPATRICK TOWNSEND & STOCKTON, LLP

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)



**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition for review by the Office of Petitions.	2013_04_24_PET_CHANGE_IN V_87790-837121-000160US.pdf	111730  0c20a4fe23dc75226c2f5fa2eb6c860c042a bdf	no	2

**Warnings:****Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	30332  1cbe9798c29942b6c5595d5eb9141eccc48 34e88	no	2
---	----------------------	--------------	---	----	---

**Warnings:****Information:**

<b>Total Files Size (in bytes):</b>	142062
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on April 24, 2013.

PATENT  
Attorney Docket No.: 87790-837121 (000160US)  
Client Ref. No.: PN759544USG

KILPATRICK TOWNSEND & STOCKTON LLP

By: /Sylvia E. Arnold/

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Hermen-ard HULST, et al.

Application No.: 13/438,754

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No.: 20350

Confirmation No.: 3525

Examiner: Le, Thien Minh

Art Unit: 2887

PETITION TO CHANGE ORDER OF  
NAMES OF JOINT INVENTORS IN  
THE HEADING OF THE PATENT  
APPLICATION UNDER 37 CFR 1.48

Mail Stop Petition  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

Applicants respectfully request under 37 CFR 1.48 that the order of names of joint inventors in the above-captioned patent application be changed to reflect inventor Patrick Racz as the first-named inventor. Both inventors are listed on the most recent filing receipt and, based on the pending claims, should be listed as inventors in the present application. Only the order of the inventors should be changed. The corrected order of inventor names is listed below:

**Patrick S. Racz**, a citizen of the United Kingdom, residing at  
19 Royal Street  
Saint Heller, JE1 4WA Jersey

**Hermen-ard Hulst**, a citizen of Netherlands, residing at  
Van Tuyll van Serooskerweg 75hs  
Amsterdam, 1076 JG Netherlands

It is respectfully requested that this change be reflected on all subsequent correspondence from the United States Patent and Trademark Office directed to this application and that any patent issuing from this application, or a continuation thereof, names the inventors in the order listed above.

The Commissioner is hereby authorized to deduct the required fee of \$140 from the undersigned's Deposit Account No. 20-1430. Pleased deduct any additional fees from, or credit any overpayment to, the above-noted deposit account.

If it is believed that a telephone conference would be helpful, please telephone the undersigned at 925-472-4741.

Respectfully submitted,

/Ben Holt/

Benjamin J. Holt  
Reg. No. 67,536

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 925-472-5000  
Fax: 415-576-0300  
BJH/sea  
65346124V.1

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754
<b>Filing Date:</b>	03-Apr-2012
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Attorney Docket Number:</b>	87790-837121 (000160US)

Filed as Large Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
Petition fee- 37 CFR 1.17(h) (Group III)	1464	1	140	140

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

**Extension-of-Time:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>140</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	15606300
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Hermen-ard Hulst
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	24-APR-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	19:21:43
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition for review by the Office of Petitions.	2013_04_24_PET_CHANGE_IN V_87790-837121-000160US.pdf	111730 0c20a4fe23dc75226c2f5fa2eb6c860c042a bdff	no	2

### Warnings:

### Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30583 f64205b911c2243df1fa1590aafb5aa1d316 cbd1	no	2
---	----------------------	--------------	---	----	---

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	142313
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on April 24, 2013.

PATENT  
Attorney Docket No.: 87790-837121 (000160US)  
Client Ref. No.: PN759544USG

KILPATRICK TOWNSEND & STOCKTON LLP

By: /Sylvia E. Arnold/

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Hermen-ard HULST, et al.

Application No.: 13/438,754

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No.: 20350

Confirmation No.: 3525

Examiner: Le, Thien Minh

Art Unit: 2887

PETITION TO CHANGE ORDER OF  
NAMES OF JOINT INVENTORS IN  
THE HEADING OF THE PATENT  
APPLICATION UNDER 37 CFR 1.48

Mail Stop Petition  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

Applicants respectfully request under 37 CFR 1.48 that the order of names of joint inventors in the above-captioned patent application be changed to reflect inventor Patrick Racz as the first-named inventor. Both inventors are listed on the most recent filing receipt and, based on the pending claims, should be listed as inventors in the present application. Only the order of the inventors should be changed. The corrected order of inventor names is listed below:

05/13/2013 MTEKLEMI 00000003 13438754

01 FC:2053

70.00 OP

**Patrick S. Racz**, a citizen of the United Kingdom, residing at  
19 Royal Street  
Saint Heller, JE1 4WA Jersey

Adjustment date: 05/13/2013 MTEKLEMI  
04/25/2013 INTEFSW 00006012 13438754  
01 FC:2464 -70.00 OP





UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/438,754, 04/03/2012, 2887, 1291, 87790-837121 (000160US), 28, 6

CONFIRMATION NO. 3525

CORRECTED FILING RECEIPT

20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834



Date Mailed: 05/22/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Inventor(s)

Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;
Hermen-ard Hulst, Amsterdam, NETHERLANDS;

Applicant(s)

Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;
Hermen-ard Hulst, Amsterdam, NETHERLANDS;

Assignment For Published Patent Application

Smartflash Technologies Limited, Wickhams' Cay, VIRGIN ISLANDS, BRITISH

Power of Attorney: The patent practitioners associated with Customer Number 20350

Domestic Priority data as claimed by applicant

This application is a CON of 13/212,047 08/17/2011 PAT 8336772
which is a CON of 12/943,872 11/10/2010 PAT 8118221
which is a CON of 12/014,558 01/15/2008 PAT 7942317
which is a CON of 11/336,758 01/19/2006 PAT 7334720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB2000/104110 10/25/2000

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

UNITED KINGDOM 9925227.2 10/25/1999 No Access Code Provided

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to

**Retrieve Electronic Priority Application(s)** (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

**If Required, Foreign Filing License Granted:** 04/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/438,754**

**Projected Publication Date:** Not Applicable

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

DATA STORAGE AND ACCESS SYSTEMS

**Preliminary Class**

235

**Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:**

### **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
13/438,754 04/03/2012 Patrick Sandor Racz 87790-837121 (000160US) 3525

20350 7590 05/29/2013
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

LE, THIEN MINH

ART UNIT PAPER NUMBER

2887

NOTIFICATION DATE DELIVERY MODE

05/29/2013

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

- ipefiling@kilpatricktownsend.com
jlhice@kilpatrick.foundationip.com
mcollins@kilpatricktownsend.com

**Supplemental  
Notice of Allowability**

<b>Application No.</b> 13/438,754	<b>Applicant(s)</b> RACZ ET AL.	
<b>Examiner</b> Thien M. Le	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

- This communication is responsive to \_\_\_\_\_.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
- An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- The allowed claim(s) is/are 40-60 and 64-70. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/oph/index.jsp](http://www.uspto.gov/patents/init_events/oph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
- Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All    b)  Some    \*c)  None of the:
- Certified copies of the priority documents have been received.
  - Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

**Interim copies:**

- a)  All    b)  Some    c)  None of the: Interim copies of the priority documents have been received.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in **ABANDONMENT** of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

- CORRECTED DRAWINGS** ( as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.  
**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
- DEPOSIT OF and/or INFORMATION** about the deposit of **BIOLOGICAL MATERIAL** must be submitted. Note the attached Examiner's comment regarding **REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL**.

**Attachment(s)**

- |  |  |
|--|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                  |
| 2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date _____    | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material | 7. <input type="checkbox"/> Other _____.   |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____.                     |  |

--	--

### DETAILED ACTION

Claim 41, line 12 contains a minor typo which necessitates this examiner's amendment.

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Benjamin Holt on 5/21/2013.

The application has been amended as follows:

In the claims,

Claim 41, line 12, change "identifying the one or items multimedia content" to - - identifying the one or more multimedia content - -.

41. (Previously Presented) A content data supply server for providing an item of multimedia content to a handheld multimedia terminal, the content data supply server comprising:

a communications interface for communicating with the handheld multimedia terminal;

a program store storing code implementable by a processor;

a data store for storing identifier data identifying one or more items of multimedia content available to the handheld multimedia terminal; and

a processor coupled to the communications interface, to the program store and the data store, the code comprising:

code to receive a request from the handheld multimedia terminal for the identifier data identifying the one or more items multimedia content available to the handheld multimedia terminal;

code to retrieve the identifier data from the data store;

code to transmit the identifier data via the communications interface to the handheld multimedia terminal;

code to receive payment validation data validating a user purchase of an item of the multimedia content; and

code responsive to the payment validation data validating the user purchase to retrieve the purchased item of multimedia content data from a multimedia content store and transmit the purchased item of multimedia content via the communications interface to the handheld multimedia terminal.

***Allowable Subject Matter***

Claims 40-60 and 64-70 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to disclose a handheld multimedia terminal comprising: a wireless interface, a non-volatile memory, a program store, a processor, a user



Art Unit: 2887

interface, a display, and having the processor control codes as recited in claims 40.

Claim 41 recites a data supply server having similar limitations as recited in claim 40.

The prior art also fails to disclose a computer system and a method of providing and downloading multimedia contents having limitations as recited in claims 50, 57 and 64.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thien M. Le whose telephone number is (571)272-2396. The examiner can normally be reached on Monday - Friday from 7:30am - 4:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve S. Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 13/438,754  
Art Unit: 2887

Page 5

/Thien M. Le/  
Primary Examiner, Art Unit 2887


<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

CPC		
Symbol	Type	Version

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version


US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION														
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED									
235	380	G	0	6	K	5 / 00										
CROSS REFERENCE(S)																
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)															
235	382															

NONE		<b>Total Claims Allowed:</b>	
(Assistant Examiner)	(Date)	28	
/THIEN M LE/ Primary Examiner. Art Unit 2887	04/01/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant																<input type="checkbox"/> CPA		<input checked="" type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original						
1	40	20	56																		
5	41	21	57																		
6	42	22	58																		
7	43	23	59																		
8	44	24	60																		
9	45	25	64																		
10	46	26	65																		
11	47	27	66																		
12	48	28	67																		
13	49	2	68																		
14	50	3	69																		
15	51	4	70																		
16	52																				
17	53																				
18	54																				
19	55																				

NONE  (Assistant Examiner) _____ (Date) _____		<b>Total Claims Allowed:</b> 28	
/THIEN M LE/ Primary Examiner.Art Unit 2887  (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 1	O.G. Print Figure 5

<b>Index of Claims</b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013						
1	40	✓	=						
5	41	✓	=						
6	42	✓	=						
7	43	✓	=						
8	44	✓	=						
9	45	✓	=						
10	46	✓	=						
11	47	✓	=						
12	48	✓	=						
13	49	✓	=						
14	50	✓	=						
15	51	✓	=						
16	52	✓	=						
17	53	✓	=						
18	54	✓	=						
19	55	✓	=						
20	56	✓	=						
21	57	✓	=						
22	58	✓	=						
23	59	✓	=						
24	60	✓	=						
	61	✓	-						
	62	✓	-						
	63	✓	-						
25	64	✓	=						
26	65	✓	=						
27	66	✓	=						
28	67	✓	=						
2	68		=						
3	69		=						
4	70		=						
	71								
	72								
	73								
	74								
	75								

<b>Index of Claims</b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013						
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								
	101								
	102								
	103								
	104								
	105								
	106								

**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**  
**or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

20350                      7596                      04/04/2013  
**KILPATRICK TOWNSEND & STOCKTON LLP**  
**TWO EMBARCADERO CENTER**  
**EIGHTH FLOOR**  
**SAN FRANCISCO, CA 94111-3834**

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Sylvia E. Arnold	(Depositor's name)
/Sylvia E. Arnold/	(Signature)
July 1, 2013	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	04/03/2012	Hermen-ard Hulst	87790-837121 (000160US)	3525

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$890	\$300	\$0	\$1190	07/05/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, THIEN MINH	2887	235-380000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.</p> <p>1 <u>Kilpatrick Townsend and Stockton LLP</u></p> <p>2 _____</p> <p>3 _____</p>
---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: **SMARTFLASH LLC**

(B) RESIDENCE: (CITY and STATE OR COUNTRY) **TYLER, TEXAS USA**

Please check the appropriate assignee category or categories (will not be printed on the patent):  Individual  Corporation or other private group entity  Government

4a. The following fee(s) are submitted:

Issue Fee

Publication Fee (No small entity discount permitted)

Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

A check is enclosed.

Payment by credit card. Form PTO-2038 is attached.

The Director is hereby authorized to charge ~~#####~~ any deficiency, or credit any overpayment, to Deposit Account Number **20-1430** (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

---

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

---

Authorized Signature /Ben Holt/

Date July 1, 2013

Typed or printed name Benjamin J. Holt

Registration No. 67,536

---

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

---



## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754
<b>Filing Date:</b>	03-Apr-2012
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Attorney Docket Number:</b>	87790-837121 (000160US)

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
Utility Appl Issue Fee	2501	1	890	890
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>1190</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	16202752
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Sylvia Arnold
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	01-JUL-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	14:03:05
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1190
RAM confirmation Number	338
Deposit Account	201430
Authorized User	KILPATRICK TOWNSEND & STOCKTON, LLP

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	2013_07_01_ISSUE_FEE_87790-837121-000160US.pdf	2042152 7908597c3542d28132851474e51c7e50c0bb3e6	no	2

**Warnings:****Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	32172 3bbf90cb5b9f1ea7815a0b39fadbeae49b77d49b	no	2
---	----------------------	--------------	---	----	---

**Warnings:****Information:**

<b>Total Files Size (in bytes):</b>	2074324
-------------------------------------	---------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/438,754, 04/03/2012, 2887, 1591, 87790-837121 (000160US), 28, 6

CONFIRMATION NO. 3525

CORRECTED FILING RECEIPT



20350
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

Date Mailed: 07/12/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Inventor(s)

Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;
Hermen-ard Hulst, Amsterdam, NETHERLANDS;

Applicant(s)

Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;
Hermen-ard Hulst, Amsterdam, NETHERLANDS;

Assignment For Published Patent Application

Smartflash Technologies Limited, Wickhams' Cay, VIRGIN ISLANDS, BRITISH

Power of Attorney: The patent practitioners associated with Customer Number 20350

Domestic Priority data as claimed by applicant

This application is a CON of 13/212,047 08/17/2011 PAT 8336772
which is a CON of 12/943,872 11/10/2010 PAT 8118221
which is a CON of 12/014,558 01/15/2008 PAT 7942317
which is a CON of 11/336,758 01/19/2006 PAT 7334720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB2000/004110 10/25/2000

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

UNITED KINGDOM 9925227.2 10/25/1999 No Access Code Provided

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to

**Retrieve Electronic Priority Application(s)** (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

**If Required, Foreign Filing License Granted:** 04/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/438,754**

**Projected Publication Date:** Not Applicable

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

DATA STORAGE AND ACCESS SYSTEMS

**Preliminary Class**

235

**Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:**

### **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



**REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL  
(Submitted Only via EFS-Web)**

Application Number	13/438,754	Filing Date	2012-04-03	Docket Number (if applicable)	87790-837121 000160US	Art Unit	3525
First Named Inventor	Patrick Sandor Racz			Examiner Name	Le, Thien Minh		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application. Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

- Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
  - Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_
  - Other \_\_\_\_\_
- Enclosed
  - Amendment/Reply
  - Information Disclosure Statement (IDS)
  - Affidavit(s)/ Declaration(s)
  - Other \_\_\_\_\_

MISCELLANEOUS

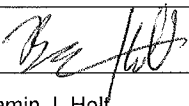
- Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months \_\_\_\_\_ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)
- Other \_\_\_\_\_

FEES

- The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
- The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 20-1430

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

- Patent Practitioner Signature
- Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature		Date (YYYY-MM-DD)	5/14/2013
Name	Benjamin J. Holt	Registration Number	67536

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on 8/19/13

PATENT  
Attorney Docket No.: 87790-837121-000160US

KILPATRICK TOWNSEND & STOCKTON LLP

By: Annette Valdivia

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of:

Patrick Sandor Racz

Application No.: 13/438,754

Filed: April 3, 2012

For: DATA STORAGE AND ACCESS  
SYSTEMS

Customer No.: 20350

Confirmation No.: 3525

Examiner: Thien Minh Le

Technology Center/Art Unit: 2887

INFORMATION DISCLOSURE

STATEMENT

Mail Stop IDS  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

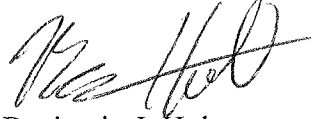
The references cited on attached form PTO/SB/08A are being called to the attention of the Examiner. Copies of the references are not enclosed.

It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that the IDS fee of \$180 is due for submission of this paper. If any additional fees are due for this submission, please deduct those fees from Deposit Account No. 20-1430.

Respectfully submitted,



Benjamin J. Holt  
Registration No. 67,536

KILPATRICK TOWNSEND & STOCKTON LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 415-576-0200  
Fax: 415-576-0300  
Attachments

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> (Not for submission under 37 CFR 1.99)	<b>Application Number</b>		13/438,754	
	<b>Filing Date</b>		April 3, 2012	
	<b>First Named Inventor</b>		Patrick Sandor Racz	
	<b>Art Unit</b>		2887	
	<b>Examiner Name</b>		Thien Minh Le	
	<b>Attorney Docket Number</b>		87790-000160US-837121	

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	6,473,794		10-29-2002	Guheen et al.	
	2.	6,476,306		11-5-2002	Huopaniemi et al.	
	3.	6,519,241		02-11-2003	Theimer	
	4.	6,552,254		04-22-2003	Hasegawa et al.	
	5.	7,043,456		05-9-2006	Lindskog et al.	
	6.	8,336,772		12-25-2012	Racz et al.	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup>	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>

EXAMINER SIGNATURE		
Examiner Signature		Date Considered
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.		
<sup>1</sup> See Kind Codes of USPTO Patent Documents at <a href="http://www.USPTO.GOV">www.USPTO.GOV</a> or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.		

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754
<b>Filing Date:</b>	03-Apr-2012
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Filer:</b>	Benjamin J. Holt/Annette Valdivia
<b>Attorney Docket Number:</b>	87790-837121 (000160US)

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
Petition Fee-37CFR 1.17(h) (Group II)	2464	1	70	70
Request for Continued Examination	2801	1	600	600

**Pages:**

**Claims:**

**Miscellaneous-Filing:**

**Petition:**

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>670</b>



## UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

Decision Date : August 19, 2013

In re Application of :

Patrick Racz

DECISION ON PETITION

UNDER CFR 1.313(c)(2)

Application No : 13438754

Filed : 03-Apr-2012

Attorney Docket No : 87790-837121 (000160US)

This is an electronic decision on the petition under 37 CFR 1.313(c)(2), filed August 19, 2013 , to withdraw the above-identified application from issue after payment of the issue fee.

The petition is **GRANTED**.

The above-identified application is withdrawn from issue for consideration of a submission under 37 CFR 1.114 (request for continued examination). See 37 CFR 1.313(c)(2).

**Petitioner is advised that the issue fee paid in this application cannot be refunded. If, however, this application is again allowed, petitioner may request that it be applied towards the issue fee required by the new Notice of Allowance.**

Telephone inquiries concerning this decision should be directed to the Patent Electronic Business Center (EBC) at 866-217-9197.

This application file is being referred to Technology Center AU 2887 for processing of the request for continuing examination under 37 CFR 1.114 .

Office of Petitions



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	16626311
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Annette Valdivia
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	19-AUG-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	18:31:08
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$670
RAM confirmation Number	4946
Deposit Account	201430
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip (if app)	Pages (if app)

1	Petition automatically granted by EFS	petition-request.pdf	31792 c2abe2965aead0ccf78500f0b288d381cfa1c64	no	2
<b>Warnings:</b>					
<b>Information:</b>					
2	Request for Continued Examination (RCE)	837121RCE.pdf	85634 814219c8c8c6d027f8af0b3bea9c7968acbaa33e	no	2
<b>Warnings:</b>					
This is not a USPTO supplied RCE SB30 form.					
<b>Information:</b>					
3		837121IDS.pdf	122790 0e501affc84ea462756cfb0335940c5fa431b3bc	yes	3
	<b>Multipart Description/PDF files in .zip description</b>				
	<b>Document Description</b>		<b>Start</b>	<b>End</b>	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	3	
<b>Warnings:</b>					
<b>Information:</b>					
4	Quick Path Information Disclosure Statement	837121QPIDS.pdf	80851 599769726cdf0965b0aa9dc68b9e18e02216ae85	no	1
<b>Warnings:</b>					
<b>Information:</b>					
5	Fee Worksheet (SB06)	fee-info.pdf	32418 7ef00e5d93b3debb178bd63b9c32b00525536b83	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			353485		

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

Electronic Petition Request	<b>PETITION TO WITHDRAW AN APPLICATION FROM ISSUE AFTER PAYMENT OF THE ISSUE FEE UNDER 37 CFR 1.313(c)</b>
Application Number	13438754
Filing Date	03-Apr-2012
First Named Inventor	Patrick Racz
Art Unit	2887
Examiner Name	THIEN LE
Attorney Docket Number	87790-837121 (000160US)
Title	DATA STORAGE AND ACCESS SYSTEMS

An application may be withdrawn from issue for further action upon petition by the applicant. To request that the Office withdraw an application from issue, applicant must file a petition under this section including the fee set forth in § 1.17(h) and a showing of good and sufficient reasons why withdrawal of the application from issue is necessary.

APPLICANT HEREBY PETITIONS TO WITHDRAW THIS APPLICATION FROM ISSUE UNDER 37 CFR 1.313(c).

A grantable petition requires the following items:

- (1) Petition fee; and
- (2) One of the following reasons:
  - (a) Unpatentability of one or more claims, which must be accompanied by an unequivocal statement that one or more claims are unpatentable, an amendment to such claim or claims, and an explanation as to how the amendment causes such claim or claims to be patentable;
  - (b) Consideration of a request for continued examination in compliance with § 1.114 (for a utility or plant application only); or
  - (c) Express abandonment of the application. Such express abandonment may be in favor of a continuing application, but not a CPA under 37 CFR 1.53(d).

**Petition Fee**

- Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).
- Applicant(s) status remains as SMALL ENTITY.
- Applicant(s) status remains as other than SMALL ENTITY

Reason for withdrawal from issue

- One or more claims are unpatentable
- Consideration of a request for continued examination (RCE) (List of Required Documents and Fees)
- Applicant hereby expressly abandons the instant application (any attorney/agent signing for this reason must have power of attorney pursuant to 37 CFR 1.32(b)).

RCE request, submission, and fee.

- I certify, in accordance with 37 CFR 1.4(d)(4) that:
- The RCE request, submission, and fee have already been filed in the above-identified application on
  - Are attached.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

- An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application.
- An attorney or agent registered to practice before the Patent and Trademark Office, acting in a representative capacity.
- A sole inventor
- A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors
- A joint inventor; all of whom are signing this e-petition
- The assignee of record of the entire interest that has properly made itself of record pursuant to 37 CFR 3.71

Signature	/Benjamin J. Holt/
Name	Benjamin J. Holt
Registration Number	67536



NOTICE OF ALLOWANCE AND FEE(S) DUE

20350 7590 09/17/2013
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

Table with 2 columns: EXAMINER (LE, THIEN MINH), ART UNIT (2887), PAPER NUMBER

DATE MAILED: 09/17/2013

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

20350                      7590                      09/17/2013  
**KILPATRICK TOWNSEND & STOCKTON LLP**  
 TWO EMBARCADERO CENTER  
 EIGHTH FLOOR  
 SAN FRANCISCO, CA 94111-3834

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	04/03/2012	Patrick Sandor Racz	87790-837121 (000160US)	3525

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$0	\$0	\$890	\$0	12/17/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, THIEN MINH	2887	235-380000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
---	---

**3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)**

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (<b>Please first reapply any previously paid issue fee shown above</b>)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	---

5. **Change in Entity Status** (from status indicated above)

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

---

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

---

Authorized Signature \_\_\_\_\_

Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_

Registration No. \_\_\_\_\_

---

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

---





UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
13/438,754 04/03/2012 Patrick Sandor Racz 87790-837121 (000160US) 3525

20350 7590 09/17/2013
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

Table with 2 columns: EXAMINER, ART UNIT, PAPER NUMBER
EXAMINER: LE, THIEN MINH
ART UNIT: 2887
PAPER NUMBER: (empty)

DATE MAILED: 09/17/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

## Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<b>Notice of Allowability</b>	<b>Application No.</b> 13/438,754	<b>Applicant(s)</b> RACZ ET AL.	
	<b>Examiner</b> Thien M. Le	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to a request for RCE filed on 8/19/2013.  
 A declaration(s)/affidavit(s) under 37 CFR 1.130(b) was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 40-60 and 64-70. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/oph/index.jsp](http://www.uspto.gov/patents/init_events/oph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All    b)  Some    \*c)  None of the:
1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.  
**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |  |
|--|--|
| <ol style="list-style-type: none"> <li>1. <input type="checkbox"/> Notice of References Cited (PTO-892)</li> <li>2. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br/>Paper No./Mail Date <u>8/19/2013</u></li> <li>3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material</li> <li>4. <input type="checkbox"/> Interview Summary (PTO-413),<br/>Paper No./Mail Date _____.</li> </ol> | <ol style="list-style-type: none"> <li>5. <input type="checkbox"/> Examiner's Amendment/Comment</li> <li>6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance</li> <li>7. <input type="checkbox"/> Other _____.</li> </ol> |
|--|--|

### **DETAILED ACTION**

The present application is being examined under the pre-AIA first to invent provisions. The information disclosure statement filed on 8/19/2013 has been entered.

### **Request To Change Inventorship**

This is a decision on the request to change inventorship under 37 C.F.R 1.48 filed on 4/24/2013.

The request is **GRANTED**.

Accordingly, the correct inventorship of the instant application should be listed as follows:

**Patrick S. Racz**, a citizen of the United Kingdom, residing at 19 Royal Street Saint Heller, JE 1 4WA Jersey;

**Hermen-ard Hulst**, a citizen of Netherlands, residing at Van Tuyll van Serooskerweg 75hs Amsterdam, 1076 JG Netherlands.

### ***Allowable Subject Matter***

Claims 40-60 and 64-70 are allowed.

Art Unit: 2887

The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to disclose a handheld multimedia terminal comprising: a wireless interface, a non-volatile memory, a program store, a processor, a user interface, a display, and having the processor control codes as recited in claims 40. Claim 41 recites a data supply server having similar limitations as recited in claim 40. The prior art also fails to disclose a computer system and a method of providing and downloading multimedia contents having limitations as recited in claims 50, 57 and 64.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thien M. Le whose telephone number is (571)272-2396. The examiner can normally be reached on Monday - Friday from 7:30am - 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve S. Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2887

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


/Thien M. Le/  
Primary Examiner, Art Unit 2887


**UNITED STATES PATENT AND TRADEMARK OFFICE**

 UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

**BIB DATA SHEET**
**CONFIRMATION NO. 3525**

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/438,754	04/03/2012	235	2887	87790-837121 (000160US)		
<b>APPLICANTS</b> Patrick Sandor Racz, Saint Heller, UNITED KINGDOM; Hermen-ard Hulst, Amsterdam, NETHERLANDS;						
<b>** CONTINUING DATA *****</b> This application is a CON of 13/212,047 08/17/2011 PAT 8336772 which is a CON of 12/943,872 11/10/2010 PAT 8118221 which is a CON of 12/014,558 01/15/2008 PAT 7942317 which is a CON of 11/336,758 01/19/2006 PAT 7334720 which is a CON of 10/111,716 09/17/2002 ABN which is a 371 of PCT/GB2000/004110 10/25/2000						
<b>** FOREIGN APPLICATIONS *****</b> UNITED KINGDOM 9925227.2 10/25/1999						
<b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **</b> 04/16/2012						
Foreign Priority claimed <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> UNITED KINGDOM	<b>SHEETS DRAWINGS</b> 17	<b>TOTAL CLAIMS</b> 28	<b>INDEPENDENT CLAIMS</b> 6
<b>ADDRESS</b> KILPATRICK TOWNSEND & STOCKTON LLP TWO EMBARCADERO CENTER EIGHTH FLOOR SAN FRANCISCO, CA 94111-3834 UNITED STATES						
<b>TITLE</b> DATA STORAGE AND ACCESS SYSTEMS						
<b>FILING FEE RECEIVED</b> 1591	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

<b>Search Notes</b>  	<b>Application/Control No.</b>  13438754	<b>Applicant(s)/Patent Under Reexamination</b>  HULST ET AL.
	<b>Examiner</b>  THIEN M LE	<b>Art Unit</b>  2887

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner


US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	380, 382, 492, 451, 486, 487	12/20/2012	LTM
updated	same as above	4/1/2013	LTM
updated	same as above	9/4/2013	LTM

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, review parent applications for double patenting	12/20/2012	LTM
EAST	4/1/2013	LTM
EAST	9/4/2013	LTM

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
235	380,382	4/1/2013	LTM
updated	same as above	9/4/2013	LTM

--	--



<b>Index of Claims</b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013	09/04/2013					
1	40	✓	=	=					
5	41	✓	=	=					
6	42	✓	=	=					
7	43	✓	=	=					
8	44	✓	=	=					
9	45	✓	=	=					
10	46	✓	=	=					
11	47	✓	=	=					
12	48	✓	=	=					
13	49	✓	=	=					
14	50	✓	=	=					
15	51	✓	=	=					
16	52	✓	=	=					
17	53	✓	=	=					
18	54	✓	=	=					
19	55	✓	=	=					
20	56	✓	=	=					
21	57	✓	=	=					
22	58	✓	=	=					
23	59	✓	=	=					
24	60	✓	=	=					
	61	✓	-	-					
	62	✓	-	-					
	63	✓	-	-					
25	64	✓	=	=					
26	65	✓	=	=					
27	66	✓	=	=					
28	67	✓	=	=					
2	68		=	=					
3	69		=	=					
4	70		=	=					
	71								
	72								
	73								
	74								
	75								

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47


CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013	09/04/2013					
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								
	101								
	102								
	103								
	104								
	105								
	106								

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

CPC			Type	Version
Symbol				


CPC Combination Sets				
Symbol	Type	Set	Ranking	Version

NONE		<b>Total Claims Allowed:</b>	
(Assistant Examiner)	(Date)	28	
/THIEN M LE/ Primary Examiner.Art Unit 2887	09/04/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

US ORIGINAL CLASSIFICATION					INTERNATIONAL CLASSIFICATION								
CLASS		SUBCLASS			CLAIMED				NON-CLAIMED				
235		380			G	0	6	K	5 / 00 (2006.01.01)				
<b>CROSS REFERENCE(S)</b>													
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)												
235	382												

NONE		<b>Total Claims Allowed:</b>	
(Assistant Examiner)		28	
/THIEN M LE/ Primary Examiner.Art Unit 2887		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)		1	5
		(Date)	(Date)
		09/04/2013	

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant																<input type="checkbox"/> CPA		<input checked="" type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original						
1	40	20	56																		
5	41	21	57																		
6	42	22	58																		
7	43	23	59																		
8	44	24	60																		
9	45	25	64																		
10	46	26	65																		
11	47	27	66																		
12	48	28	67																		
13	49	2	68																		
14	50	3	69																		
15	51	4	70																		
16	52																				
17	53																				
18	54																				
19	55																				

NONE		<b>Total Claims Allowed:</b>	
		28	
(Assistant Examiner)	(Date)	O.G. Print Claim(s)	O.G. Print Figure
/THIEN M LE/ Primary Examiner.Art Unit 2887	09/04/2013	1	5
(Primary Examiner)	(Date)		

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> (Not for submission under 37 CFR 1.99)	<b>Application Number</b>		13/438,754	
	<b>Filing Date</b>		April 3, 2012	
	<b>First Named Inventor</b>		Patrick Sandor Racz	
	<b>Art Unit</b>		2887	
	<b>Examiner Name</b>		Thien Minh Le	
	<b>Attorney Docket Number</b>		87790-000160US-837121	

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	6,473,794		10-29-2002	Guheen et al.	
	2.	6,476,306		11-5-2002	Huopaniemi et al.	
	3.	6,519,241		02-11-2003	Theimer	
	4.	6,552,254		04-22-2003	Hasegawa et al.	
	5.	7,043,456		05-9-2006	Lindskog et al.	
	6.	8,336,772		12-25-2012	Racz et al.	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup>	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>

EXAMINER SIGNATURE			
Examiner Signature	/Thien Le/	Date Considered	09/04/2013

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L5	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L7	0	L1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L8	32660	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L9	1	L8 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L10	43143	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L11	3	L10 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L13	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L14	3684	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L15	3	L14 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L17	41860	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L18	1	L16 and L17	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54

L19	15904	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L20	0	L19 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L23	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/09/04 13:54
L27	1	L26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L28	0	L27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L29	0	L27 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L30	0	L26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L31	2763	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L37	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L39	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L41	0	L35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L42	32660	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L43	1	L42 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L44	43143	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L45	3	L44 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54



L47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L48	3684	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L49	3	L48 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L51	41860	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L52	1	L50 and L51	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L53	15904	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L54	0	L53 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L57	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/09/04 13:54
L61	1	L60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L62	0	L61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L63	0	L61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L64	0	L60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L65	2763	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L69	570	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L81	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/09/04 13:54
L84	2	L83 and memory.clm.	US-PGPUB; USPAT;	OR	OFF	2013/09/04 13:54

			EPO; JPO; DERWENT			
L85	4	L83 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L86	4	L83 and processor.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L87	1	L83 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L88	2	L83 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L89	2	L84 and L88	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L90	2	L89 and L85 and L86	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L91	1	L83 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L92	4	L83 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L93	2	L90 and L92	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L94	2	L93 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L95	4	L83 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L96	4	L83 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L97	2	L94 and L94	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L98	2	L94 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54

L99	2	L94 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L100	1	L94 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L101	2	L94 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L103	4	L83 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L104	1	L83 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L105	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/09/04 13:54
L106	0	L105 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L107	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/09/04 13:54
L110	6336	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L111	18113	light adj4 control adj4 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L112	591	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L114	314	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L115	0	L114 and L110	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L116	0	L114 and 235/462.\$ .ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L117	0	L114 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L118	9206	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT;	OR	OFF	2013/09/04 13:54

			EPO; JPO; DERWENT			
L120	468	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L123	1927	(light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L124	2029	(illumination or light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L127	980	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L131	1059	pulse\$4 adj20 decreas\$4 adj20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L136	30	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L137	993	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L139	199591	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L141	4280	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L142	4714	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L143	314	L142 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L144	1	L143 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L146	2451	((light or illumination) near20 pulse\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L148	3832	((light or illumination) near20 control near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54

L150	4787	((light or illumination) near20 (width or control) near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L155	7914	(decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L157	498	light same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L158	512	((illumination or light) same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L160	385	((illumination or light) same (decreas\$4 adj20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L162	6545	((illumination or light) near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L165	176	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L166	505362	l61and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L168	492	((pulse\$1) near10 zero) same (scanner or reader)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L172	878	((light or illumination) adj20 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L173	735	((light or illumination) adj10 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L174	65	((light or illumination) adj10 (zero)) same strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L176	0	((zero) near20 pulse\$4 near20 ("off")) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L177	1093	((zero) near20 pulse\$4 near20 ("off")) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L181	554	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/09/04 13:54

			DERWENT			
L182	285	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L183	0	L182 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L185	774	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L189	185	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L190	3	(pulse\$1 near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L192	329	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L194	13435	light near20 control\$4 near20 decrea\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L195	135	light near20 control\$4 near20 decrea\$4 near20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L196	867	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L198	4671	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L200	598	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L201	218	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L202	0	L201 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L205	8553	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L206	8942	pulse\$1 near10 width\$1 near10	US-PGPUB;	OR	OFF	2013/09/04

		(dimming or decreasing or reducing)	USPAT; EPO; JPO; DERWENT			13:54
L209	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/09/04 13:54
L210	2	L209 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L211	2	L209 and retrieving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L212	3	L209 and transmitting.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L213	3	L209 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L218	0	L216 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L220	0	L216 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L222	0	L216 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L223	32660	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L224	1	L223 and L216	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L225	43143	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L226	3	L225 and L216	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54
L228	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/04 13:54

## EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
-------	------	--------------	-----	------------------	---------	------------

L70	33127	code.clm. same request.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L71	3817	code.clm. same payment.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L72	16137	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L73	2720	memory same network same parameter\$1 same card	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L74	94	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L76	23282	(235/375,380,382,492,383,486,487).OCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L77	234	L72 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L78	526	L70 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L79	463	L71 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54
L80	19	L74 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2013/09/04 13:54

9/ 4/ 2013 2:05:23 PM

C:\Users\tle4\Documents\EAST\Workspaces\13438754.wsp



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO**

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

 Practitioners associated with the Customer Number:

42624

OR

 Practitioner(s) named below (If more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

 The address associated with Customer Number:

42624

OR

<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		


Assignee Name and Address:

Smartflash LLC  
100 E. Ferguson, First Place, Suite 406  
Tyler, Texas 75702

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

**SIGNATURE of Assignee of Record**

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	 Leon Unterhalter for LU Management	Date	October 16, 2013
Name	Services Inc, as Manager of Smartflash LLC.	Telephone	561 315 3153
Title	President		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**STATEMENT UNDER 37 CFR 3.73(b)**

Applicant/Patent Owner: Patrick Sandor Racz

Application No./Patent No.: 13/438,754 Filed/Issue Date: 04/03/2012

Titled: Data Storage and Access Systems

SMARTFLASH, LLC, a Corporation  
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

- 1.  the assignee of the entire right, title, and interest in;
- 2.  an assignee of less than the entire right, title, and interest in  
(The extent (by percentage) of its ownership interest is \_\_\_\_\_ %); or
- 3.  the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A.  An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy therefore is attached.

OR

B.  A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Herman-Ard Hulst To: Smartflash Limited

The document was recorded in the United States Patent and Trademark Office at  
Reel 013583, Frame 0554, or for which a copy thereof is attached.

2. From: Smartflash Limited To: Patrick Racz

The document was recorded in the United States Patent and Trademark Office at  
Reel 024710, Frame 0790, or for which a copy thereof is attached.

3. From: Patrick Racz To: Smartflash Technologies Limited

The document was recorded in the United States Patent and Trademark Office at  
Reel 024710, Frame 0796, or for which a copy thereof is attached.

Additional documents in the chain of title are listed on a supplemental sheet(s).

As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/ Michael R. Casey /  
Signature

11-14-2013  
Date

Michael R. Casey  
Printed or Typed Name

Attorney of Record  
Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Continuation Sheet for Statement under 37 CFR 3.73(b) for U.S. Patent Serial no. 13/438,754

4. From: Smartflash Technologies Limited      To: Smartflash LLC

The document was recorded in the United States Patent and Trademark Office at

Reel: 030522 Frame: 0877.

## Supplemental Application Data Sheet

### Application Information

Application number:: 13/438,754  
Filing Date:: 04/03/2012  
Application Type:: Regular  
Subject Matter:: Utility  
Suggested classification::  
Suggested Group Art Unit::  
CO-ROM or CD-R??:Number of CD disks::  
Number of copies of COs::  
Sequence Submission::  
Computer Readable Form (CRF)?::  
Number of copies of CRF::  
Title:: Data Storage and Access Systems  
Attorney Docket Number:: ~~87790-837121 (000160US)~~ 4037-0003  
Request for Early Publication:: No  
Request for Non-Publication:: No  
Suggested Drawing Figure::  
Total Drawing Sheets:: 17  
Small Entity?:: ~~Yes~~ No  
Latin name::  
Variety denomination name::  
Petition included?:: No  
Petition Type::  
Licensed US Govt. Agency::  
Contract or Grant Numbers One::  
Secrecy Order in Parent Appl.::

**Applicant Information**

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: United Kingdom  
Status:: Full Capacity  
Given Name:: Patrick  
Middle Name:: Sandor  
Family Name:: Racz  
Name Suffix::  
City of Residence:: Saint ~~Heller~~ Hellier  
State or Province of Residence:: Jersey  
Country of Residence:: United Kingdom  
Street of Mailing Address:: 19 Royal Street  
City of Mailing Address:: Saint Heller  
State or Province of mailing address:: Jersey  
Country of mailing address:: United Kingdom  
Postal or Zip Code of mailing address:: JE1 4WA

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: Netherlands  
Status:: Full Capacity  
Given Name:: Hermen-ard  
Middle Name::  
Family Name:: Hulst  
Name Suffix::  
City of Residence:: Amsterdam  
State or Province of Residence::  
Country of Residence:: Netherlands  
Street of Mailing Address:: Van Tuyll van Serooskerweg 75hs  
City of Mailing Address:: Amsterdam  
State or Province of mailing address::  
Country of mailing address:: Netherlands  
Postal or Zip Code of mailing address:: 1076 JG

### Correspondence Information

Correspondence Customer Number:: ~~20350~~ 42624

### Representative Information

Representative Customer Number:: ~~20350~~ 42624

### Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	13/212,047	08/17/11
13/212,047	Continuation of	12/943,872	11/10/10
12/943,872	Continuation of	12/014,558	01/15/08
12/014,558	Continuation of	11/336,758	01/19/06
11/336,758	Continuation of	10/111,716	09/17/02
<u>10/111,716</u>	<u>National Stage of</u>	<u>PCT/GB2000/004110</u>	<u>10/25/00</u>

### Foreign Priority Information

Country::	Application number::	Filing Date::
<del>PCT</del>	<del>GB00404110</del>	<del>10/25/00</del>
United Kingdom	9925227.2	10/25/99

### Assignee Information

Assignee Name:: ~~Smartflash Technologies Limited~~ Smartflash LLC

Street of mailing address:: ~~1070908 Palm Grove House, P.O. Box 438~~ 100 E. FERGUSON ST.  
406 FIRST PLACE

City of mailing address:: ~~Wickhams' Cay, Road Town~~ Tyler

State or Province of mailing address:: ~~Tortola~~ TX

Country of mailing address:: ~~British Virgin Islands~~ US

Postal or Zip Code of mailing address:: 75702

/ Michael R. Casey /

Dated: 11/14/2013

Michael R. Casey, Reg. No. 40,294

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17404964
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	20350
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	14-NOV-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	16:02:44
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	20131016NewPOAsigned-signed.pdf	170306 <small>68f603a54006acde74a608bff7063d423b0f687e</small>	no	1

### Warnings:

### Information:

2	Assignee showing of ownership per 37 CFR 3.73.	20131030_AssigneeShowingWithCont.pdf	96321 d26be33d49bda5255cfc558d45acb52844d26143	no	2
---	--	--------------------------------------	---	----	---

**Warnings:**

**Information:**

3	Application Data Sheet	20131114_Supplemental_ADS.pdf	79999 7f8b9077dd792071476da6b50e719a8c96e66a01	no	3
---	------------------------	-------------------------------	---	----	---

**Warnings:**

**Information:**

This is not an USPTO supplied ADS fillable form

<b>Total Files Size (in bytes):</b>	346626
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:	Confirmation No.:	3525
Patrick Sandor Racz	Attorney Docket:	4037-0003
Appl. S.N.: 13/438,754	Group Art Unit:	2887
Filing Date: 04-03-2012	Examiner:	LE, THIEN MINH
Title: DATA STORAGE AND ACCESS SYSTEMS	Date:	November 19, 2013

Notice Regarding Previously Submitted Priority Document

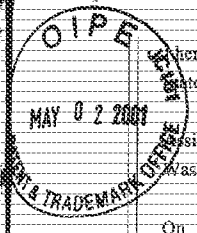
Hon. Commissioner of Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Madam:

The attention of the PTO is hereby directed to the fact that, on information and belief, the UK priority document (UK Patent Application No. 9925227.2, filed October 25, 1999) for the above-identified patent application was previously submitted to the USPTO such that the status of the priority document in the Notice of Allowance should be updated to reflect the previous receipt of that document. More specifically, as shown in Exhibit 1, the UK priority document was submitted by mail on April 30, 2001 in application serial No. 09/697,534 (which also claims priority to that UK application). As shown in Exhibit 2, the "Notification of Missing Requirements" mailed July 17, 2002 in 10/111,716 (to which the present application claims priority) lists the "Priority Document" as one of the documents "submitted by the applicant or the IB [International Bureau] to the United States Patent and Trademark Office."

<b>CHARGE STATEMENT:</b> Deposit Account No. 501860, order no. <b>4037-0003</b> .	
The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 ( <u>missing or insufficiencies only</u> ) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a <u>duplicate</u> copy of this sheet is attached.	
<b>This CHARGE STATEMENT <u>does not authorize</u> charge of the <u>issue fee</u> until/unless an issue fee transmittal sheet is filed.</b>	
CUSTOMER NUMBER <b>42624</b>	Respectfully submitted, By: / Michael R. Casey /  _____ Michael R. Casey, Ph.D. Registration No.: 40,294

EXHIBIT 1



I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Assistant Commissioner for Patents  
Washington, D.C. 20231

#3 2177  
PATENT  
Attorney Docket No.: 80528-000000US  
Client Reference No.: F/USP81421

On April 30, 2001

TOWNSEND and TOWNSEND and CREW LLP

By: Erasmus J. Taylor

RECEIVED  
MAY 4 - 2001  
Technology Center 2100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:  
  
Patrick Sandor Racz  
  
Application No.: 09/697,534  
  
Filed: October 25, 2000  
  
For: DATA STORAGE, RETRIEVAL  
AND ACCESS SYSTEMS

Examiner: Unassigned  
Art Unit: 2177  
SUBMISSION OF CERTIFIED COPY OF  
PRIORITY DOCUMENT

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

Submitted herewith is the certified copy of the priority document, United Kingdom Patent Application No. 9925227.2 filed October 25, 1999, in the above-identified patent application.

Respectfully submitted,

Henry K. Woodward  
Henry K. Woodward  
Reg. No. 2,672

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, 8<sup>th</sup> Floor  
San Francisco, California 94111-3834  
Tel: (650) 326-2400  
Fax: (650) 326-2422  
HKW:ejt  
PA 3142524 v1



INVESTOR IN PEOPLE

The Patent Office  
Concept House  
Cardiff Road  
Newport  
South Wales  
NP10 8QQ

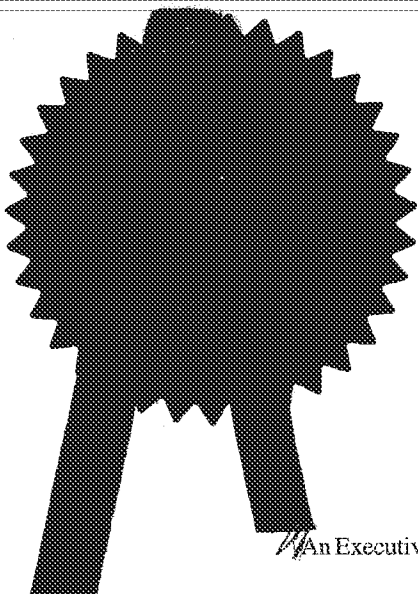
RECEIVED  
MAY 4 - 2001  
Technology Section 2100

I, the undersigned being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed *W. Evans*

Dated 20 April 2001

For official use

26OCT99 E486875-5 D03312  
PS1/7700 0.00 - 9925227.2

25 OCT 1999

Your reference 230P81421

25 OCT 1999

9925227.2

**Notes**

Please type, or write in dark ink using CAPITAL letters. A prescribed fee is payable for a request for grant of a patent. For details, please contact the Patent Office (telephone 071-438 4700).

Rule 16 of the Patents Rules 1990 is the main rule governing the completion and filing of this form.

Do not give trading styles, for example, 'Trading as XYZ company', nationality or former names, for example, 'formerly (known as) ABC Ltd' as these are not required.

**Warning**

After an application for a Patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977 and will inform the applicant if such prohibition or restriction is necessary. Applicants resident in the United Kingdom are also reminded that under Section 23, applications may not be filed abroad without written permission unless an application has been filed not less than 6 weeks previously in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction revoked.

**The Patent Office** **Request for grant of a Patent** **Form 1/77** **Patents Act 1977**

**1 Title of invention**

1 Please give the title of the invention *Data Storage, Retrieval and Access Systems.*

**2 Applicant's details**

**First or only applicant**

2a If you are applying as a corporate body please give:

Corporate name *Internet Limited*

Country (and State of incorporation, if appropriate) *United Kingdom*

2b If you are applying as an individual or one of a partnership please give in full:

Surname

Forenames

2c **In all cases, please give the following details:**

Address *Upper Nordens, High Hurst Wood, Uckfield, East Sussex, TN22 4AN*  
*United Kingdom*

UK postcode (if applicable)

Country  
ADP number (if known)

*7767106001*

2d, 2e and 2f: If there are further applicants: please provide details on a separate sheet of paper.

**Second applicant (if any)**

2d If you are applying as a corporate body please give:

Corporate name

Country (and State of incorporation, if appropriate)

2e If you are applying as an individual or one of a partnership please give in full:

Surname

Forenames

2f In all cases, please give the following details:

Address

UK postcode (if applicable)

Country

ADP number (if known)

An address for service in the United Kingdom must be supplied

Please mark correct box

**Address for service details**

3a Have you appointed an agent to deal with your application?

Yes  No  go to 3b

please give details below

Agent's name

Marks & Clerk

Agent's address

57-60 Lincoln's Inn Fields  
LONDON  
WC2A 3LS.

Postcode

Agent's ADP number

18001

3b: If you have appointed an agent, all correspondence concerning your application will be sent to the agent's United Kingdom address.

3b If you have not appointed an agent please give a name and address in the United Kingdom to which all correspondence will be sent:

Name

Address

Postcode

ADP number (if known)

Daytime telephone number (if available)

**④ Reference number**

4 Agent's or applicant's reference number (if applicable) 230PB1421

**⑤ Claiming an earlier application date**

5 Are you claiming that this application be treated as having been filed on the date of filing of an earlier application?

Please mark correct box

Yes  No  go to 6

please give details below

number of earlier application or patent number

filing date (day month year)

and the Section of the Patents Act 1977 under which you are claiming:

Please mark correct box

15(4) (Divisional)  8(3)  12(6)  37(4)

⑥ If you are declaring priority from a PCT Application please enter 'PCT' as the country and enter the country code (for example, GB) as part of the application number.

**⑥ Declaration of priority**

6 If you are declaring priority from previous application(s), please give:

Please give the date in full number format, for example, 31/05/90 for 31 May 1990.

Country of filing	Priority application number (if known)	Filing date (day, month, year)

- The answer must be 'No' if:
- any applicant is not an inventor
- there is a inventor who is not an applicant, or
- any applicant is a corporate body.

### 7 Inventorship

7 Are you (the applicant or applicants) the sole inventor or the joint inventors?  
 Please mark correct box  
 Yes  No  **A Statement of Inventorship on Patents Form 7/77 will need to be filed (see Rule 15).**

• Please supply duplicates of claim(s), abstract, description and drawing(s).

### 8 Checklist

8a Please fill in the number of sheets for each of the following types of document contained in this application.

Continuation sheets for this Patents Form 1/77

Claim(s)  Description

Abstract  Drawing(s)  *(Informal)*

8b Which of the following documents also accompanies the application?

Priority documents (please state how many)

Translation(s) of Priority documents (please state how many)

Patents Form 7/77 - Statement of Inventorship and Right to Grant (please state how many)

Patents Form 9/77 - Preliminary Examination/Search

Patents Form 10/77 - Request for Substantive Examination

Please mark correct box(es)

• You or your appointed agent (see Rule 90 of the Patents Rules 1990) must sign this request.

### Request

I/We request the grant of a patent on the basis of this application.

Please sign here ➡

Signed *Marks & Clerk* Date *25-10-99*  
(day month year)

A completed fee sheet should preferably accompany the fee.

Please return the completed form, attachments and duplicates where requested, together with the prescribed fee to:

The Comptroller  
 The Patent Office  
 Cardiff Road  
 Newport  
 Gwent  
 NP9 1RH

or  The Comptroller  
 The Patent Office  
 25 Southampton Buildings  
 London  
 WC2A 1AY



### DATA STORAGE, RETRIEVAL AND ACCESS SYSTEMS

This invention is generally concerned with data storage, retrieval and access systems. More particularly it relates to apparatus and methods for mobile and/or portable data retrieval and use and to data storage means and to means for controlling access to, and paying for, data and to apparatus, methods and systems therefor. The invention may be used, for example, for providing and controlling access to MP3 audio and compressed video data sources.

Once problem associated with the increasingly wide use of the internet is the growing prevalence of so-called data pirates. Such pirates obtain data either by unauthorised or legitimate means and then make this data available essentially world-wide over the internet without authorisation. Data can be a very valuable commodity, but once it has been published on the Internet it is difficult to police access to and use of it by Internet users who may not even realise that it is pirated. This is a particular problem with audio recordings, and, once the bandwidth becomes available, is also likely to be evident with video.

Over the past three or four years MP3 (MPEG3 format encoded) audio sources have become increasingly widely available on web pages. MP3 or MPEG3 is an internationally defined standard for compressing audio information such as speech or music. It relies on psycho-acoustic properties of human hearing to achieve very large factors of data compression. It is thus feasible to download usefully long passages of music in a practically convenient short time. Pirate data suppliers have not been slow to realise the potential of this and many unauthorised website have sprung up offering popular music including recent releases by world famous bands. This has caused the recording industry considerable concern and there is an urgent need to find a way to address the problem of data piracy.

The invention described below addresses this problem and may be able to convert this threat into a potential opportunity.

According to the present invention there is therefore provided a mobile data retrieval device [as claim 1].

According to a second aspect of the invention there is provided a data processing system [as claim 18].

According to a third aspect of the invention there is provided a data storage means [as claim 22].

According to a yet further aspect of the invention there is provided a method [as claim 28].

The payment validation means is, for example, means to validate payment with an external authority such as a bank or building society. The combination of the payment validation means with the data storage means allows the access to the downloaded data which is to be stored by the data storage means, to be made conditional upon checked and validated payment being made for the data. Binding the data access and payment together allows the legitimate owners of the data to make the data available themselves over the internet without fear of loss of revenue. This has the potential to undermine the position of the data pirates.

A further advantage of the system is that it allows users under the age of 18 to make internet purchases. Currently internet users pay for goods and/or services by credit card. Since credit cards cannot be legitimately be used by persons under the age of 18 (at least in the UK), a significant fraction of adventurous internet users are excluded from e-commerce, one of the most significant predicted uses of the internet. In one embodiment of the invention however, the payment validation means comprises e-cash - that is the payment validation means stores transaction value information on a cash value of transactions validatable by the data storage means. In simple terms, the data storage means can be a card which is charged up to a desired cash value (if necessary limited to a maximum value) at a suitable terminal. This might be an internet access terminal but could, more simply, be a device to accept the data storage card and to receive and count money deposited by the user to charge the card, writing update cash value information onto the card. More sophisticated ways of updating the cash value on the card are also possible, such as direct bank transfer. Since, with this type of embodiment, the

data storage means is, essentially, precharged with cash rather than acting as a credit card it can be used by young people without the risk of their incurring large debts.

In one embodiment the data storage means is powered by the retrieval device when it is connected to the device and retains a memory of the downloaded data when it is unpowered. This can be achieved by the use of Flash RAM or, more generally, any form of programmable read-only memory. Alternatively the data storage means may incorporate a rechargeable cell of capacitor and store information in battery backed-up static RAM.

The downloaded data maybe entered into the data storage device by means of an interface such as a magnetically or capacitatively coupled connection or an optical connection, but preferably the interface comprises contacts for direct electrical connection to the storage means. The payment validation means may likewise have one of a variety of interfaces but again preferably comprises a set of electrical contacts. The payment validation means could, however comprise a magnetic or holographic data-strip such as is known for use with credit cards and phone cards. Preferably, the interface to receive the downloaded data, is separate from the interface to the payment validation means, to allow separate and simultaneous access to both these systems. Advantageously the payment validation means includes a memory storing information to identify the person who is paying for the downloaded data.

For additional security the downloaded data may be encrypted. In this case data decryption may be necessary at some stage, either in the data storage means or in the retrieval device or in an information-delivering apparatus such as the data access terminal. Alternatively the data decryption function can be shared amongst one or more of these devices. The skilled person will be aware of a range of suitable encryption/decryption techniques including Pretty Good Privacy (Registered Trade Mark) and PKI. Normally when the downloaded data is encrypted a decryption key must be supplied. This can be generated automatically by the data access terminal or data access service provider or it can be entered by the user into the data access terminal or into the mobile data retrieval device.

The data storage means and/or the retrieval device can be provided with access control means to prevent unauthorised access to the downloaded data. Alternatively, this access control

means can be used to stop or provide only limited access of the user to the downloaded data in accordance with the amount paid. Thus, for example, a complete set of data information relating to a particular topic, a particular music track, or a particular software package might be downloaded, although access to part of the data set might thereafter be controlled by payments made by a user at a later stage. Thus, a user could pay to enable an extra level on a game or to enable further tracks of an album.

In embodiments where the access control means is responsive to the payment validation means access control information may be stored with the downloaded data or in a separate storage area, for example in the payment validation means. The user's access to the downloaded data could advantageously be responsive to the payment validation means, for example, by means of a control line coupling the payment validation means with a memory access or decryption control element.

In a preferred embodiment the data storage means comprises an electronic memory card or smart card and the mobile data retrieval device is provided with a slot to receive the card. Preferably the card is a push-fit within the retrieval device, and retention of the card may be effected by pressure from electrical interface connections and/or resilience of the housing, or by using a resilient retaining means. In a preferred embodiment the retrieval device includes an audio output and a display, to play a downloaded track and to show information about the track and/or an accompanying video.

To download data onto the data storage means the user can employ a data access terminal coupled to the internet. The terminal can directly validate payment - for example in the case of a smart card charged with electronic cash it can deduct a cash value from the card.

Alternatively it can communicate with a bank or other financial services provider to control payment. In a preferred embodiment, however, the terminal connects to a data access service provider which provides a portal to other sites and which validates payment and then forwards data from a data supplier to the user's local access terminal. The data access service provider may alternatively forward payment validation information and/or information from the payment validation authority to the data supplier for control by the supplier of the data

supplied. Thus, access to the payment validation system and/or data for downloading may be entirely controlled by the data supplier.

Data held on the data storage means may advantageously include data relating to the user's or payer's usage of the system. This information may include, for example, information on a user's spending pattern, information on data supplies used and information on the downloaded data. This information may be accessed by the data supplier and/or data access service provider and can be used for targeted marketing or loyalty-based incentive schemes such as air miles or the like.

The data access terminal may be a conventional computer or, alternatively, it may be a mobile phone. The Wireless Application Protocol (WAP) allows mobile phones to efficiently access the internet and this allows a mobile phone to be used to download data to the data storage means, advantageously, directly. The data storage means can, if desired, incorporate the functionality of a mobile phone SIM card, which cards already include a user identification means allowing through the phone network operator, user billing.

In preferred embodiment the downloaded data is MP3 encoded audio data, but the system finds more general application for other data types. For example, download data can include software, share price information, current news information, transport timetable information, weather information and catalogue shopping information. The downloaded information may also include compressed video data. The storage capacity of the data storage means is adaptable to suit the type of data intended to be downloaded - for example, 32 megabytes is sufficient for CD quality music, but for video it is preferable that the data storage means has a capacity of 128 megabytes or greater.

These and other aspects of the invention will now be further described, by way of example only, with reference to the accompanying figures in which:-

Figure 1 shows an embodiment of a mobile data retrieval device according to the present invention, a) from the top; b) from the front; and c) from the side;

Figure 2 shows an embodiment of a data storage means according to the present invention;

Figures 3a and b show data access terminals;

Figure 4a shows a logical signal path between elements of a data providing system; and  
Figure 4b shows a physical representation of a data providing system.

Referring to Figure 1, this shows a mobile data retrieval device for playing MP3 audio (10) with operator controls (12) and LCD display (14). The outline of a smart card data storage device is shown at (16). The operator controls allow a user to select and play tracks, whilst track information and still or video images are provided on display (14). A slot (18) is provided in the front of the device to receive a smart card-type data storage means. This smart card occupies space (20) and interfaces with resilient contacts (24); it is held in the data retrieval device against the contacts, by resilient housing element (22).

Referring now to Figure 2, this shows a data storage means (30) suitable for use with the retrieval device of Figure 1. The data storage means is based on a standard smart card; it is plastic, about the size of a standard credit card, and has some flexibility. On the card (30) are two sets of contacts, contacts (32) for interfacing with the payment validation means and contacts (34) for interfacing with the memory for storing downloaded data. The surface of the card can be embellished with suitable graphics.

Preferably the smart card retains all its useable functionality as specified for standard Electronics Point of Sale Systems (EPOSS) and, if desired, the memory for storing the downloaded data can be electrically separate from this. However, it may be preferable to provide interaction between the standard smart card device and the data memory in order to accomplish the access control/decryption functions described above.

Referring now to Figure 3, one embodiment of a data access terminal is shown at (40). This has a screen (42) and a slot (44) to receive the data storage means (30). Alternatively the data storage means may interface to the terminal via the data retrieval device (10) and an interface (46) to the terminal (40). In Figure 3b a dedicated terminal (50) has a slot (52) to receive the

data storage means, a display (54) and controls (56). Coins can be inserted into the terminal at (58) and notes at (60) to charge the data storage means with cash.

Referring now to Figure 4a, this illustrates the logical connections and data flow between data processing systems involved in payment validation, and data download to storage means (30). A user connects the data storage means (30) to terminal (40) and logs on to a data web page of data access service provider (60). Either terminal (40) or service provider (60) then communicates via data paths (62) with payment validation authority (70) to check and authorise the user's or payer's payment. In the case of electronic cash the terminal (40) may immediately validate the payment information, updating the service provider and/or payment validation authority (70) at a later stage. The logical connection (64) between the terminal and the service provider is preferably made over the internet.

The service provider may provide a direct portal to data suppliers (80) or may collect information from data suppliers (80) and provide a "front end" to present data from the suppliers to the terminal user. Alternatively service provider (60) may regulate direct access between terminal (40) and data suppliers (80), as shown by links (66), by communicating with the terminal and the data suppliers to provide communication regulation information to, for example, instruct data suppliers about what information the user of terminal (40) should have access to.

In a preferred embodiment service provider (60) pays royalties at an agreed rate - for example, 10 pence per track or 10 pence per minute - to an appropriate organ of the recording industry and the user of terminal (40) effectively pays the service provider. Billing can also be regulated by bandwidth and/or data download time.

Preferably the service provider (60) monitors the user's access to the system and either stores or forwards to data suppliers (80), or downloads to data storage means (30), usage information. In a preferred embodiment the service provider sends information via terminal (40) to data storage means (30) which can be used to determine incentives to be provided to users of the system.

Figure 4B shows a physical configuration of the system of Figure 4A in which a plurality of terminals (40), a plurality of service providers (60) and a plurality of data suppliers (80) all interact via the internet. The physical embodiment of the system is not critical and a skilled person will understand that the terminals, data processing systems and the like can all take a variety of forms.

The skilled person will understand that many variants to the system are possible and the invention is not limited to the described embodiments.



**CLAIMS:**

1. A mobile data retrieval device comprising:
  - a removable data storage means;
  - data access means, to access downloaded data on the data storage means;
  - storage interface means adapted to couple the data storage and data access means; and
  - data output means to provide the downloaded data, in a useful form, to a user of the device;wherein the data storage means further comprises payment validation means to validate payment for the downloaded data.
2. A mobile data retrieval device as claimed in claim 1 wherein the data storage means receives power from the retrieval device when connected to the device and retains storage by the downloaded data when unpowered.
3. A mobile data retrieval device as claimed in claim 1 or 2 wherein the data storage means comprises external data interface means to receive data downloaded from an external source onto the card for storage and wherein the payment validation means comprises means to validate payment to the external source.
4. A mobile data retrieval device according to any preceding claim wherein the payment validation means comprises memory means to store transaction value information on a cash value of transactions validatable by the data storage means.
5. A mobile data retrieval device according to any preceding claim wherein the payment validation means comprises memory means to store information to identify a payer for the downloaded data.

6. A mobile data retrieval device according to any preceding claim wherein one of the data storage means and the retrieval device further comprises data description means to at least partially decrypt downloaded data.
7. A mobile data retrieval device according to any preceding claim wherein one of the data storage means and the retrieval device comprises access control means to prevent unauthorised access to the downloaded data.
8. A mobile data retrieval device according to claim 7 wherein the access control means is responsive to the payment validation means.
9. A mobile data retrieval device according to any one of claims 3 to 8 wherein the payment validation means comprises a payment validation means interface operable simultaneously with the external data interface means.
10. A mobile data retrieval device according to any preceding claim wherein the data storage means comprises an electronic memory card or smart card.
11. A mobile data retrieval device according to claim 10 having a housing with a slot therein to receive the data storage means.
12. A mobile data retrieval device according to claim 11 further comprising local storage means and means to copy data from the data storage means into the local storage means.
13. A mobile data retrieval device according to claim 11 or 12 wherein the retrieval device is portable and, in two directions, is not substantially larger than the data storage means.

14. A mobile data retrieval device according to any preceding claim wherein the storage interface means is adapted for repeated removal and reconnection of the data storage means to the retrieval device.
15. A mobile data retrieval device according to any preceding claim further comprising display means to display information derived from the downloaded data to the user.
16. A mobile data retrieval device according to any preceding claim further comprising audio output means to provide an audio output corresponding to the downloaded data to the user.
17. A mobile data retrieval device according to any preceding claim comprising a first set of contacts for the storage interface means and a second set of contacts for interfacing to the payment validation means.
18. A data providing system comprising a mobile data retrieval device as claimed in any preceding claim, and  
a data access terminal to interface with the data storage means to download data and to co-operate with the payment validation means to validate payment for the downloaded data.
19. A data providing system as claimed in claim 18 wherein the data access terminal is couplable to the internet and co-operates with the payment validation means to validate payment with a payment validation authority and is operable to download data to the data storage means from a data supplier on the internet.
20. A data providing system as claimed in claim 19 wherein the data access terminal operates through a data access service provider, the data access service provider being configured to communicate with the payment validation authority and to control access of data access terminal to data from the data supplier.

21. A data storage means for use with the device or system of any preceding claim.
22. A data storage means comprising an external data interface means to receive data downloaded from an external source onto the card for storage; and payment validation means comprising means to validate payment to the external source, and/or to a payment validation authority.
23. A data storage means as claimed in claim 22 further comprising data decryption means to at least partially decrypt the downloaded data.
24. A data storage means as claimed in claim 22 or 23 further comprising access control means to prevent unauthorised access to the downloaded data.
25. A data storage means as claimed in claim 24 wherein the access control means is responsive to the payment validation means.
26. A data storage means according to any one of claims 22 to 25 wherein the payment validation means comprises a payment validation means interface operable simultaneously with the external data interface means.
27. A data storage means according to any one of claims 22 to 26 wherein the data storage means comprises an electronic memory card or smart card.
28. A method of providing portable data comprising the steps of:
  - (i) providing a portable data storage device comprising downloaded data storage means and payment validation means;
  - (ii) providing a terminal for internet access;
  - (iii) coupling the portable data storage device to the terminal;

- (iv) reading payment information from the payment validation means using the terminal;
  - (v) validating the payment information; and
  - (vi) downloading data into the portable storage device from a data supplier.
29. A method as claimed in claim 28 further comprising writing updated payment information into the payment validation means.
30. A method as claimed in claim 28 or 29 further comprising communicating a result of the validating step to the data supplier.
31. A method as claimed in any one of claims 28 to 30 further comprising controlling access by the terminal to data from the data supplier using another data processing system on the internet.
32. A method as claimed in claim 31 wherein the another data processing system performs said step of validating.
33. A method as claimed according to any one of claims 28 to 32 wherein said step of coupling is performed by a mobile data retrieval device as claimed in any one of claims 1 to 17.
34. A method as claimed in claims 28 to 34 further comprising writing usage information into the data storage means, the usage information relating to use made of the data storage means, such as information relating to the downloaded data, to data supplier or suppliers used; and/or to a user's spending patterns.
35. A method as claimed in claims 28 to 33 wherein said portable data storage device comprises an electronic memory card or smart card.

36. A device, system, data storage means, or method as claimed in any preceding claim wherein the data is MP3 encoded audio data.

37. A data retrieval device, system, data storage means, or method substantially as hereinbefore described.

**ABSTRACT:**

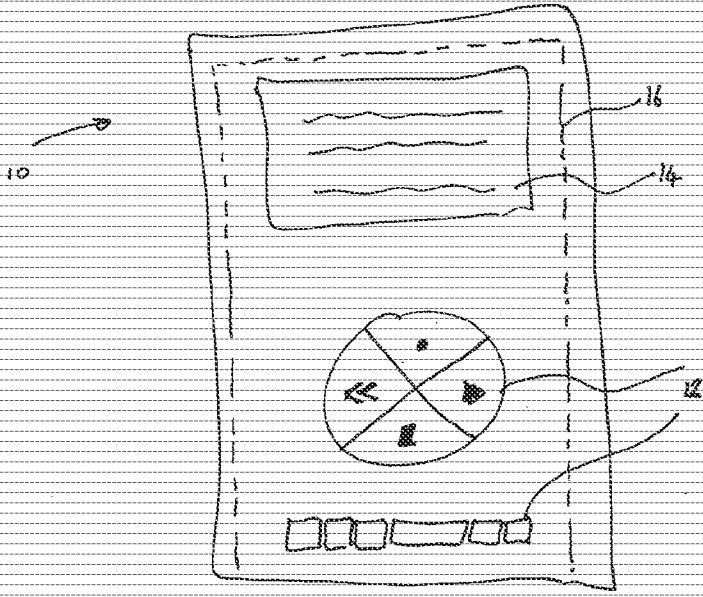
A mobile data retrieval device comprising: a removable data storage means; data access means, to access downloaded data on the data storage means; storage interface means adapted to couple the data storage and data access means; and data output means to provide the downloaded data, in a useful form, to a user of the device; wherein the data storage means further comprises payment validation means to validate payment for the downloaded data.

A data storage means comprising an external data interface means to receive data downloaded from an external source onto the card for storage; and payment validation means comprising means to validate payment to the external source, and/or to a payment validation authority.

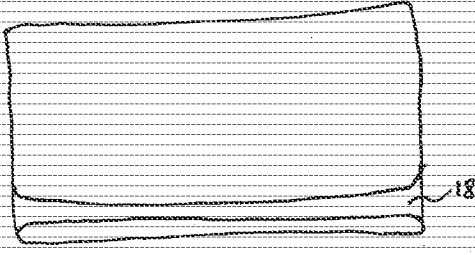
(Fig. 4A)

FIGURE 1

A



B



C

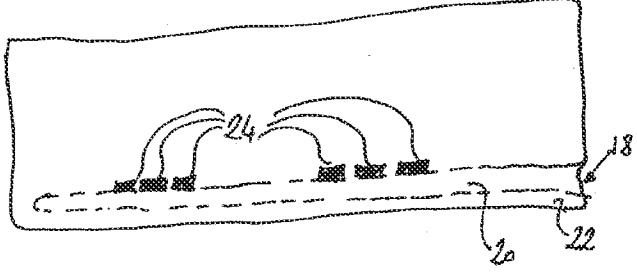




FIGURE 2

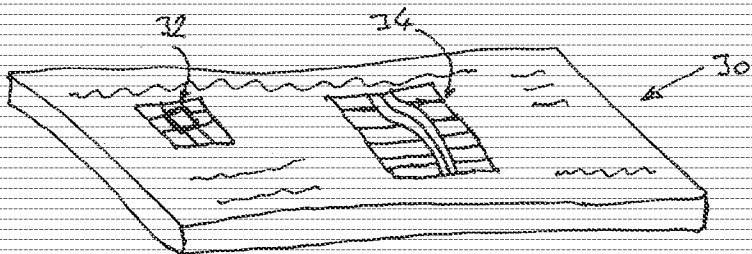


FIGURE 3

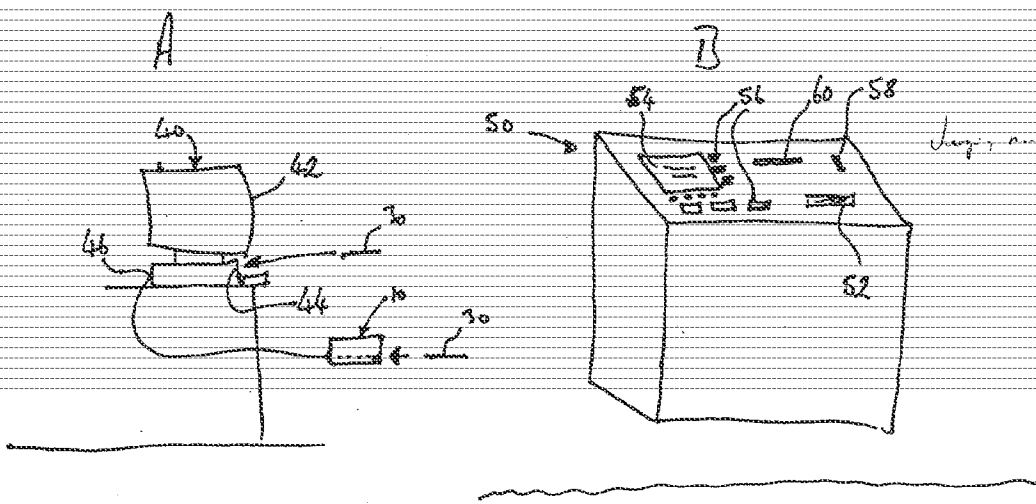
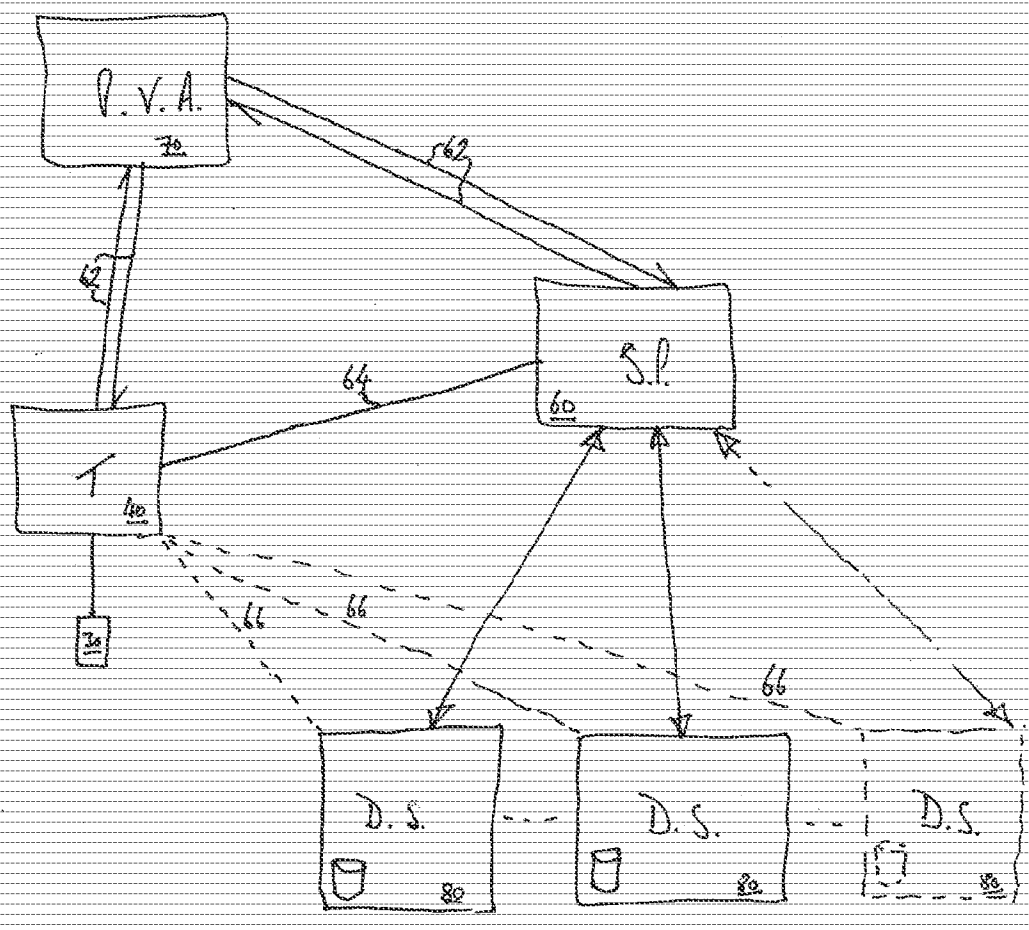
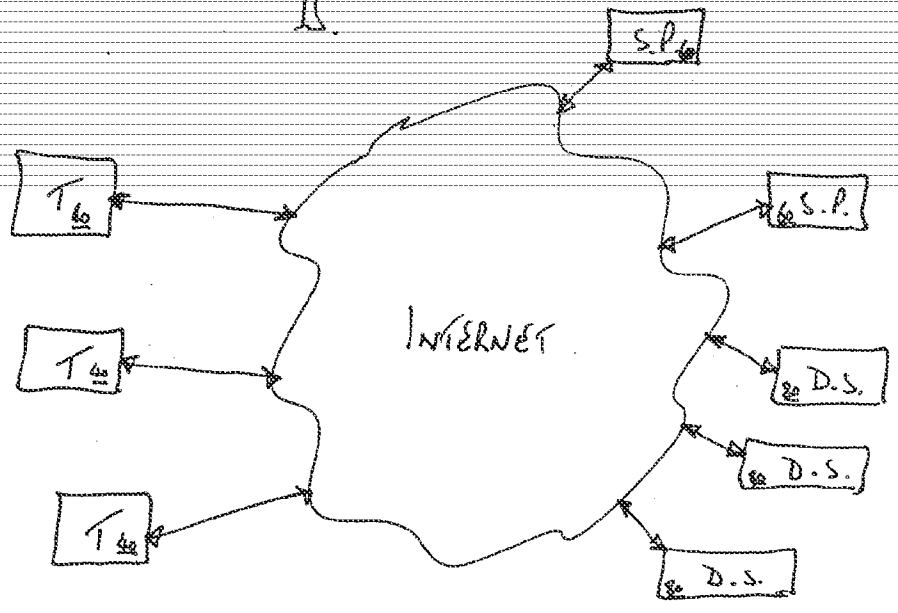


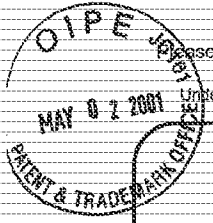
FIGURE 4

A.



B.





Please type a plus sign (+) inside this box

Approved for use through 10/31/2002. OMB 0661-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>TRANSMITTAL FORM</b>  <i>(to be used for all correspondence after initial filing)</i>	Application Number	09/697,534	
	Filing Date	October 25, 2000	
	First Named Inventor	Patrick Sandor Racz	
	Group Art Unit	2177	
	Examiner Name	Unassigned	
Total Number of Pages in This Submission	1	Attorney Docket Number	080528000000

ENCLOSURES (check all that apply)		
<input type="checkbox"/> Fee Transmittal Form  <input type="checkbox"/> Fee Attached  <input type="checkbox"/> Amendment / Response  <input type="checkbox"/> After Final  <input type="checkbox"/> Affidavits/declaration(s)  <input type="checkbox"/> Extension of Time Request  <input type="checkbox"/> Express Abandonment Request  <input type="checkbox"/> Information Disclosure Statement <input checked="" type="checkbox"/> Certified Copy of Priority Document(s)  <input type="checkbox"/> Response to Missing Parts/ Incomplete Application <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Assignment Papers (for an Application)  <input type="checkbox"/> Drawing(s)  <input type="checkbox"/> Licensing-related Papers  <input type="checkbox"/> Petition Routing Slip (PTO/SB/69) and Accompanying Petition  <input type="checkbox"/> Petition to Convert to a Provisional Application  <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address  <input type="checkbox"/> Terminal Disclaimer  <input type="checkbox"/> Request for Refund  <input type="checkbox"/> CD, Number of CD(s)	<input type="checkbox"/> After Allowance Communication to Group  <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences  <input type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)  <input type="checkbox"/> Proprietary Information  <input type="checkbox"/> Status Letter  <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): <b>Submission of Certified Copy of Priority Document</b> <b>Return Receipt Postcard</b>
Remarks		The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

RECEIVED  
MAY 4 2001  
TECHNOLOGICAL CENTER

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm and Individual name	Townsend and Townsend and Crew LLP Henry K. Woodward Reg No. 22,672
Signature	<i>Henry K. Woodward</i>
Date	<i>April 30, 2001</i>

CERTIFICATE OF MAILING	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on this date: <u>April 30, 2001</u>	
Typed or printed name	<u>Eleanor J. Taylor</u>
Signature	<i>Eleanor J. Taylor</i>
Date	<u>April 30, 2001</u>

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231. PA 3142572 v1

EXHIBIT 2



UNITED STATES PATENT AND TRADEMARK OFFICE

 Commissioner for Patents, Box PCT  
 United States Patent and Trademark Office  
 Washington, D.C. 20231  
 www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
10/111,716	Hulst Hermen-Ard	080379-000000US

INTERNATIONAL APPLICATION NO.
PCT/GB00/04110

I.A. FILING DATE	PRIORITY DATE
10/25/2000	11/25/1999

Kevin T LeMond  
 Townsend and Townsend and Crew  
 Two Embarcadero Center  
 Suite 800  
 San Francisco, CA 94111-3834

**CONFIRMATION NO. 8373****371 FORMALITIES LETTER**

\*OC00000008454782\*

Date Mailed: 07/17/2002

### NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as an Elected Office (37 CFR 1.495):

- U.S. Basic National Fees
- Indication of Small Entity Status
- Priority Document
- Copy of IPE Report
- Copy of references cited in ISR
- Copy of the International Application
- Copy of the International Search Report
- Information Disclosure Statements
- Oath or Declaration
- Preliminary Amendments
- Request for Immediate Examination

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date. The current oath or declaration does not comply with 37 CFR 1.497(a) and (b) in that it:
  - is not executed in accordance with either 37 CFR 1.66 or 37 CFR 1.68.
- \$65 Surcharge for providing the oath or declaration later than the appropriate 30 months months from the priority date (37 CFR 1.492(e)) is required.

**ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTH FROM THE DATE OF THIS NOTICE OR BY 22 or 32 MONTHS (where 37 CFR 1.495 applies) FROM THE PRIORITY DATE FOR**

**THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.**

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Additionally the following defects have been observed:

- Additional claim fees of **\$546** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

**SUMMARY OF FEES DUE:**

Total additional fees required for this application is **\$611** for a Small Entity:

- **\$65** Late oath or declaration Surcharge.
- Total additional claim fee(s) for this application is **\$546**
  - **\$546** for **13** independent claims over 3.

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

*A copy of this notice **MUST** be returned with the response.*

INDIA L EVANS

Telephone: (703) 305-2936

**PART 2 - OFFICE COPY**

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/111,716	PCT/GB00/04110	080379-000000US

FORM PCT/DO/EO/905 (371 Formalities Notice)

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17443828
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	42624
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	4037-0003
<b>Receipt Date:</b>	19-NOV-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	15:26:32
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	20131119_NoticeOfPreviousPriorityDocumentSubmission.pdf	2317689 <small>765d3338df54333ed538f52129cb6bac9de105b3</small>	no	30

### Warnings:

### Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		13438754	
	Filing Date		2012-04-03	
	First Named Inventor	Patrick Sandor Racz		
	Art Unit		2887	
	Examiner Name	LE, THIEN MINH		
	Attorney Docket Number		4037-0003	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup> j	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1	3-73481	JP		1991-03-28		(Partial Translation)	<input type="checkbox"/>
	2	59-195391	JP		1984-11-06		(Partial Translation)	<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS								Remove
---------------------------------	--	--	--	--	--	--	--	--------

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number	13438754
	Filing Date	2012-04-03
	First Named Inventor	Patrick Sandor Racz
	Art Unit	2887
	Examiner Name	LE, THIEN MINH
	Attorney Docket Number	4037-0003

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
	1	Decision of Rejection dated July 23, 2013 in Japanese Application No. 2011-066325 (which also claims priority to the same UK priority document as the present application)	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

#### EXAMINER SIGNATURE

Examiner Signature	Date Considered
--------------------	-----------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	13438754		
Filing Date	2012-04-03		
First Named Inventor	Patrick Sandor Racz		
Art Unit	2887		
Examiner Name	LE, THIEN MINH		
Attorney Docket Number	4037-0003		

**CERTIFICATION STATEMENT**

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

**OR**

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

**SIGNATURE**

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ Michael R. Casey /	Date (YYYY-MM-DD)	2013-11-19
Name/Print	Michael R. Casey	Registration Number	40294

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754			
<b>Filing Date:</b>	03-Apr-2012			
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS			
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz			
<b>Filer:</b>	Michael R. Casey			
<b>Attorney Docket Number:</b>	4037-0003			
Filed as Large Entity				
<b>Utility under 35 USC 111(a) Filing Fees</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Submission- Information Disclosure Stmt	1806	1	180	180
<b>Total in USD (\$)</b>				<b>180</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17445640
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	42624
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	4037-0003
<b>Receipt Date:</b>	19-NOV-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	16:35:26
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$180
RAM confirmation Number	3839
Deposit Account	501860
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	NP-JpOA.pdf	902455 0e9fd90d977b95e4b2c6e975d0c966c2e7d2a91	no	9
<b>Warnings:</b>					
<b>Information:</b>					
2	Foreign Reference	3-073481-withSOR.pdf	825861 ca3a46c015c746586d7166b0ded016f649736263	no	10
<b>Warnings:</b>					
<b>Information:</b>					
3	Foreign Reference	59-195391-withSOR.pdf	1433158 4d2b99624d4b05c784ad220c76a660c4039c2402	no	15
<b>Warnings:</b>					
<b>Information:</b>					
4	Information Disclosure Statement (IDS) Form (SB08)	20131119_updated_IDS-3refs.pdf	612257 ed18e6ff77835396b341b3a7f0bc24764a118b9	no	4
<b>Warnings:</b>					
<b>Information:</b>					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
5	Fee Worksheet (SB06)	fee-info.pdf	30280 283941332570bdc0c64b56ed296e7ffb01519ab	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			3804011		



**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

Statement of Relevancy

JP 03-073481 was cited in Japanese Application No. 2011-066325 (which also claims priority to the same UK priority document as the present application)

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-073481

(43)Date of publication of application : 28.03.1991

(51)Int.Cl. G11B 23/30

G11B 7/24

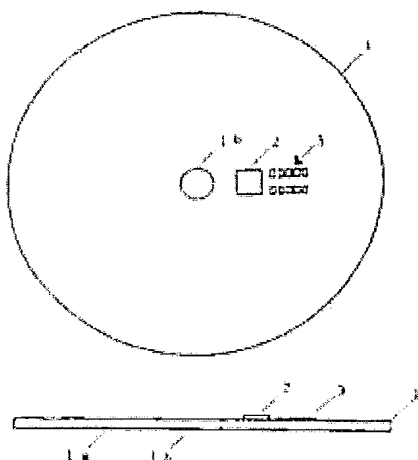
(21)Application number : 01-209056

(71)Applicant : YAMAHA CORP

(22)Date of filing : 11.08.1989

(72)Inventor : KAGEYAMA YASUO

## (54) DISK-SHAPED MEMORY MEDIUM



### (57)Abstract:

**PURPOSE:** To allow the memory of information on the end point of reading out, etc., and to improve the reading out efficiency by providing a memory which allows reading and writing on the disk-shaped memory medium.

**CONSTITUTION:** The non-volatile memory 2 which allows reading and writing on the surface or in the inside of the medium 1 to allow the transmission and reception of data to and from the outside via terminals 3. Contacts for data transmission and reception are provided on a medium reader, by which the program of the address during the course of reading out and reading out sequence, etc., are stored in this non-volatile memory 2. Such data is stored into the medium 1 itself in such a manner, by which the restarting of the reading in accordance with this data is possible even when the medium 1 is set in any

reader. The efficient data reading is thus executed.

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

平3-73481

⑬ Int. Cl.<sup>3</sup>

識別記号

庁内整理番号

⑭ 公開 平成3年(1991)3月28日

G 11 B 23/30  
7/24

B 8622-5D  
Z 8120-5D

審査請求 未請求 請求項の数 1 (全7頁)

⑮ 発明の名称 ディスク状記憶媒体

⑯ 特 願 平1-209056

⑰ 出 願 平1(1989)8月11日

⑱ 発 明 者 藤 山 保 夫 静岡県浜松市中沢町10番1号 ヤマハ株式会社内  
 ⑲ 出 願 人 ヤマハ株式会社 静岡県浜松市中沢町10番1号  
 ⑳ 代 理 人 弁理士 小 森 久 夫

明 細 書

1. 発明の名称

ディスク状記憶媒体

2. 特許請求の範囲

(1) 記憶媒体の表面または内部に、リードライ  
ト可能な不揮発性メモリを設け、この不揮発性メ  
モリを外部からアクセス可能な端子を前記記憶媒  
体表面に設けたことを特徴とするディスク状記憶  
媒体。

3. 発明の詳細な説明

(a) 産業上の利用分野

この発明はCDROM等のディスク状記憶媒体  
に関し、特に、読出経過等のデータをメモしてお  
くことができるディスク状記憶媒体に関する。

(b) 従来の技術

現在実用化されているディスク状記録媒体に光  
ディスクがある。光ディスクには大量のデータが  
記憶でき、読取ヘッドを移動させることにより、  
ランダムなアクセスが可能である。このため、た

えば音楽用CDを再生する装置では再生曲順を  
自由に設定できるプログラム再生モードを備えて  
いるものも実用化されている。

(c) 発明が解決しようとする課題

しかし、従来CD自体にこのプログラムを書き  
込むことができなかったため、CDをセットする  
度にプログラムする必要がある極めて面倒であっ  
た。これを解決しようと、CDのコントロールデ  
ータを検索キーとするテーブルを本体内に設けて  
再生順序のプログラム等を記憶しておき、CDが  
セットされたときそのCDのコントロールデータ  
でテーブルを検索してプログラムを読み出せるよ  
うにし、CDセット毎にプログラムをしなくても  
よいCD再生装置も実用化されている。

しかし、このようなCD再生装置では、デー  
タを記憶できるCDの枚数に制限があるうえ、ある  
CD再生装置にプログラムを記憶しても他の再生  
装置に同じCDをセットした場合にはこのプログ  
ラムは有効でない欠点があった。

また、CD等のランダムアクセス媒体は、テー

ブ媒体等の順次読出媒体とは異なり、読み出しを中断した状態を保持することができないため、読出を中断したのち再開する場合には、最初から再度読み出しを行わなければならないため読出効率が低下する欠点があった。

この発明は、CD等のディスク状記憶媒体にリードライト可能なメモリを設けることにより、読み出し終了点等の情報の記憶を可能にし、読出効率を向上したディスク状記憶媒体に関する。

#### (d) 課題を解決するための手段

この発明は、記憶媒体の表面または内部に、リードライト可能な不揮発性メモリを設け、この不揮発性メモリを外部からアクセス可能な端子を前記記憶媒体表面に設けたことを特徴とする。

#### (e) 発明の作用

この発明のディスク状記憶媒体では、媒体の表面または内部にリードライト可能な不揮発性メモリを設け、端子を介して外部とデータの送受を可能にした。媒体読取装置にデータ送受用の接点を設けることにより、この不揮発性メモリに読み出

し途中のアドレスや読出順序のプログラム等を記憶することができる。媒体そのものにこのようなデータを記憶しておくことにより、この媒体をどの読取装置にセットされた場合でもこのデータに基づいて読み取りを再開することができ効率的なデータの読み取りを行うことができる。

#### (f) 実施例

第1図はこの発明の実施例であるコンパクトディスク(CD)の外観を示す図である。同図(A)は正面図であり同図(B)は側面図である。CD1の裏面には光学的にデータを記録した記録部1aが形成されており、中央部に設けられた開口部1bを中心に回転する。CD1表面にはEEPROM2が実装されている。実装方法としてはCOB等が適当である。EEPROM2にはデータ送受用およびアドレス指定用の端子3が接続されている。端子3はCD表面に金を蒸着させて形成されている。

第2図は前記EEPROM2に設定されるメモリエリアを示す図である。このメモリエリアには

直前に再生されたときの再生データが記憶される。M1はプログラムフラグである。プログラムフラグは直前の再生でプログラム再生が行われていたか否かを記憶するフラグである。M2はプログラムテーブルである。プログラムテーブルには、操作者が任意に設定したこのCDに記録(録音)されている曲の再生順序が記憶される。M3はポイント記憶エリアである。ポイントはCD再生装置において演奏順を指示する歩進カウンタであり、このポイント記憶エリアM3には直前の再生時に以後に再生された曲順が記憶される。

第3図は同CDを再生するためのCD再生装置の制御部のブロック図である。CDの全体の動作はコントローラ20が制御する。このコントローラ20にはバス21が接続されており、このバス21を介してデータの入力や指示情報の出力を行う。バス21には操作盤22、表示器23、接点24、モータ制御回路25およびピックアップ28が接続されている。操作盤22には第4図に示すようなキーシステムが接続されており、表示器

23も操作盤に隣接するパネル上に設けられている。表示器23はマトリックスの点灯管表示器である。接点24はCDをセットするターンテーブル上に設けられており、セットされたCDが所定位置に停止することにより端子3と接触してデータ等の送受を行う。モータ制御回路25はピックアップ28から入力されるトラッキング信号や同期信号等に基づいてコントローラ20が計算した動作量データに基づきディスク回転モータ26およびトラッキングモータ27を制御する回路である。CDのデータ記録方式は線速度一定方式であるため内側のトラックを再生するときと外側のトラックを再生するときとはCDを回転させる速度が異なる。また、ピックアップの水平方向の移動をサーボ制御することによりトラッキング精度を保たなければならない。モータ制御回路25はこれらの制御を行う。ピックアップが検出したオーディオデータは復調回路29に入力される。オーディオ信号はPCM録音されているため、復調回路がこれをデコードしてアナログの音楽信号に

復調し、これをアンプ30に入力する。このアンプはオーディオ信号を数百ミリボルトから数ボルトに増幅するプリアンプであり、この信号をメインアンプが増幅してスピーカを駆動する。

第4図は前記操作盤22の構成を示す図である。この操作盤22には通常のCDプレーヤ同様プレイキー11、停止キー12、一時停止キー13および逆戻しキー14、速送りキー15が設けられ、さらに、途中再生キー10が設けられている。途中再生キー10は、最後まで再生されず途中でストップされたCDの再生をそのストップされた曲から再開するためのキーである。このキー以外にもリピートキー16、プログラムセットキー17、プログラムオン・オフキー18およびプログラムセット用の曲番指定キー19がこの操作盤に設けられている。リピートキー16はそのとき演奏中の曲1曲をリピートする1曲リピートモードとCD全曲をリピートする全曲リピートモードとを切り換えることができる。プログラムセットキー17がオンされると演奏曲順をセットするプ

ログラムモードに入る。プログラムオンオフキー18はプログラム再生と通常再生(CDに記録されている曲の順序で再生するモード)とを切り換えるキーである。

第5図は同CD再生装置のコントローラ20に設定されるメモリエリアを説明する図である。このメモリエリアにはプログラムフラグM11、プログラムテーブルM12、リピートフラグM13、ポインタM14およびCDデータエリアM15が設定されている。プログラムテーブルM12には利用者が曲番指定キー19を操作して指定した再生順序(プログラム)が記憶され、プログラムフラグM11がセットしているとき(プログラム再生モード時)にこの曲順で再生が行われる。リピートフラグM13は3ステートフラグであり、リセット時にはノンリピートモードを意味し、1がセットされているときには1曲リピートモードを意味し、2がセットされている時には全曲リピートモードを意味する。ポインタM14は、前述したように現在何曲目の再生を行っているかを記

憶する歩進カウンタであり、このレジスタの内容に基づいて再生する曲が検索される。CDデータエリアM15は、CDの記録部1aに記憶されているコントロールデータ(曲数や演奏時間が記憶されている。)を記憶するエリアである。このコントロールデータはCDがセットされたとき、自動的に読み出される。

なおプログラムフラグM11は前記プログラムオンオフキー18がオンされる毎にセットリセットを繰り返し、リピートフラグM13はリピートキー16がオンされる毎に0, 1, 2のデータが繰り返しセットされる。

第6図は同CD再生装置の制御部の動作を示すフローチャートである。

同図(A)はCDがセットされたときの動作を示す。CDがセットされるとまず記録部1aのコントロールトラックを読み出し、CDデータエリアM15に記憶する。このとき同時に表示器23に全曲数と演奏時間を表示する。つぎに接点24の導通状態からCD1の端子3がどの位置にある

かを検出し(n2)、接点24が端子3と正確に接触する位置でCDの回転を停止させる(n3)。この状態でEEPROM2に記憶されているデータを読み出しエリアM1~M3に記憶されているデータを対応するメモリエリア(M11, M12, M14)に記憶する(n4)。この状態でプレイキー11等がオンされるまで待機する。

同図(B)はプログラムセットキー17がオンされたときの動作を示す。このキーがオンされるとプログラムテーブルをクリアして歩進カウンタiに1をセットする(n5)。次に曲番キー19またはプログラムセットキー17がオンされるまで待機し(n6, n7)、曲番キーが押されるとn6→n8に進む。n8では曲番キー19で指定された曲番をプログラムテーブルのi番目エリアに記憶し、iに1を加算して(n9)、n6, n7の待機ルーチンに戻る。プログラムセットキー17が再度オンされるとn7→n10に進み、プログラムテーブルのi番目のエリアにエンドコードを記憶して(n10)リターンする。

同図(C)はプレイキー11がオンされたときの動作を示す。まずポインタに1をセットし(n11)、プログラムフラグがセットしているかリセットしているかをn12で判断する。リセットしているときには順次再生であるためポインタの数值に対応する曲番の曲を検索して(n13)、その曲を再生する(n14)。この演奏中にストップキーや一時停止キーまた送りキー逆戻しキー等がオンされるとそれに対応する動作を実行する。この曲の再生が終了するとリピートフラグが1であるか否かを判断し(n15)、1であれば1曲リピートモードであるためn13にもどる。リピートフラグが1でなければポインタに1を加算し(n16)、これでこの曲が終わりであるか否かを判断する(n17)。順次再生の場合曲の終わりはコントロールデータ(曲数データ)を参照することにより判断することができる。曲が終わりであればM13にもどり、終わりであればn18でリピートフラグが2であるか否かを判断する。リピートフラグが2であれば全曲リピート

を開始する。これによって直前の再生で中断した曲から演奏を再開することができる。

同図(D)はイジェクトキー(図示は省略)がオンされたときの動作を示す。イジェクトキーがオンされるとCDを回転して接点を検出し(n26)、接点の位置でCDを停止させる(n27)。この状態でEEPROM2にプログラムフラグ、プログラムテーブルおよびポインタ(M11, M12, M14)の内容を書き込み(n28)、書き込みののちCDを排出する(n29)。排出されたCDをまたこの再生装置に挿入すればプログラムフラグ、プログラムテーブルおよびポインタの内容が再生装置内の記憶エリアにセットされ演奏途中からの再生やプログラム再生が容易に行われる。

以上の実施例ではCD表面にEEPROMを設け、このEEPROMと再生装置とのデータの送受を接点を介して行うようにしたが、CDに設ける記憶素子はバッテリーバックアップを有するRAMでもよい。またディスク状記憶媒体としては

モードであるため再度n11にもどって上記の動作を繰り返す。リピートフラグが2でなければ終了処理を行ったのち(n19)リターンする。終了処理とはポインタのクリアやディスク回転モード26の停止等である。

一方プログラムフラグがセットされていた場合にはプログラム再生を実行する。まずポインタで示されるプログラムテーブルの欄を読み出し(n20)、この欄のデータがエンドコードであるか否かを判断する(n21)。エンドコードであればn18に進み、エンドコードでなく曲番が記憶されていればその曲番に対応する曲をCD上で検索し(n22)、プレイ動作を実行する(n23)。プレイが終了するとリピートフラグが1であるか否かを判断し(n24)、1であればn22にもどり、1でなければポインタに1を加算して(n25)n21にもどる。

また途中プレイキー10がオンされた場合にはポインタに1をセットせずそのときポインタに記憶されている数値を維持したままn12から動作

、光学式のものに限らず磁気式のものであってもよい。

なお、本発明におけるディスク状記憶媒体とは、磁気ディスク等を保護するためのカートリッジ等も含むものである。したがって、EEPROM、RAM等を第7図に示すようにカートリッジ表面に設けてもよい。

#### (4)発明の効果

以上のようにこの発明のディスク状記憶媒体では読み出し順序や読み出しが中断した場所等を媒体そのものに設けられた不揮発性メモリに記憶しておくことができるため、この媒体をどの読取装置にセットした場合でも前回の読取時のデータを参照することができ効率的な読み取りを行うことができる。

#### 4.図面の簡単な説明

第1図(A)、(B)はこの発明の実施例であるコンパクトディスクの外観を示す図である。第2図は同コンパクトディスクのEEPROMに設定

される記憶エリアを示す図である。

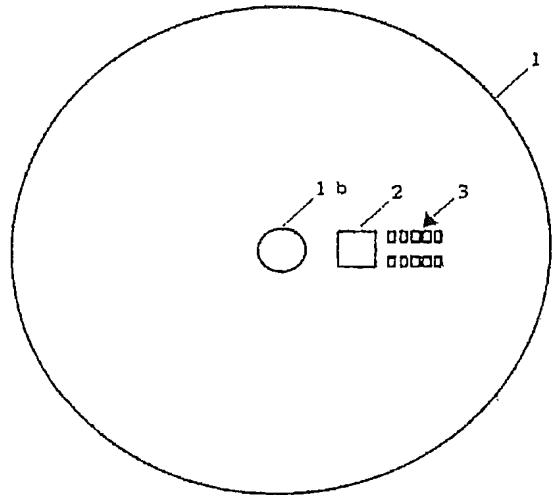
第3図は同コンパクトディスクが再生されるCD再生装置の制御部のブロック図、第4図は同CD再生装置の操作盤の構成を示す図、第5図は同制御部のメモリエリアを説明する図、第6図(A)~(D)は同制御部の動作を示すフローチャートである。

第7図はこの発明の他の実施例を示す図である。

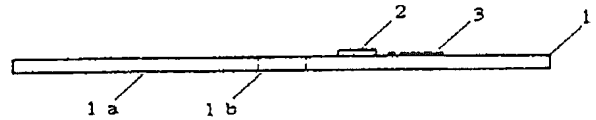
1-コンパクトディスク、2-EEPROM、3-端子。

第 1 図

(A)

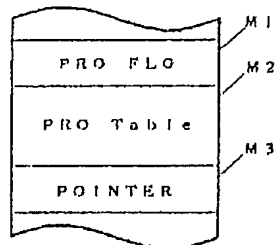


(B)

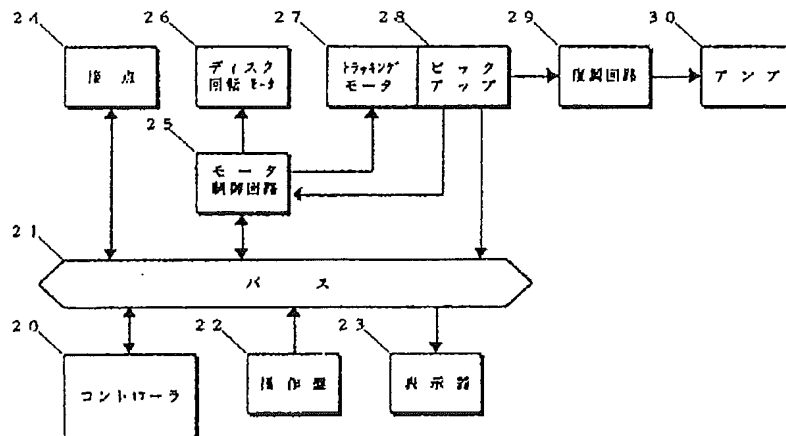


出願人 ヤマハ株式会社  
代理人 弁理士 小森久夫

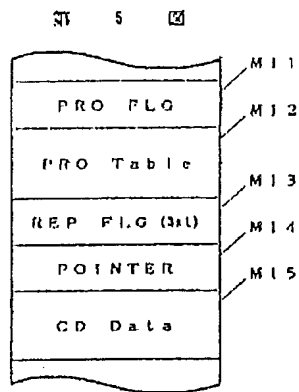
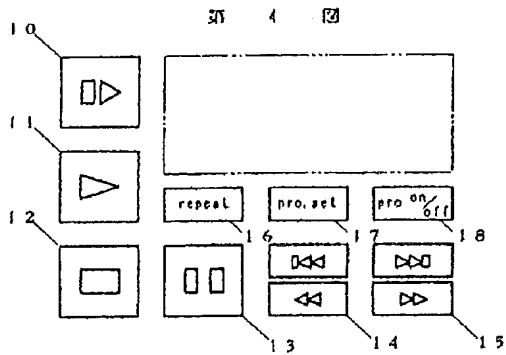
第 2 図



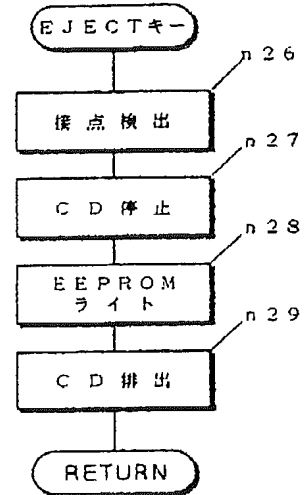
第 3 図



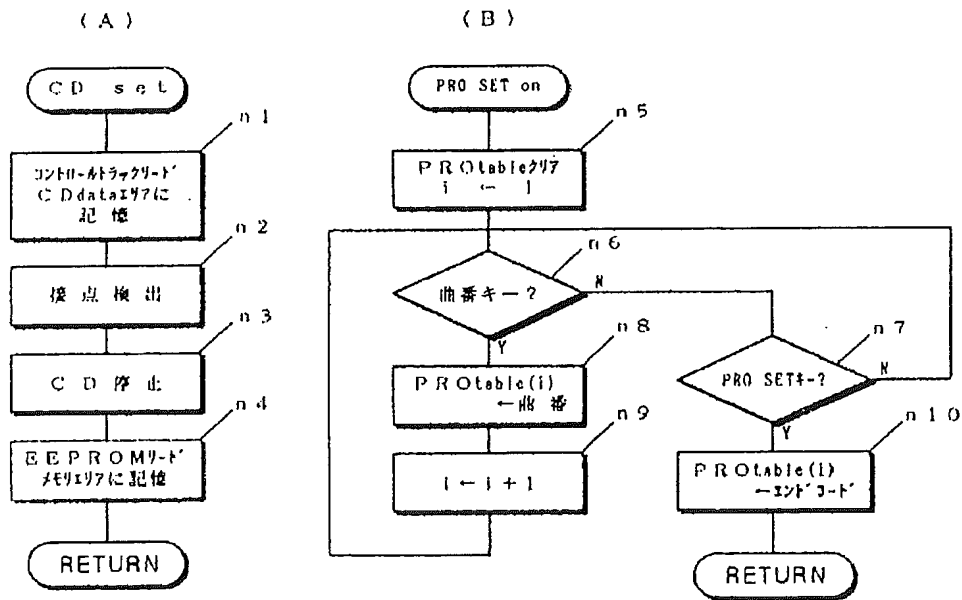


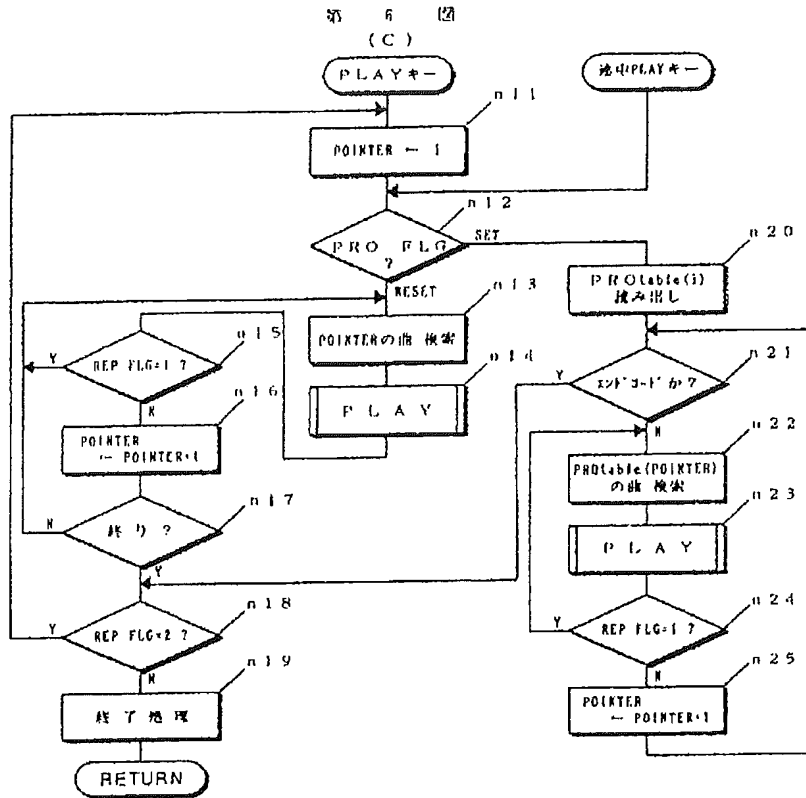


第 6 図 (D)

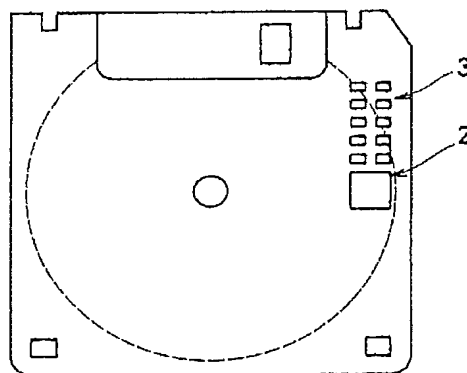


第 6 図





第 7 図



## Partial Translation of Document 1

Jpn. Pat. Appln. KOKAI Publication No. 3-73481

Filing No.: 1-209056

Filing Date: August 11, 1989

Applicant: Yamaha Corporation

Priority: Not Claimed

KOKAI Date: March 28, 1991

Request for Examination: Not filed

Int.Cl.: G11B 23/30

7/24

---

FIG. 5 is a diagram describing a memory area set in a controller 20 of the CD reproduction device. A program flag M11, a program table M12, a repeat flag M13, a pointer M14, and a CD data area M15 are set in the memory area. A reproduction order (program) which the user designates by operating a music number designation key 19 is stored in the program table M12 and when the program flag M11 is set (in a program reproduction mode), the program is reproduced in this music order. The repeat flag M13 is a 3-state flag and indicates a non-repeat mode when the repeat flag M13 is reset, indicates a 1-music repeat mode when the repeat flag M13 is set to 1, and indicates a full-music repeat mode when the repeat flag M13 is set to 2. The pointer M14 is a stepping counter storing what pieces of music is reproduced as described above and reproduced music is retrieved based on a content of the register. The CD data area M15 is an area storing controller data (storing the number of pieces of music and a playing time) stored in a recording part 1a of the CD. The control data is automatically read when the CD is set.

Further, the program flag M11 repeats set and reset every time when the program on/off key 18 is turned on and the repeat flag M13 is repeatedly set to data of 0, 1, and 2 every time when a repeat key 16 is turned on.

Statement of Relevancy

JP 59-195391 was cited in Japanese Application No. 2011-066325 (which also claims priority to the same UK priority document as the present application)

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 59-195391

(43)Date of publication of application : 06.11.1984

(51)Int.Cl.	G11B 27/10	G06F 13/04	G11B 19/02
	G11B 21/08		

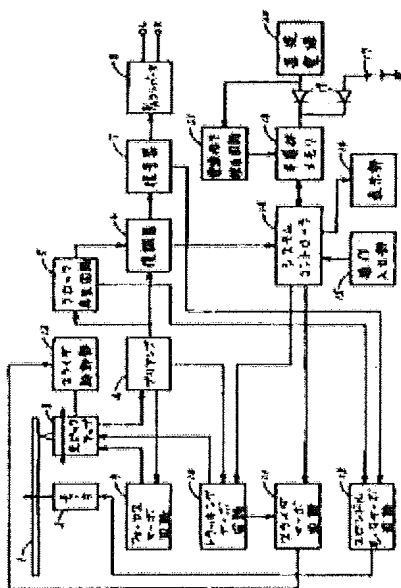
(21)Application number : 58-071600

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 20.04.1983

(72)Inventor : NIWAYAMA MASANORI

## (54) COMPACT DISK PLAYER



### (57)Abstract:

**PURPOSE:** To reproduce a play which is started again with application of a power supply right after the play performed before discontinuation by storing the data on the process of the play and deciding the play that is restarted after the discontinuation of the play based on said data.

**CONSTITUTION:** A function which performs a play again right at the position performed before the discontinuation of the play is considered together with a function which continue the play of the precedent program supplied and operated In such a case, the minimum necessary data to be stored in a semiconductor memory 18 requires the time information (last time information) showing the position that is so far reproduced, the information (program information) on the procedure of the program play and the information (pointer) showing the number of music that is

reproduced during the program play. It is unknown that when the power supply is cut off for the last time and the pointer. Therefore it is necessary to read frequently the latest information out of a disk and transfer it to a semiconductor memory 18. For this purpose, a system controller 14 is used. The memory 18 is also used to store data when the proper power supply is given to a player. This eliminates the necessity for the save of the data.

① 日本国特許庁 (JP)

① 特許出願公開

② 公開特許公報 (A)

昭59—195391

⑤ Int. Cl.<sup>3</sup>  
G 11 B 27/10  
G 06 F 13/04  
G 11 B 19/02  
21/08

識別記号

庁内整理番号  
6507—5D  
7361—5B  
7346—5D  
7541—5D

④ 公開 昭和59年(1984)11月6日

発明の数 1  
審査請求 未請求

(全 12 頁)

⑥ コンパクトディスクプレーヤ

機株式会社京都製作所内

⑦ 特 願 昭58—71600  
⑧ 出 願 昭58(1983)4月20日  
⑨ 発 明 者 庭山正紀  
長岡京市馬場岡所1番地三菱電

⑩ 出 願 人 三菱電機株式会社  
東京都千代田区丸の内2丁目2  
番3号  
⑪ 代 理 人 弁理士 大岩増雄 外2名

明 細 書

1. 発明の名称

コンパクトディスクプレーヤ

2. 特許請求の範囲

(1) コンパクトディスクの演奏経過段階に関するデータ、あるいは該データと演奏方法に関するデータを記憶する記憶手段と、演奏中止後に再開される演奏動作を前記記憶手段に記憶されているデータに基づいて決定する決定手段を有するコンパクトディスクプレーヤ。

(2) 前記演奏中止は電源停止によるものであり、演奏動作の再開は電源再投入によりなされるものであることを特徴とする特許請求の範囲第1項記載のコンパクトディスクプレーヤ。

(3) 電源停止時間が予め定めた制限値以内の場合にのみ前記決定手段の動作が行なわれることを特徴とする特許請求の範囲第2項記載のコンパクトディスクプレーヤ。

(4) 前記決定手段の動作はプレーヤに対し操作入力された命令に基づいて行なわれることを

特徴とする特許請求の範囲第1項記載のコンパクトディスクプレーヤ。

(5) 前記命令は予めプレーヤに操作入力され演奏中止時にも保存されるものであることを特徴とする特許請求の範囲第4項記載のコンパクトディスクプレーヤ。

(6) 前記命令は演奏中止後に再開された演奏開始後に操作入力されたものであることを特徴とする特許請求の範囲第4項記載のコンパクトディスクプレーヤ。

3. 発明の詳細な説明

本発明は光ディスクにPCM化されて記録されている音声信号を再生するコンパクトディスクプレーヤに関するものであり、特にその演奏機能に関する。

コンパクトディスクプレーヤは直径12cm、厚さ1.2mm程度の小さなディスク(コンパクトディスク)にPCM化されて記録されている音声信号を再生するプレーヤであり、そのディスクにおける音声信号の記録形態と相まって高忠実度の再

生を可能にするが、その特徴は単に高忠実度の再生という点に留まらず、任意の曲の頭出しやリビート演奏といった豊富な機能がスピーディに行なわれるという特徴を有する。

なお、前述のような各種機能はディスクに記録されている制御、表示信号を用いることによつて行なわれる。制御、表示信号として記録されている情報にはリードインエリアと呼ばれるディスク内周部分にスタート曲番、エンド曲番、演奏時間、各曲スタート時間があり、一方、音声情報が記録されているプログラムエリアに曲番(曲の番号)、インデックス(曲内小区分)、曲内経過時間、累積経過時間がある。本明細書では、これら8個の情報を「曲番、時間情報」と呼ぶことにする。

ところで、従来のコンパクトディスクプレーヤ(以下「プレーヤ」と称する)において行なわれている任意頭出しやリビート演奏等の特殊再生機能を実施する際に必要な基本的機能は、(I)制御、表示信号を読取る機能と、(II)目的の位置を探索する機能であり、かかる2つの基本的機能

されたPCM信号をアナログの音声信号に変換している。9はフォーカスサーボ回路であつて、プリアンプ4から得られるフォーカスエラー信号によつて信号読取用光ビームの焦点を制御する。10はトラッキングサーボ回路であつて、プリアンプ4から得られるトラッキングエラー信号によつて信号読取用光ビームのディスク1に対する半径方向の動きを制御する。11はスライダサーボ回路であつて、光ピックアップ3のみで追従できないディスク1の半径方向の移動をスライダ駆動部12を制御することでカバーする。13はスピンドルモータサーボ回路であつて、ディスク1の回転が線速度一定(CLV: Constant Linear Velocity と称す)となるようスピンドルモータ2の回転を制御する。14はシステムコントローラであつて、操作入力部15を含めたプレーヤ各部の状態を監視したり、表示部16を含むプレーヤ各部に命令を出して各種動作を行なわせる役割を持つ。

ここで前述の制御、表示信号をディスク読出デ

をCPUなどの高度なコントロール手段と組合せて行なうことにより上記特殊再生機能が達成される。そこで、前記2つの基本的機能を中心に従来のプレーヤの動作を以下に説明しておく。

第1図において、1はディスクであつてスピンドルモータ2によつて回転力を与えられる。3は光ピックアップであつて、光学的読取手段、フォーカスおよびトラッキング調整手段などを有する。4はプリアンプであつて、ディスク1からの読出データを波形整形するとともに、フォーカスエラーおよびトラッキングエラー信号を生成する。5はクロック再生回路であつて、読出データの復調時のクロックを生成する。6は復調器であつて、EFM(Eight-Fourteen Modulation)変調を受けている読出データを8ビット単位のデータに復調するとともに、読出データに含まれるサブコード信号の抽出を行なう。7は復号器であつて誤り訂正、誤り補正、デインタリーブを含む訂正符号の復号およびジッタ吸収動作を行なう。8はD/Aコンバータであつて、復号器7から入力

ータから抽出する基本的機能について詳しく述べる。第2図はディスク読出信号に、繰返し周波数7.35kHzで現われるフレームと呼ぶ単位のフォーマットを示したもので、24チャンネルビット(チャンネルビットはディスク記録信号に関する情報単位)の同期信号(イ)、14チャンネルビットの制御、表示信号(ロ)、336チャンネルビットのデータ(ハ)、112チャンネルビットの誤り訂正用ビット(ニ)、および102チャンネルビットの接続、低周波抑圧用ビット(ホ)の計588チャンネルビットが含まれ、定まった配列で現われる。上記制御、表示信号の14チャンネルビットはEFM変調前の情報単位であるデータビットに換算して8データビットの情報量である。さらに制御、表示信号は98フレームすなわち75Hz(7.35kHz/98=75Hz)で繰返される1つのブロック(サブコーディングブロック)を単位として記録内容が更新される。サブコーディングブロックには2フレーム分のサブコーディング用同期パターンと8種類の情報が含まれ、1

つの種類の情報は、1フレームに1ビットずつ一定の桁に割当てられている。前記曲番、時間情報もこの1つの桁に含まれる。この8種類の情報には曲番、時間情報のほかに、プリエンファシスの有無を示す情報、曲間か曲内かを示す情報などがある。なお、曲番、時間情報が含まれるビットは、チャンネルQと呼ばれ、他の情報記録に用いられることもあり、同じチャンネルQに含まれる識別番号によって区別される。第3図はプログラムエリアでチャンネルQが曲番、時間情報を示す際の記録フォーマットである。同図におけるモードコントロール信号はプリエンファシスの有無を示す情報とステレオ2チャンネルか否かを示す情報で形成されている。ADR1はADR以後のデータが何を表わしているかを区別する情報である。ディスクのリードインエリアでは、ポイントと称すフラグによって区別された各曲のスタート時間(累積経過時間)、プログラムの最初の曲番、プログラムの最終の曲番、全演奏時間の情報が3回繰返されている。曲番、時間情報の抽出は、まず第1図のク

ロック再生回路5から得られるクロックによってディスク読出値をビット同期化し、復調器6はフレーム同期信号検出およびサブコーディング用同期パターンの検出を行ない、この同期信号によってEFM復調データからサブコードを分離抽出する。システムコントローラ14は必要に応じて8ビットのサブコード全部あるいは特定ビットをサブコーディングブロック分入力し、符号誤り検出を行なって誤りがあれば新たにサブコードを入力する。チャンネルQに対応するビット列が曲番、時間情報であることを前記識別番号で確認して曲番、時間情報の入力が終わる。第4図のシステムコントローラの動作を中心とした時間読取りのフローチャートを示す。第4図④のデータ並べ替えは96ビット(98-2)分のシリアルデータをCPUで処理しやすいよう内容ごとに並べ替える動作をさす。さて任意頭出し機能といった特殊再生を実現する上で不可欠な第2の基本的機能は、先にも述べたように目的の位置を探索する機能であって、これがスピーディに行なわれることも重

要である。曲番、時間情報の形式で指定された目的の位置を探索するには、光ピックアップ3のトレース位置を移動する手段とこの移動量を決定する手段とが必要となる。

トレース位置の移動には螺旋状の信号トラックをはずれることなく、そのままトレースして目的の位置まで行く方法とトラックをジャンプして移動する方法があるが、前者は確実であっても通常再生と同じ時間がかかることから、後者と組合わせて用いられている。ジャンプ動作は、トラッキングサーボ回路10に対しパルス(ジャンプパルスと称す)を印加し、光ピックアップ3のトレース位置を強制移動させることで行なわれるが、高速移動を実現するため大きなジャンプパルスとともに急停止用の逆極性パルス(ブレーキパルスと称す)を組合わせている。システムコントローラ14から出力されたフォワードジャンプ(ディスク外周方向ジャンプ)命令あるいはリバースジャンプ(ディスク内周方向ジャンプ)命令の回数分トラックジャンプが実行される。但し、光ピック

アップ3内の半径方向のトレース位置可動量には限界があり、これをスライダサーボ回路11とスライダ駆動部12とで自動的に補っている。

次に目的位置までの移動量決定であるが、時間情報として与えられる現在位置と目的位置との距離はシステムコントローラ14で大まかに計測し、その結果に基づいてジャンプ命令を出力し、次の位置において曲番、時間情報を読取って再び目的位置までの距離を算出してジャンプ命令を出力するという動作を繰返すという方法が採られる。もし目的位置のごく近傍であれば、ジャンプせずにそのままトレースすることで目的位置に達するのを待つ。

目的位置探索動作をシステムコントローラ14の処理を中心にして表わしたのが第5図であるが、ここで①および②の処理は、曲の頭出し動作においては決して曲の先頭の音が割られないよう目的位置を曲開始の1秒前に設定するとともに、目的位置を累積経過時間表現(第5図では絶対時間と称す)に変換している。なお、第5図においてt



$t_{a0}$  は現在の曲のスタート絶対時間、 $t_{a1}$  は現在の位置の曲内時間、 $t_{a2}$  は現在の位置の絶対時間、 $t_{b0}$  は目的の曲のスタート絶対時間、 $t_{b1}$  は目的の位置の曲内時間、 $t_{b2}$  は目的の位置の絶対時間をそれぞれ表わし、また  $N_1 < N_2 < N_3 < N_4$ 、 $T_1 < T_2 < T_3 < T_4 < T_5 < T_6$  であるとする。目的の曲のスタート時間はリードインデータを予め読取って記憶してある(図示せず)。④のPLLロック検出はトレース位置の移動に対しCLV制御が追従したことを確認する処理、⑤は第4図に示した時間読取処理、⑥と⑦は移動方向を決定する処理で、この結果をジャンプパルスの極性を示すグラフPに与え、⑧から⑩は現在位置と目的位置の時間差 $|\Delta t|$ からジャンプパルスの数を決定する処理であって、特に⑨および⑩は現在位置が目的位置と同じか、ごく近傍、すなわち探索終了を判断し、また⑧の $T_2 > |\Delta T|$ はジャンプすると目的位置を飛び越えてしまう場合を判断し、⑧は決定されたジャンプパルス数Nと方向Pを出力する処理である。

スピーディな機能を実現し、この点でランダムアクセスのできないカセットテープに対し優位性を持つ。しかし、カセットテープあるいはオープンリールテーププレーヤにおいては、テープの巻取り状態が過去の再生終了位置を保存していることから循環再投入を行なった場合あるいはテープをプレーヤから取出し再びプレーヤに装着した場合でも、同じ演奏内容を聞くことも、あるいは特別の操作をする必要もないというメリットを有しているのに対し、従来のコンパクトディスクプレーヤにおいては一度電源を切断したり、あるいはディスク着脱操作を実行すると、その前に再生していたディスクに対する情報は揮発してしまい、再びディスクの1曲目から再生するか、あるいは前記頭出し操作を行なう必要がある。このとき操作者が以前何曲目まで再生が終了していたかを記憶していない場合は、その位置を捜すためにいくつもの曲の内容をサンプリング的に聞くという操作が必要となつて、かなりの手数と時間がかかってしまう。またディスク面に記載されたタイトル部

④と⑤は音声のミュートイングに関する処理であつて、探索開始位置と目的位置が同じか、ごく近傍のときはジャンプもミュートイングも行なわれないようになっている。

以上述べた制御信号読取機能と目的位置探索機能をシステムコントローラ14と組合わせることで特殊な再生動作が実現される。たとえば、ディスク内に順番に並べられた曲を任意な順番で再生する機能(以下プログラム演奏と称す)では、操作入力部15から定められた手法で演奏順番が入力され、システムコントローラ14はこれらプログラム情報を記憶回路(図示せず)に格納する。次にシステムコントローラ14は上記目的位置探索(ここでは頭出し)を実行して再生を開始させ、1つの曲が終了することにより上記記憶回路から次の曲の情報を取り込んでいくという動作を繰返すので、プログラム演奏が実現できるのである。

さて、コンパクトディスクプレーヤは以上述べたようにディスクに記録されているサブコード、すなわち制御、表示信号を用いることで豊富かつ

分を見て曲名の確認などを行なおうとしてディスクをプレーヤから取出したとすれば上と同様の結果になってしまう。かかる従来のコンパクトディスクプレーヤの問題は車載用コンパクトディスクプレーヤにおいて一層顕著になる。すなわち車載用プレーヤは車の直流電源を使用するが、車においてはエンジン始動時にエンジン以外への電源供給が停止されるものが大部分であること、運転者が車を降りるときエンジンはもちろん電源が切断されること、ほとんど毎日ごく短い時間だけ車を利用し、その際、音楽を聞くという使われ方が多いことなどを考えれば、従来のコンパクトディスクプレーヤでは操作性が極めて悪いといえる。特に運転者にとって、プレーヤの操作に手数と時間がかかるとは、運転の安全上好ましくないという重大な問題となる。

それゆえに、本発明の主たる目的は、電源解除などによるプレーヤの演奏中止後に電源再投入などにより再開される演奏動作を中止前の演奏に引き続く状態で再現できるようにした機能を持つコ

コンパクトディスクプレーヤを提供することにある。

本発明の他の目的は、かかる連続的再生機能の実行、不実行の選択を可能にしたコンパクトディスクプレーヤを提供することである。

本発明は、要約すればコンパクトディスクの演奏経過段階に関するデータ、あるいは該データと演奏方法（たとえばプログラム演奏）に関するデータを記憶する記憶手段と、演奏中止後に再開される演奏動作を前記記憶手段に記憶されているデータに基づいて決定する決定手段を設けたものである。

この発明の上述の目的およびその他の目的と特徴は、図面を参照して行なう以下の詳細な説明から一層明らかとなる。

第6図は本発明の第1の実施例の概略ブロック図であって、第1図と同一符号は同一内容を示す。第6図において、17は電池であって、半導体メモリ18のバックアップを行なう。19はダイオードであって、電源スイッチ（図示せず）を通じて供給される電源から生成される直流電源20と

としては充電式の電池あるいは大容量コンデンサ、もしくは電源スイッチなどを介さず常に導通状態にする構成としてもよい。また半導体メモリ18のみをバックアップせずにシステムコントローラ14のCPU部分またはその他の回路を含めてバックアップするように構成してもよい。

さて、半導体メモリ18によって保存されるべきデータに関しては、電源再接入後に連続して行なわれる機能の選択で異なるが、本実施例では、以前再生していた位置から再び演奏する（以下「シーケンシャルプレイ」と称す）機能と以前操作入力されたプログラム演奏（前述）が引き続き行なわれる機能とを考えるとすれば、最低限必要なデータは、以前再生していた位置を示す時間情報（以下「ラストタイム情報」と称す）、プログラム演奏の手順の情報（以下「プログラム情報」と称す）、およびプログラム演奏のときはどの順番の曲を再生していたかを示す情報（「ポイント」と称す）が必要となる。このうちラストタイムとポイントについてはいつ電源切断が行なわれるか

電池17とのORをとるOR回路を構成している。

21は電源低下検出回路であってデータ保存を完全に行なう役目をなす。電池17を内蔵することで半導体メモリ18（揮発性）は等価的に不揮発性メモリとして使用できる。電源切断などによって直流電源20の出力が低下したときのみ半導体メモリ18にデータを退避するようにしてもよいが、本実施例ではプレーヤに本来の電源供給がされたときにも半導体メモリ18をデータの格納レジスタと用いることとし、これによってデータ退避動作を不要としている。但し、直流電源20低下的にCPUなどで構成されるシステムコントローラ14が半導体メモリ18に対し誤ったアクセスを行なう危険があるので、電源低下検出回路21がハードウェア的に半導体メモリ18へのアクセスの禁止を行なうと同時にメモリ回路以外への電流流出による電力消費を防ぐ。前記半導体メモリ18としては不揮発性半導体メモリを使用してもよく、その場合にはバックアップ用電池が不要となる利点が生じる。一方、バックアップ手段

不明であるため、ディスクから頻りに最新情報を跳取って半導体メモリ18に転送しておく必要があり、システムコントローラ14がこの働きを行なうよう構成されているものとする。

電源切断時はハードウェア的手段によって上記ラストタイム情報およびプログラム情報は保存されるので、システムコントローラ14は第1図の場合と特に異なる処理は行なわないが、電源再接入が行なわれたときは特別な処理を行なう。

第7図はシステムコントローラ14の動作を中心としたシーケンシャルプレイ動作のフローチャートである。ここで $t_{min}$ は最初の曲のスタート絶対時間、 $t_{max}$ は全演奏時間、 $A_i$ はポイント $[A_i]$ はレジスタ $A_i$ の内容、 $[A_p]$ はポイントが示すアドレスの内容をそれぞれ表わす。本フローチャート以前でシステムコントローラ14自身の初期化およびプレーヤ各部の初期化動作などは終了しているものとし、またフローチャート内では表示のための処理などは省いている。第8図は半導体メモリ18内に設けられたラストタイ

ムの記憶レジスタA<sub>0</sub>、プログラム情報の記憶レジスタA<sub>1</sub>～A<sub>N</sub>およびポイントの記憶レジスタA<sub>P</sub>の構成を示し、プログラム演奏はA<sub>1</sub>の示す曲の次にA<sub>2</sub>の示す曲を演奏するという順番である。ラストタイムおよびプログラム情報は各々曲番と絶対時間(累積経過時間)が記憶され、プログラム情報における絶対時間は各々の曲のスタート絶対時間を意味する。ポイントにはプログラム演奏がA<sub>1</sub>～A<sub>N</sub>のどのアドレスの段階にあるかをA<sub>1</sub>～A<sub>N</sub>のアドレスで記憶し、このポイントおよびラストタイムはその内容が0(リセット)ならば、全プログラム演奏が以前に終了していることを示す。なおプログラム演奏が指定されていない場合には、以前にディスク全体を演奏終了していることを意味する。

第7図において③～⑥はレジスタA<sub>0</sub>～A<sub>N</sub>の内容チェックを行っており、A<sub>0</sub>がリセットされている場合、またはA<sub>0</sub>の内容がリードインあるいはリードアウトの位置を示す場合はシーケンシャルプレイを行わない。A<sub>0</sub>の内容すなわち

ラストタイムの位置を⑦で探索して再生を開始し、⑧で現在の曲の終了が検出されるまで⑨、⑩で最新の曲番、時間情報を読取りA<sub>0</sub>へ格納する。曲の終わりを検出するとプログラム演奏が否かを⑪で判定し、プログラム演奏であれば⑫でポイントの内容(アドレス)を1だけインクリメントし、⑬で次に演奏すべき曲の有無を判断して演奏を終了するか、あるいは次の曲の探索に進む処理を行なう。一方、プログラム演奏でない場合は、⑭においてディスクの最終の曲か否かを判断し、最終の曲であれば演奏を終了し、最終の曲でなければ⑮に戻って次曲の演奏を行なう。⑯はプログラム演奏のときは全手順の終了、プログラム演奏でない場合は、ディスクの最終曲の演奏終了をA<sub>0</sub>のリセットによって保存する処理である。なお、第7図における⑦「探索」および⑩「時間読取り」の処理は各々第5図および第4図に対応する。

さて以上シーケンシャルプレイ動作について述べたが、シーケンシャルプレイを自動的に実行することで操作性が向上することは前述のとおりで

あるが、常に本動作が求められるとは限らないので次にのべる実施例にその対策を示す。

電源再投入時にシーケンシャルプレイを行わずに特定の初期状態あるいは初期動作を行なうことも可能なようにシーケンシャルプレイ動作の実行、非実行操作入力手段を備えておくことと便利である。かかる手段によりシーケンシャルプレイが選択的に実現できるようにした第2実施例としては、(I)機械的ロック可能なシーケンシャルプレイ実行/非実行のスイッチを有し、このスイッチが非実行である場合は前記実施例におけるラストタイム用レジスタA<sub>0</sub>をリセットしておくか、逆に、A<sub>0</sub>の内容を無視するという機能をシステムコントローラ14に付加する。(II)アンロック式のシーケンシャルプレイ実行/非実行スイッチと、半導体メモリ18にさらにシーケンシャルプレイ実行/非実行命令レジスタとを有し、このスイッチが押されるとこのレジスタの内容を論理的に反転させ、メモリの内容に応じてシーケンシャルプレイ動作の実行/非実行を決定するような処理

をシステムコントローラ14に付加するという方法がある。前者は機械的に後者は電気的にシーケンシャルプレイ実行/非実行命令を記憶している(フローチャート略)。

次に第3実施例として短時間の電源切断に対してのみシーケンシャルプレイを行ない、長時間の電源切断の電源再投入においてはシーケンシャルプレイは行なわずに初期化された動作を行なう機能について以下に述べる。これはたとえば車載プレーヤにおいて、エンジン始動時の電源切断や短時間の停車に対してのみシーケンシャルプレイを行なう機能である。第9図はかかる機能を有する第3実施例の要部を示すブロック回路図であって第5図に対しシステムコントローラ14周辺を除いて同一であり同一符号は同一内容である。

第9図において21は抵抗であって、これを通じて半導体メモリ18への給電を行なう。22はダイオードであって、逆流防止用であり、23は大容量のコンデンサで短時間のバックアップ電源となり、24はコンパレータであって、半導体メ

メモリ18の電源電圧が25の基準電圧に比べ高いときはハイレベル("H"と示す)、逆のときはローレベル("L"と示す)をシステムコントローラ14に出力する。プレーヤへの給電が正帯で直流電源20の出力が正規の場合、半導体メモリ18へは抵抗21およびダイオード22を通じて電流が供給されるが、プレーヤへの給電が停止したり、給電電圧が低下すると、ダイオード22の作用で直流電源20とメモリ回路は分離される。この場合半導体メモリ18の電源電圧はコンデンサ23の充電容量により次第に低下するが、半導体メモリ18は或る程度までの電源低下に対してはその内容を保持する。コンパレータ24は、半導体メモリ18の電源電圧の低下を基準電圧25と比較することでタイマとしての動作を行なうと同時に基準電圧25を半導体メモリ18の内容保持限界電圧以上に選ぶことで、メモリの内容保持に対する補償を与えている。この場合、タイマ(換言すれば時間検出手段)は図示の実施例に拘泥することなく、周波数カウンタなどのディジタ

ル的検出手段で構成してもよい。第3実施例におけるシステムコントローラ14の処理を示したのが第10図のフローチャートであり、電源再投入時の初期化の後直ちに①でコンパレータ24の出力を検出し、これが"H"であればシーケンシャルプレイを行ない、一方"L"であれば電源停止が一定時間を越えたとして第8図における全レジスタA<sub>0</sub>~A<sub>n</sub>、およびA<sub>p</sub>をリセットし、初期化されたプレーヤ動作を行なう(A<sub>0</sub>がリセットされるとシーケンシャルプレイをしないのは前述のとおりである)。電源再投入後の抵抗21によるコンデンサ23への充電速度は遅くなるように選ばれ、システムコントローラ14がコンパレータ24の出力をチェックする際にはコンデンサ23の電圧は電源再投入直前の値とほとんど変わらないようにしている。

次に第11図は第4実施例のフローチャートを示しており、ここでは電源再投入時シーケンシャルプレイ実行命令が与えられず、このため一度初期化された演奏動作(たとえば1曲目から順番に

演奏する)を行なってもそれが一定時間内であれば、その間に操作入力されたシーケンシャルプレイ実行命令を受入れて実行する機能を持たせている。かかる機能は操作者の不注意、あるいは意思変更を補償する機能として有効である。なお、ここでは第6図のプレーヤに前記第2実施例で述べたシーケンシャルプレイの実行/非実行を操作入力する機械的ロック式スイッチのシーケンシャルプレイスイッチを設けておくものとする。

第11図は上記機能を実現するシステムコントローラの処理を示して、第7図の処理を変更したものであり、記号は同一のものは同一内容であることを示す。

第11図において、電源再投入後、①でまずリードインデータを読取り、②~⑤でラストタイム情報(A<sub>0</sub>の内容)がリセットされているか、あるいは有効な時間情報でないと判断すると⑥以後の処理でディスク1曲目から演奏することになり、一方、②~⑤でラストタイム情報が有効と判断すればA<sub>0</sub>のラストタイム情報をA<sub>0</sub>なるアドレス

を持ったレジスタに退避させ(A<sub>0</sub>は不揮発性でなくてもよい)、⑥でシーケンシャルプレイスイッチの状態を見る。ここでシーケンシャルプレイスイッチがON(シーケンシャルプレイ実行命令)であれば、⑦でタイマをリセット、スタートさせA<sub>0</sub>の示す再生位置を探索して演奏させ、逆にシーケンシャルスイッチがOFF(非実行命令)であれば、⑧を経てディスクの1曲目からの演奏を始める。ここでフラグSはシーケンシャルプレイスイッチの状態を示しS=0で同スイッチOFF、S=1で同スイッチONである。

⑨でディスク1曲目あるいはA<sub>0</sub>の示す曲を探索して演奏開始すると⑩、⑪で常に新しい曲番、時間情報をA<sub>0</sub>に書き込む一方、⑫でタイマの時間経過をチェックし、タイマの時間Tが制限時間T<sub>max</sub>未満であれば⑬でシーケンシャルプレイスイッチの状態を見る。⑭は以前のスイッチの状態Sと今回のスイッチの状態S'の排他的論理和をとってスイッチの状態の変化を検出し、状態が変化していなければ(S⊕S'=0)特に処理せず、

一方、スイッチの状態に変化があれば次の処理を行なう。以前シーケンシャルプレイが実行され ( $S = 1$ )、今度スイッチがOFF ( $S' = 0$ ) となった場合はシーケンシャルプレイを止め、 $A_0$  ハディスク1曲目のデータを伝送して1曲目からの演奏を行なう(㉔~㉕)。一方、以前シーケンシャルプレイは実行されておらず ( $S = 0$ )、今度スイッチがON ( $S' = 1$ ) となった場合は、㉔で  $A_0$  に退避した正規のラストタイム情報があれば、㉕で  $A_0$  の内容を  $A_0$  に復帰させてシーケンシャルプレイを行ない、一方、㉔で  $A_0$  がリセットされていればそのまま演奏を続ける。㉕でタイム時間が制限時間  $T_{max}$  を越えると判断すると、その後シーケンシャルスイッチの状態は無視する。㉕以後の処理は第7図の場合と同様であるので説明は略す。なお第11図では第7図における操作入力スイッチなどの処理は説明上省いた。以上述べた実施例において、頭出し動作など単発的操作が与えられ、その動作が完結しないうちに電源停止が生ずる場合への対応として、電源停止時に操

作命令そのものを記憶しておくことも考えられる。なお、コンパクトディスク規格が変更されても、時間、曲番などに関する情報がディスクに記録されている限り、本発明は適用可能である。

以上のように本発明によれば、電源を切って再度電源を投入した場合などのように演奏の中止を含む場合であっても中止の前と後で連続的な演奏が可能となり、演奏再開時に改めて選曲する手順が不要となる効果があり、とりわけ車載用のコンパクトディスクプレーヤのごとく中止の機会が多く、しかも安全運転上から操作手数を減らす必要のあるものにおいて有効である。

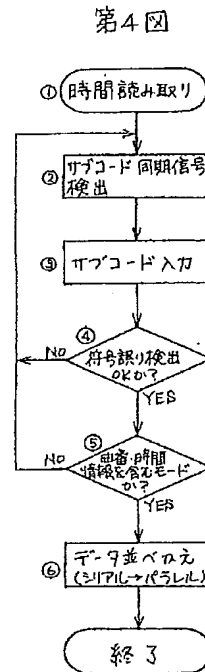
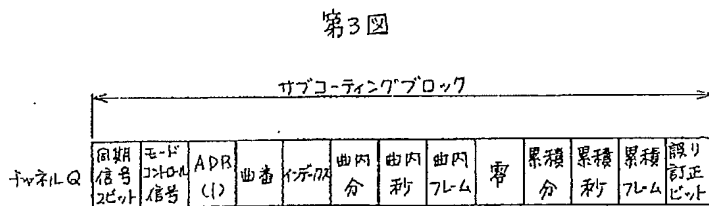
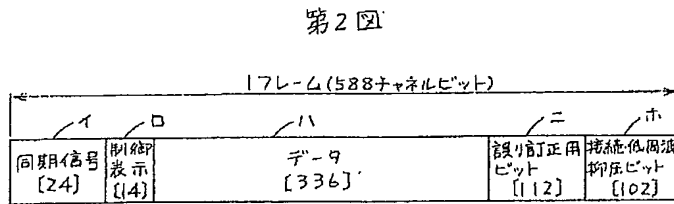
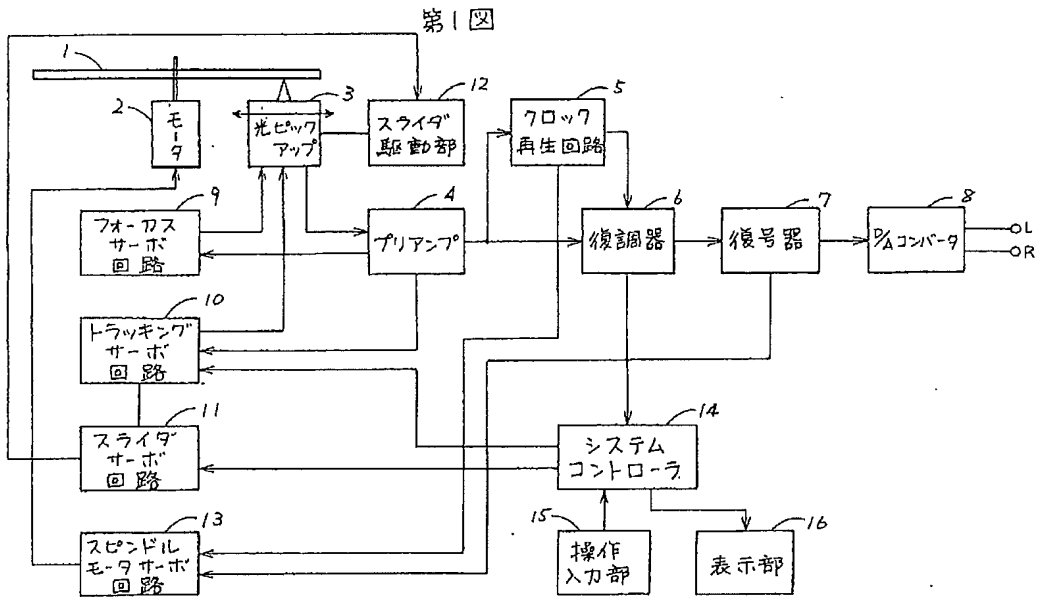
#### 4. 図面の簡単な説明

第1図は従来のコンパクトディスクプレーヤのブロック図である。第2図および第3図はコンパクトディスクに記録されている番号を説明するための図である。第4図は従来のコンパクトディスクプレーヤにおける時間跳取りのフローチャートを示す図であり、第5図は同じく探索のフローチャートを示す図である。第6図は本発明を実施し

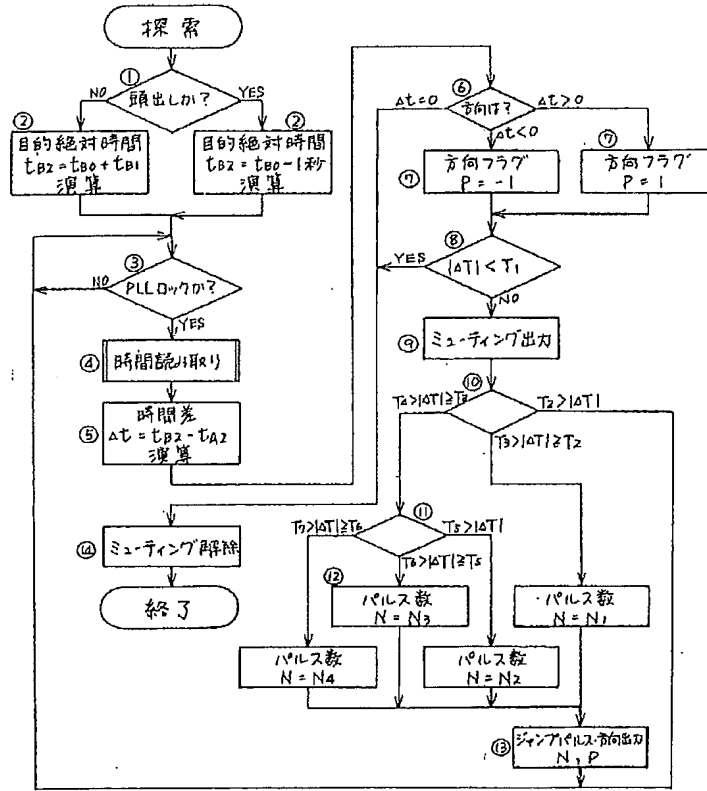
たコンパクトディスクプレーヤのブロック図であり、第7図はその動作のフローチャートを示す図、第8図は第5図の一部の構成を説明する図である。第9図は本発明の他の実施例における要部の構成を示すブロック回路図であり、第10図はその説明図である。第11図は本発明のさらに他の実施例の動作のフローチャートを示す図である。

図において、1はコンパクトディスク、3は光ピックアップ、5はクロック再生回路、6は復調器、7は復号器、14はシステムコントローラ、17は電池、18は半導体メモリ、20は直流電源、21は電源低下検出回路である。

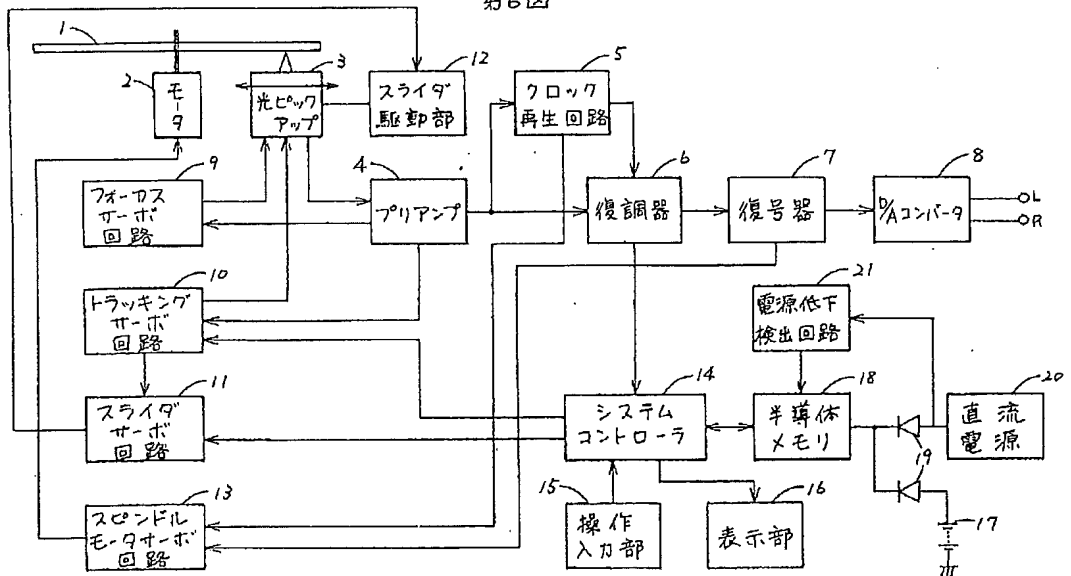
代 理 人      大 岩 増 雄



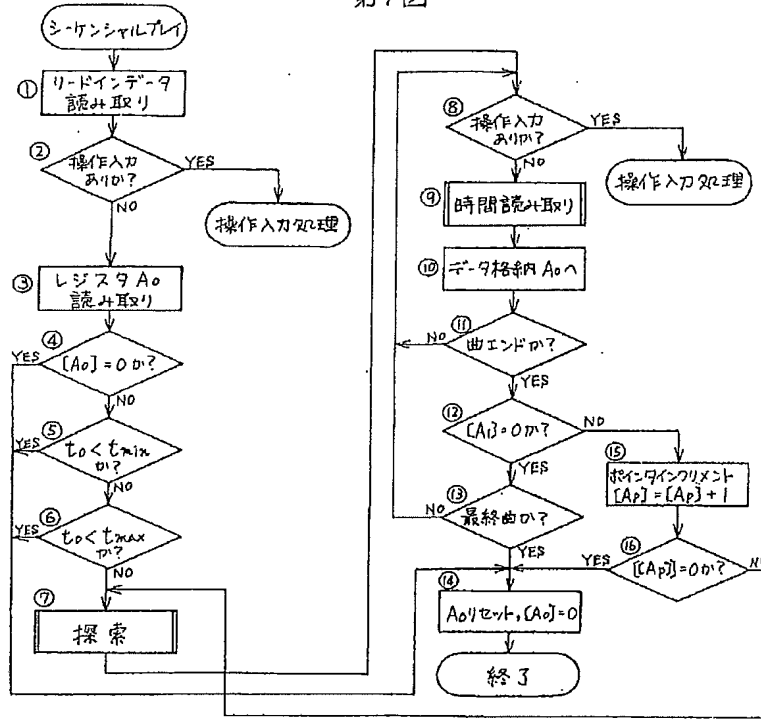
第5図



第6図



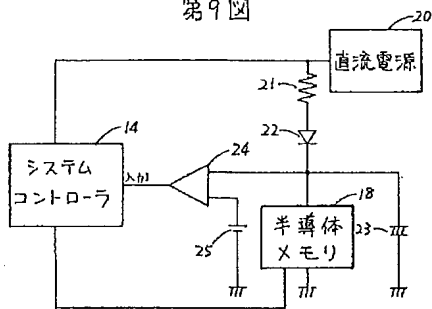
第7図



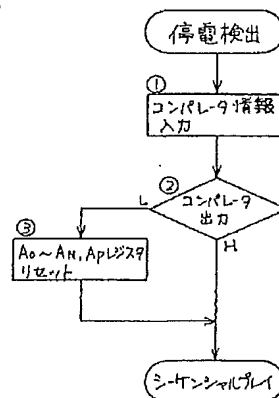
第8図

アドレス	曲番	絶対時間
A <sub>0</sub>	P <sub>0</sub> (=P <sub>N</sub> )	t <sub>0</sub>
A <sub>1</sub>	P <sub>1</sub>	t <sub>1</sub> (スタート位置)
A <sub>2</sub>	P <sub>2</sub>	t <sub>2</sub> "
A <sub>3</sub>	P <sub>3</sub>	t <sub>3</sub> "
⋮	⋮	⋮
A <sub>M</sub>	P <sub>M</sub>	t <sub>M</sub> "
⋮	⋮	⋮
A <sub>N</sub>	P <sub>N</sub>	t <sub>N</sub> "
A <sub>P</sub>	A <sub>M</sub> (PFLS)	

第9図

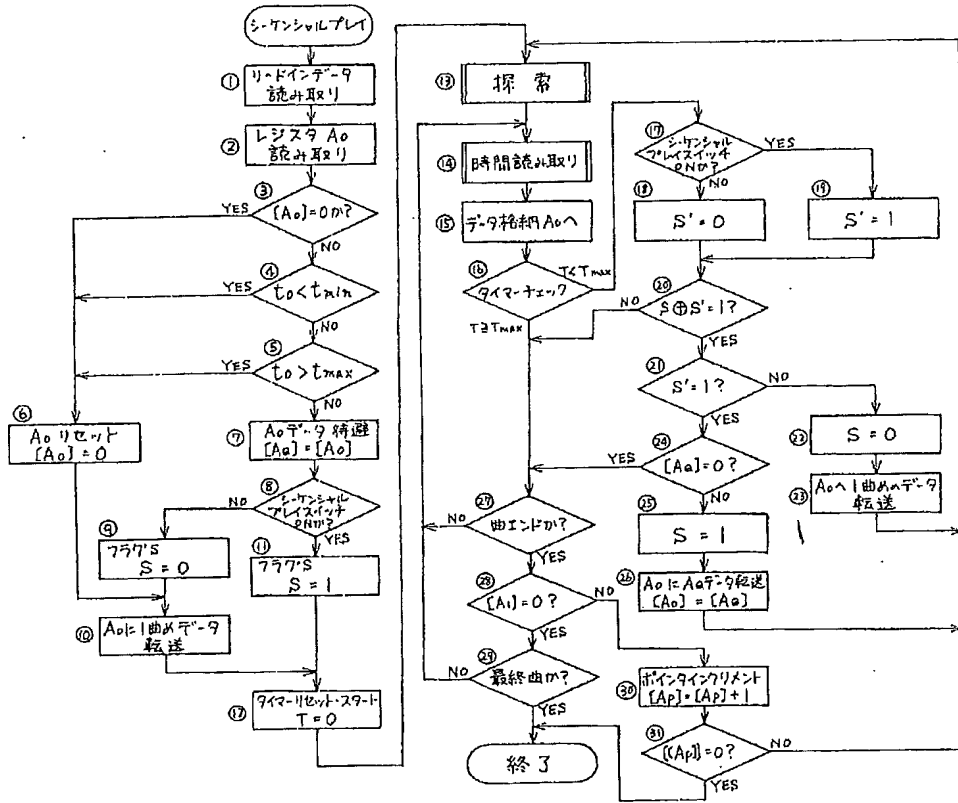


第10図





第11図



Partial Translation of Document 2

Jpn. Pat. Appln. KOKAI Publication No. 59-195391

Filing No.: 58-71600  
Filing Date: April 20, 1983  
Applicant: Mitsubishi Electric Corporation  
Priority: Not Claimed  
KOKAI Date: November 6, 1984  
Request for Examination: Not filed  
Int.Cl.: G11B 27/10  
G06F 13/04  
G11B 19/02  
21/08

---

In FIG. 7, (3) to (8) check contents of registers  $A_0$  to  $A_N$ , and when  $A_0$  is reset or when the content of  $A_0$  indicates a read-in location or a read-out location, a sequential play is not performed. Reproduction starts by retrieving the content of  $A_0$ , that is, a location of a last time through (7), and latest music number and time information is read and stored in  $A_0$  through (9) and (10) until termination of a current music is retrieved in (11). When the termination of the music is detected, whether the program is played is judged in (12) and when the program is played, a content (address) of the pointer is incremented by 1 in (15) and whether there is music to be played next is judged in (16) to terminate playing or retrieve the next music. Meanwhile, when the program is not played, whether the music is the final music of the disk is judged in (13) and when the music is the final music, playing is terminated and when the music is not the final music, the process returns to (8) to play the next music. (14) is processing that saves termination of the full procedures when the program is played and termination of playing the final music of the disk when the program is not played by resetting  $A_0$ . Further, 'retrieval' of (7) and 'time reading' of (9) in FIG. 7 correspond to FIGS. 5 and 4, respectively.

Although a sequential playing operation has been described above, operability is improved by automatically executing a sequential play as described above, but the operation is not always required. A countermeasure thereof will be described in an embodiment to be described below.

It is convenient to install execution and non-execution operation inputting means of the sequential playing operation so as to perform a specific initial state or initial operation without performing the sequential play when power is reinput. As a second embodiment to selectively implement the sequential play by the means, (i) a sequential play execution/non-execution switch which is mechanically lockable is provided, and in case of the non-execution switch, a function to set the last time register  $A_0$  in the embodiment, while disregard the content of  $A_0$  is added to a system controller 14. (ii) An unlock type sequential play execution/non-execution switch and a sequential play execution/non-execution command register are provided in a semiconductor memory 18, and when the switch is pressed, a content of the register is logically inverted and processing such as determining execution/non-execution of the sequential playing operation is added to the system controller 14 depending on the content of the memory. The former mechanically stores the sequential play execution/non-execution command and the latter electrically stores the sequential play execution/non-execution command (a flowchart is omitted).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/438,754	04/03/2012	Patrick Sandor Racz	87790-837121 (000160US)

**CONFIRMATION NO. 3525**

**POWER OF ATTORNEY NOTICE**

20350  
KILPATRICK TOWNSEND & STOCKTON LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834



Date Mailed: 11/20/2013

**NOTICE REGARDING CHANGE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 11/14/2013.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/ddinh/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/438,754	04/03/2012	Patrick Sandor Racz	4037-0003

**CONFIRMATION NO. 3525**

**POA ACCEPTANCE LETTER**

42624  
DAVIDSON BERQUIST JACKSON & GOWDEY LLP  
4300 WILSON BLVD., 7TH FLOOR  
ARLINGTON, VA 22203



Date Mailed: 11/20/2013

**NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 11/14/2013.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ddinh/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/438,754, 04/03/2012, 2887, 1591, 4037-0003, 28, 6

CONFIRMATION NO. 3525

REPLACEMENT FILING RECEIPT

42624
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203



Date Mailed: 11/20/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Inventor(s)

Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;
Hermen-ard Hulst, Amsterdam, NETHERLANDS;

Applicant(s)

Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;
Hermen-ard Hulst, Amsterdam, NETHERLANDS;

Assignment For Published Patent Application

Smartflash LLC, Tyler, TX

Power of Attorney: The patent practitioners associated with Customer Number 42624

Domestic Priority data as claimed by applicant

This application is a CON of 13/212,047 08/17/2011 PAT 8336772
which is a CON of 12/943,872 11/10/2010 PAT 8118221
which is a CON of 12/014,558 01/15/2008 PAT 7942317
which is a CON of 11/336,758 01/19/2006 PAT 7334720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB2000/004110 10/25/2000

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

UNITED KINGDOM 9925227.2 10/25/1999 No Access Code Provided

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper Request to

**Retrieve Electronic Priority Application(s)** (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

**If Required, Foreign Filing License Granted:** 04/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/438,754**

**Projected Publication Date:** Not Applicable

**Non-Publication Request:** No

**Early Publication Request:** No

**Title**

DATA STORAGE AND ACCESS SYSTEMS

**Preliminary Class**

235

**Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:** No

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	04/03/2012	Patrick Sandor Racz	4037-0003	3525

42624 7590 11/22/2013  
DAVIDSON BERQUIST JACKSON & GOWDEY LLP  
4300 WILSON BLVD., 7TH FLOOR  
ARLINGTON, VA 22203

EXAMINER
----------

LE, THIEN MINH

ART UNIT	PAPER NUMBER
----------	--------------

2887

MAIL DATE	DELIVERY MODE
-----------	---------------

11/22/2013

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



**Supplemental  
Notice of Allowability**

<b>Application No.</b> 13/438,754	<b>Applicant(s)</b> RACZ ET AL.	
<b>Examiner</b> Thien M. Le	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to \_\_\_\_\_.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 40-60 and 64-70. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/oph/index.jsp](http://www.uspto.gov/patents/init_events/oph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All    b)  Some    \*c)  None of the:
1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. 09/697,534.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in **ABANDONMENT** of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  **CORRECTED DRAWINGS** ( as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.  
**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  **DEPOSIT OF and/or INFORMATION** about the deposit of **BIOLOGICAL MATERIAL** must be submitted. Note the attached Examiner's comment regarding **REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL**.

**Attachment(s)**

- |  |  |
|--|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Examiner's Amendment/Comment                             |
| 2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date _____    | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material | 7. <input type="checkbox"/> Other _____.   |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____ .                    |  |

### **DETAILED ACTION**

The present application is being examined under the pre-AIA first to invent provisions.

This Office Action is needed to update the status of a claim for foreign priority. Accordingly, the certified copies of the priority documents have been received in Application No. 09/697,534.

### ***Allowable Subject Matter***

Claims 40-60 and 64-70 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to disclose a handheld multimedia terminal comprising: a wireless interface, a non-volatile memory, a program store, a processor, a user interface, a display, and having the processor control codes as recited in claims 40. Claim 41 recites a data supply server having similar limitations as recited in claim 40. The prior art also fails to disclose a computer system and a method of providing and downloading multimedia contents having limitations as recited in claims 50, 57 and 64.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thien M. Le whose telephone number is (571)272-2396. The examiner can normally be reached on Monday - Friday from 7:30am - 4:00pm.

Art Unit: 2887

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve S. Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thien M. Le/  
Primary Examiner, Art Unit 2887



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
13/438,754 04/03/2012 Patrick Sandor Racz 4037-0003 3525

42624 7590 12/09/2013
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

LE, THIEN MINH

ART UNIT PAPER NUMBER

2887

MAIL DATE DELIVERY MODE

12/09/2013

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



**UNITED STATES DEPARTMENT OF COMMERCE  
U.S. Patent and Trademark Office**

Address : COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

<b>APPLICATION NO./ CONTROL NO.</b>	<b>FILING DATE</b>	<b>FIRST NAMED INVENTOR / PATENT IN REEXAMINATION</b>	<b>ATTORNEY DOCKET NO.</b>
13/438,754	03 April, 2012	RACZ ET AL.	4037-0003

DAVIDSON BERQUIST JACKSON & GOWDEY LLP 4300 WILSON BLVD., 7TH FLOOR ARLINGTON, VA 22203	<b>EXAMINER</b>	
	Thien M. Le	
	<b>ART UNIT</b>	<b>PAPER</b>
	2887	20131205

DATE MAILED:

**Please find below and/or attached an Office communication concerning this application or proceeding.**

Commissioner for Patents

The information disclosure statement filed on 11/19/2013 has been considered.

/Thien M. Le/  
Primary Examiner, Art Unit 2887

Receipt date: 11/19/2013

13438754 - GAI: 2887

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		13438754	
	Filing Date		2012-04-03	
	First Named Inventor	Patrick Sandor Racz		
	Art Unit	2887		
	Examiner Name	LE, THIEN MINH		
	Attorney Docket Number	4037-0003		

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup> j	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1	3-73481	JP		1991-03-28		(Partial Translation)	<input type="checkbox"/>
	2	59-195391	JP		1984-11-06		(Partial Translation)	<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS								Remove
---------------------------------	--	--	--	--	--	--	--	--------

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		13438754	13438754 - GAU: 2887
	Filing Date		2012-04-03	
	First Named Inventor	Patrick Sandor Racz		
	Art Unit		2887	
	Examiner Name	LE, THIEN MINH		
	Attorney Docket Number		4037-0003	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
	1	Decision of Rejection dated July 23, 2013 in Japanese Application No. 2011-066325 (which also claims priority to the same UK priority document as the present application)	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

**EXAMINER SIGNATURE**

Examiner Signature	/Thien Le/	Date Considered	12/05/2013
--------------------	------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number	13438754	13438754 - GAU: 2887
	Filing Date	2012-04-03	
	First Named Inventor	Patrick Sandor Racz	
	Art Unit	2887	
	Examiner Name	LE, THIEN MINH	
	Attorney Docket Number	4037-0003	

**CERTIFICATION STATEMENT**

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

**OR**

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

**SIGNATURE**

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ Michael R. Casey /	Date (YYYY-MM-DD)	2013-11-19
Name/Print	Michael R. Casey	Registration Number	40294

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**



**Privacy Act Statement**

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

20350                      7590                      09/17/2013  
**KILPATRICK TOWNSEND & STOCKTON LLP**  
 TWO EMBARCADERO CENTER  
 EIGHTH FLOOR  
 SAN FRANCISCO, CA 94111-3834

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	04/03/2012	Patrick Sandor Racz	87790-837121 (000160US)	3525

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	<del>SMALL</del> Undiscounted	\$ <del>1,780</del> 1,780	\$0	\$890	\$ <del>890</del> 890	12/17/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, THIEN MINH	2887	235-380000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>1 <u>Davidson Berquist</u></p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,</p> <p>2 <u>Jackson &amp; Gowdey, LLP</u></p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.</p> <p>3 _____</p>
---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Smartflash, LLC	Tyler, Texas

Please check the appropriate assignee category or categories (will not be printed on the patent) :     Individual     Corporation or other private group entity     Government

<p>4a. The following fee(s) are submitted:</p> <p><input checked="" type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input checked="" type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number <u>501860</u> (enclose an extra copy of this form).</p>
--	---

5. **Change in Entity Status** (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

---

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

---

Authorized Signature           / Michael R. Casey /           Date           December 10, 2013            
Typed or printed name           Michael R. Casey           Registration No.           40,294          

---

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

---

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17612470
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	42624
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	4037-0003
<b>Receipt Date:</b>	10-DEC-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	11:08:44
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	20131210_Issue_Form.pdf	114332 <small>339c275c2b0105e8c28934597de352e3de9a514c</small>	no	2

### Warnings:

### Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

JPW

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

20350 7590 09/17/2013
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834



Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Form with fields for Depositor's name, Signature, and Date.

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE.

Table with 3 columns: EXAMINER, ART UNIT, CLASS-SUBCLASS.

Form with 2 main sections for correspondence address and printing on patent front page.

Form section 3: ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT.

Please check the appropriate assignee category or categories (will not be printed on the patent):

Form section 4a and 4b: Fee(s) submitted and Payment of Fee(s).

Adjustment date: 12/12/2013 SDIRETA2
12/12/2013 SDENB02 00000022 13438754 -890.00 OP
01 FC:2501
12/12/2013 SDIRETA2 00000002 501860 13438754
01 FC:1501 890.00 DA 890.00 OP

5. Change in Entity Status (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature                     / Michael R. Casey /                    

Date                     December 10, 2013                    

Typed or printed name                     Michael R. Casey                    

Registration No.                     40,294                    

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Adjustment date: 12/12/2013 SDIREIA2  
12/11/2013 SDENB082 00000022 13438754  
01 FC:2501 -890.00 OP



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	16626311
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	20350
<b>Filer:</b>	Benjamin J. Holt/Annette Valdivia
<b>Filer Authorized By:</b>	Benjamin J. Holt
<b>Attorney Docket Number:</b>	87790-837121 (000160US)
<b>Receipt Date:</b>	19-AUG-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	18:31:08
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$670
RAM confirmation Number	4946
Deposit Account	201430
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754
<b>Filing Date:</b>	03-Apr-2012
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Filer:</b>	Benjamin J. Holt/Annette Valdivia
<b>Attorney Docket Number:</b>	87790-837121 (000160US)

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
Petition Fee-37CFR 1.17(h) (Group II)	2464	1	70	70
Request for Continued Examination	2801	1	600	600

**Pages:**

**Claims:**

**Miscellaneous-Filing:**

**Petition:**

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

Adjustment date: 12/13/2013 SDIRETA1  
 08/20/2013 INTERSW 00004946 201430 13438754  
 02-FC:2801 600.00 CR

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>670</b>



APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	01/14/2014	8628009	4037-0003	3525

42624 7590 12/24/2013  
DAVIDSON BERQUIST JACKSON & GOWDEY LLP  
4300 WILSON BLVD., 7TH FLOOR  
ARLINGTON, VA 22203

### ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

#### **Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)** (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Patrick Sandor Racz, Saint Heller, UNITED KINGDOM;  
Hermen-ard Hulst, Amsterdam, NETHERLANDS;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](http://SelectUSA.gov).

**REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL  
(Submitted Only via EFS-Web)**

Application Number	13/438,754	Filing Date	2012-04-03	Docket Number (if applicable)	4037-0003	Art Unit	2887
First Named Inventor	Patrick Sandor Racz			Examiner Name	Thien Minh Le		

**This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.**  
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

**SUBMISSION REQUIRED UNDER 37 CFR 1.114**

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_

Other \_\_\_\_\_

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other \_\_\_\_\_

**MISCELLANEOUS**

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months \_\_\_\_\_  
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other \_\_\_\_\_

**FEES**

**The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 501860

**SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED**

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Michael R. Casey/	Date (YYYY-MM-DD)	2013-12-23
Name	Michael R. Casey	Registration Number	40294

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re PATENT Application of:		Confirmation No.:	3525
Patrick Sandor Racz		Attorney Docket:	4037-0003
Appl. S.N.:	13/438,754	Group Art Unit:	2887
Filing Date:	April 3, 2012	Examiner:	Le, Thien Minh
Title:	DATA STORAGE AND ACCESS SYSTEMS	Date:	12/31/2013

**INFORMATION DISCLOSURE STATEMENT**

Hon. Commissioner of Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. § 1.56, the attention of the Patent and Trademark Office is hereby directed to the reference(s) listed on the attached PTO-1449. One copy of each non-U.S. Patent reference is attached. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the reference(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

The submission of any document herewith, which is not a statutory bar, is not intended that any such document constitutes prior art against any of the claims of the present application or is considered to be material to patentability as defined in 37 C.F.R. § 1.56(b). Applicants do not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference against the claims of the present application.



This Information Disclosure Statement (IDS) is being filed within three (3) months of the U.S. filing date OR before the mailing date of a first Office Action on the merits after an RCE. No certification or fee is required.

This IDS includes a copy of a subpoena from an on-going litigation (Smartflash LLC, et al., v. Apple Inc., et al., Civil Action No. 6:13-CV-00447-MHS-KNM, Eastern District of Texas). That subpoena identifies two patents, U.S. Patent Nos. 6,226,618 and 6,389,538, and the modified PTO-1449 includes those two patents and the patents cited on the face of those patents. On information and belief, the file histories of those two patents are not available on the IFW system, so copies of any foreign and/or non-patent literature cited therein are not included herewith.

**CHARGE STATEMENT: Deposit Account No. 501860, order no. 4037-0003.**

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached

**This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.**

CUSTOMER NUMBER

42624

Davidson Berquist Jackson & Gowdey LLP  
4300 Wilson Blvd., 7th Floor,  
Arlington Virginia 22203  
Main: (703) 894-6400 • FAX: (703) 894-6430

Respectfully submitted,

By: / Michael R. Casey /

---

Michael R. Casey  
Registration No.: 40,294

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 1 of 4

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	1-1	US-4200770	Apr-80	Hellman et al.
	1-2	US-4218582	Aug-80	Hellman et al.
	1-3	US-4272810	Jun-81	Gates et al.
	1-4	US-4405829	Sep-83	Rivest et al.
	1-5	US-4424414	Jan-84	Hellman et al.
	1-6	US-4463387	Jul-84	Hashimoto et al.
	1-7	US-4528643	Jul-85	Freeny, Jr.
	1-8	US-4731840	Mar-88	Mniszewski et al.
	1-9	US-4757534	Jul-88	Matyas et al.
	1-10	US-4782529	Nov-88	Shima
	1-11	US-4796220	Jan-89	Wolfe
	1-12	US-4803725	Feb-89	Horne et al.
	1-13	US-4809327	Feb-89	Shima
	1-14	US-4825306	Apr-89	Robers
	1-15	US-4868687	Sep-89	Penn et al.
	1-16	US-4868877	Sep-89	Fischer
	1-17	US-4878246	Oct-89	Pastor et al.
	1-18	US-4879747	Nov-89	Leighton et al.
	1-19	US-4905163	Feb-90	Garber et al.
	1-20	US-4926479	May-90	Goldwasser et al.
	1-21	US-4944006	Jul-90	Citta et al.
	1-22	US-4995082	Feb-91	Schnorr
	1-23	US-5005200	Apr-91	Fischer
	1-24	US-5130792	Jul-92	Tindell et al.
	1-25	US-5159634	Oct-92	Reeds, III
	1-26	US-5191573	Mar-93	Hair

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 2 of 4

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	2-1	US-5214702	May-93	Fischer
	2-2	US-5220604	Jun-93	Gasser et al.
	2-3	US-5224163	Jun-93	Gasser et al.
	2-4	US-5224166	Jun-93	Hartman, Jr.
	2-5	US-5260788	Nov-93	Takano et al.
	2-6	US-5261002	Nov-93	Perlman et al.
	2-7	US-5276901	Jan-94	Howell et al.
	2-8	US-5315658	May-94	Micali
	2-9	US-5319705	Jun-94	Halter et al.
	2-10	US-5347580	Sep-94	Molva et al.
	2-11	US-5355302	Oct-94	Martin et al.
	2-12	US-5369705	Nov-94	Bird et al.
	2-13	US-5371794	Dec-94	Diffie et al.
	2-14	US-5388211	Feb-95	Hornbuckle
	2-15	US-5412717	May-95	Fischer
	2-16	US-5420927	May-95	Micali
	2-17	US-5497421	Mar-96	Kaufman et al.
	2-18	US-5509071	Apr-96	Petrie, Jr. et al.
	2-19	US-5519778	May-96	Leighton et al.
	2-20	US-5537475	Jul-96	Micali
	2-21	US-5557541	Sep-96	Schulhof et al.
	2-22	US-5581479	Dec-96	McLaughlin et al.
	2-23	US-5588060	Dec-96	Aziz
	2-24	US-5592664	Jan-97	Starkey
	2-25	US-5604804	Feb-97	Micali
	2-26	US-5606617	Feb-97	Brands

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 3 of 4

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	3-1	US-5636139	Jun-97	McLaughlin et al.
	3-2	US-5646992	Jul-97	Subler et al.
	3-3	US-5646998	Jul-97	Stambler
	3-4	US-5649187	Jul-97	Hornbuckle
	3-5	US-5666420	Sep-97	Micali
	3-6	US-5673316	Sep-97	Auerbach et al.
	3-7	US-5675734	Oct-97	Hair
	3-8	US-5706347	Jan-98	Burke et al.
	3-9	US-5710887	Jan-98	Chelliah et al.
	3-10	US-5745574	Apr-98	Muftic
	3-11	US-5765152	Jun-98	Erickson
	3-12	US-5796841	Aug-98	Cordery et al.
	3-13	US-5864620	Jan-99	Pettitt
	3-14	US-5892900	Apr-99	Ginter et al.
	3-15	US-5915025	Dec-99	Taguchi et al.
	3-16	US-5925127	Jul-99	Ahmad
	3-17	US-5982892	Nov-99	Hicks et al.
	3-18	US-5991399	Nov-99	Graunke et al.
	3-19	US-5999629	Dec-99	Heer et al.
	3-20	US-6064739	May-00	Davis
	3-21	US-6098056	Aug-00	Rusnak et al.
	3-22	US-6275936	Aug-01	Kyojima et al.
	3-23			
	3-24			
	3-25			
	3-26			

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

Sheet 4 of 4

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	4-1	Smartflash LLC v. Apple Inc., Civil Action 6:13-CV-00447-MHS-KNM, Subpoena to Testify	
	4-2		
	4-3		
	4-4		
	4-5		
	4-6		
	4-7		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754			
<b>Filing Date:</b>	03-Apr-2012			
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS			
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz			
<b>Filer:</b>	Michael R. Casey			
<b>Attorney Docket Number:</b>	4037-0003			
Filed as Large Entity				
<b>Utility under 35 USC 111(a) Filing Fees</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
RCE - 2nd and Subsequent Request	1820	1	1700	1700
<b>Total in USD (\$)</b>				<b>1700</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17790913
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	42624
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	4037-0003
<b>Receipt Date:</b>	31-DEC-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	16:16:42
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1700
RAM confirmation Number	2984
Deposit Account	501860
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)



Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	20131223_RCE_4037-0003.pdf	697605	no	3
			ffd2d35d169b1f1ecd69bd94155427e128a31eaf		
<b>Warnings:</b>					
<b>Information:</b>					
2	Transmittal Letter	20131231_IDS_Transmittal.pdf	135928	no	2
			03f3ef2d675c17cfd1dadbd4b8ad5462c31b3c004		
<b>Warnings:</b>					
<b>Information:</b>					
3	Information Disclosure Statement (IDS) Form (SB08)	20131231_1449_modified.pdf	63540	no	4
			42748ebabf6ae755647f15898e457387c07078bd		
<b>Warnings:</b>					
<b>Information:</b>					
This is not an USPTO supplied IDS fillable form					
4	Non Patent Literature	NP0000.pdf	1353075	no	14
			21b87beeb4f7dca1c7800d2f6250ed8a1f66ab5e		
<b>Warnings:</b>					
<b>Information:</b>					
5	Fee Worksheet (SB06)	fee-info.pdf	29965	no	2
			dd455c40c9e8b5a871ef18b1f34c56fbb81f0a28		
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			2280113		

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

Electronic Petition Request	<b>PETITION TO WITHDRAW AN APPLICATION FROM ISSUE AFTER PAYMENT OF THE ISSUE FEE UNDER 37 CFR 1.313(c)</b>
Application Number	13438754
Filing Date	03-Apr-2012
First Named Inventor	Patrick Racz
Art Unit	2887
Examiner Name	THIEN LE
Attorney Docket Number	4037-0003
Title	DATA STORAGE AND ACCESS SYSTEMS

An application may be withdrawn from issue for further action upon petition by the applicant. To request that the Office withdraw an application from issue, applicant must file a petition under this section including the fee set forth in § 1.17(h) and a showing of good and sufficient reasons why withdrawal of the application from issue is necessary.

APPLICANT HEREBY PETITIONS TO WITHDRAW THIS APPLICATION FROM ISSUE UNDER 37 CFR 1.313(c).

A grantable petition requires the following items:

- (1) Petition fee; and
- (2) One of the following reasons:
  - (a) Unpatentability of one or more claims, which must be accompanied by an unequivocal statement that one or more claims are unpatentable, an amendment to such claim or claims, and an explanation as to how the amendment causes such claim or claims to be patentable;
  - (b) Consideration of a request for continued examination in compliance with § 1.114 (for a utility or plant application only); or
  - (c) Express abandonment of the application. Such express abandonment may be in favor of a continuing application, but not a CPA under 37 CFR 1.53(d).

Petition Fee

<input type="radio"/> Small Entity
<input type="radio"/> Micro Entity
<input checked="" type="radio"/> Regular Undiscounted

Reason for withdrawal from issue

- One or more claims are unpatentable
- Consideration of a request for continued examination (RCE) (List of Required Documents and Fees)
- Applicant hereby expressly abandons the instant application (any attorney/agent signing for this reason must have power of attorney pursuant to 37 CFR 1.32(b)).

RCE request, submission, and fee.

- I certify, in accordance with 37 CFR 1.4(d)(4) that:  
 The RCE request, submission, and fee have already been filed in the above-identified application on 2014.01.02
- Are attached.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

- An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application.
- An attorney or agent registered to practice before the Patent and Trademark Office, acting in a representative capacity.
- A sole inventor
- A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application
- A joint inventor; all of whom are signing this e-petition

Signature	/ Michael R. Casey /
Name	Michael R Casey
Registration Number	40294

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13438754
<b>Filing Date:</b>	03-Apr-2012
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Filer:</b>	Michael R. Casey
<b>Attorney Docket Number:</b>	4037-0003

Filed as Large Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
Petition fee- 37 CFR 1.17(h) (Group III)	1464	1	140	140

**Pages:**

**Claims:**

**Miscellaneous-Filing:**

**Petition:**

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

**Extension-of-Time:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>140</b>



UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

Decision Date : December 31, 2013

In re Application of :

Patrick Racz

DECISION ON PETITION

UNDER CFR 1.313(c)(2)

Application No : 13438754

Filed : 03-Apr-2012

Attorney Docket No : 4037-0003

This is an electronic decision on the petition under 37 CFR 1.313(c)(2), filed December 31, 2013, to withdraw the above-identified application from issue after payment of the issue fee.

The petition is **GRANTED**.

The above-identified application is withdrawn from issue for consideration of a submission under 37 CFR 1.114 (request for continued examination). See 37 CFR 1.313(c)(2).

**Petitioner is advised that the issue fee paid in this application cannot be refunded. If, however, this application is again allowed, petitioner may request that it be applied towards the issue fee required by the new Notice of Allowance.**

Telephone inquiries concerning this decision should be directed to the Patent Electronic Business Center (EBC) at 866-217-9197.

This application file is being referred to Technology Center AU 2887 for processing of the request for continuing examination under 37 CFR 1.114.

Office of Petitions

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17790938
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	42624
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	4037-0003
<b>Receipt Date:</b>	31-DEC-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	16:22:37
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$140
RAM confirmation Number	3048
Deposit Account	501860
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)



Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition automatically granted by EFS	petition-request.pdf	31447 827c95f6108e720fcccbb2575fdc895d5f7437c	no	2

### Warnings:

### Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30108 7dc3f54aae25cee201e45c6e909ae68e0be26bc1	no	2
---	----------------------	--------------	---	----	---

### Warnings:

### Information:

**Total Files Size (in bytes):** 61555

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

#### **New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

#### **National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

#### **New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 1 of 1

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	1-1	US-6226618	May 2001	Downs et al.
	1-2	US-6389538	May 2002	Downs et al.
	1-3			
	1-4			
	1-5			
	1-6			
	1-7			
	1-8			
	1-9			
	1-10			
	1-11			
	1-12			
	1-13			
	1-14			
	1-15			
	1-16			
	1-17			
	1-18			
	1-19			
	1-20			
	1-21			
	1-22			
	1-23			
	1-24			
	1-25			
	1-26			

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17791169
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	42624
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	4037-0003
<b>Receipt Date:</b>	31-DEC-2013
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	16:37:18
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	20131231_1449_modified-2.pdf	54352 <small>9e7b5a13fb346eac876f615a30326cf1547c6f00</small>	no	1

### Warnings:

### Information:

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

## PATENT WITHDRAWAL NOTICE

DATE WITHDRAWN

1/2/2014

WITHDRAWAL NUMBER

23978

The following application has been **WITHDRAWN** from the  
1/14/2014 issue.

SERIAL NO.

13438754

PATENT NUMBER

8628009

TITLE

DATA STORAGE AND ACCESS SYSTEMS

NAME AND ADDRESS

PATRICK SANDOR RACZ, ET AL  
SAINT HELLER, UNITED KINGDOM

REASON FOR WITHDRAWAL

Auto-petition to withdraw - Granted.

APPROVED

/Kimberly Terrell/, Manager

Patent Publication Branch  
Office of Data Management

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 1 of 3

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	1-1	US-5103392	Apr-91	Mori
	1-2	US-5530235	Jun-96	Stefik
	1-3	US-5629980	May-97	Stefik
	1-4	US-5634012	May-97	Stefik
	1-5	US-5638443	Jun-97	Stefik
	1-6	US-5715403	Feb-98	Stefik
	1-7	US-5790423	Aug-98	Lau
	1-8	US-5915019	Jun-99	Ginter
	1-9	US-5926624	Jul-99	Katz et al.
	1-10	US-5982891	Nov-99	Ginter et al.
	1-11	US-6055314	Apr-2000	Spies
	1-12	US-6170060	Jan-01	Mott et al.
	1-13	US-6223291	Apr-01	Puhl et al.
	1-14	US-6282653	Aug-01	Berstis et al.
	1-15	US-6367019	Apr-02	Ansell et al.
	1-16	US-6385596	May-02	Wiser et al.
	1-17	US-6434535	Aug-02	Kupka et al.
	1-18	US-6697948	Feb-04	Rabin et al.
	1-19	US-6829711	Dec-04	Kwok et al.
	1-20	US-7191153	Mar-07	Braitberg et al.
	1-21	US-7225160	May-07	Stefik et al.
	1-22	US-7233948	Jun-07	Shamoon et al.
	1-23	US-7249382	Jul-07	Kawell, Jr. et al.
	1-24	US-7263497	Aug-07	Wiser et al.
	1-25	US-7315829	Jan-08	Tagawa et al.
	1-26	US-7523072	Apr-2009	Stefik et al.

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 2 of 3

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	2-1	US-7636691	Dec-2009	Maari
	2-2			
	2-3			
	2-4			
	2-5			
	2-6			
	2-7			
	2-8			
	2-9			
	2-10			
	2-11			
	2-12			
	2-13			
	2-14			
	2-15			
	2-16			
	2-17			
	2-18			
	2-19			
	2-20			
	2-21			
	2-22			
	2-23			
	2-24			
	2-25			
	2-26			

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 3 of 3	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	3-1	Smartflash LLC v. Apple Inc., Civil Action 6:13-CV-00447-MHS-KNM, Defendants' Disclosure of Prior Art, dated Jan. 13, 2014	
	3-2		
	3-3		
	3-4		
	3-5		
	3-6		
	3-7		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17924787
<b>Application Number:</b>	13438754
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	3525
<b>Title of Invention:</b>	DATA STORAGE AND ACCESS SYSTEMS
<b>First Named Inventor/Applicant Name:</b>	Patrick Sandor Racz
<b>Customer Number:</b>	42624
<b>Filer:</b>	Michael R. Casey
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	4037-0003
<b>Receipt Date:</b>	15-JAN-2014
<b>Filing Date:</b>	03-APR-2012
<b>Time Stamp:</b>	17:47:55
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	20140115_IDS_Transmittal.pdf	135850 <small>2a34b2a12b51e5481f339e1b473d59bcc8661090</small>	no	2

### Warnings:

### Information:

2	Information Disclosure Statement (IDS) Form (SB08)	20140115_1449.pdf	60547	no	3
			33ff9311806b6ff0ae5bc7fcbd7b59d372ce36443		

**Warnings:**

**Information:**

This is not an USPTO supplied IDS fillable form

3	Non Patent Literature	NP0000.pdf	110252	no	7
			e9e30a1d22f4e7a31fe26f3f9b2350fe765c3a		

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	306649
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re PATENT Application of:		Confirmation No.:	3525
Patrick Sandor Racz		Attorney Docket:	4037-0003
Appl. S.N.:	13/438,754	Group Art Unit:	2887
Filing Date:	April 3, 2012	Examiner:	Le, Thien Minh
Title:	DATA STORAGE AND ACCESS SYSTEMS	Date:	01/15/2014

**INFORMATION DISCLOSURE STATEMENT**

Hon. Commissioner of Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. § 1.56, the attention of the Patent and Trademark Office is hereby directed to the reference(s) listed on the attached PTO-1449. One copy of each non-U.S. Patent reference is attached. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the reference(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

The submission of any document herewith, which is not a statutory bar, is not intended that any such document constitutes prior art against any of the claims of the present application or is considered to be material to patentability as defined in 37 C.F.R. § 1.56(b). Applicants do not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference against the claims of the present application.

This Information Disclosure Statement (IDS) is being filed within three (3) months of the U.S. filing date OR before the mailing date of a first Office Action on the merits after an RCE. No certification or fee is required.

This IDS includes a copy of US patents cited in Defendants' Disclosure of Prior Art in an on-going litigation (Smartflash LLC, et al., v. Apple Inc., et al., Civil Action No. 6:13-CV-00447-MHS-KNM, Eastern District of Texas). The non-patent literature cited therein, if material and available, will be submitted separately.

**CHARGE STATEMENT: Deposit Account No. 501860, order no. 4037-0003.**

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached

**This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.**

CUSTOMER NUMBER

42624

Davidson Berquist Jackson & Gowdey LLP  
4300 Wilson Blvd., 7th Floor,  
Arlington Virginia 22203  
Main: (703) 894-6400 • FAX: (703) 894-6430

Respectfully submitted,

By: / Michael R. Casey /

Michael R. Casey  
Registration No.: 40,294



**PRIORITY DOCUMENT EXCHANGE**

**FAILURE STATUS REPORT**

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 9925227.2 to which priority is claimed has FAILED on 01/24/2014.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

[pdx@uspto.gov](mailto:pdx@uspto.gov) (email)

Priority Document Exchange Website: [http://www.uspto.gov/patents/process/file/pdx/pdx\\_index.jsp](http://www.uspto.gov/patents/process/file/pdx/pdx_index.jsp)



NOTICE OF ALLOWANCE AND FEE(S) DUE

42624 7590 01/27/2014
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER
LE, THIEN MINH
ART UNIT PAPER NUMBER

2887

DATE MAILED: 01/27/2014

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

13/438,754 04/03/2012 Patrick Sandor Racz 4037-0003 3525

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional UNDISCOUNTED \$0 \$0 \$1780 \$0 04/28/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

42624 7590 01/27/2014  
**DAVIDSON BERQUIST JACKSON & GOWDEY LLP**  
 4300 WILSON BLVD., 7TH FLOOR  
 ARLINGTON, VA 22203

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	04/03/2012	Patrick Sandor Racz	4037-0003	3525

TITLE OF INVENTION: DATA STORAGE AND ACCESS SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$0	\$0	\$1780	\$0	04/28/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, THIEN MINH	2887	235-380000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
---	---

**3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)**

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (<b>Please first reapply any previously paid issue fee shown above</b>)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

**5. Change in Entity Status** (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscouted fee status.

**NOTE:** Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

**NOTE:** If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

**NOTE:** Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

**NOTE:** This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Values: 13/438,754, 04/03/2012, Patrick Sandor Racz, 4037-0003, 3525

42624 7590 01/27/2014
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

LE, THIEN MINH

ART UNIT PAPER NUMBER

2887

DATE MAILED: 01/27/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.



## OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

### Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<b>Notice of Allowability</b>	<b>Application No.</b> 13/438,754	<b>Applicant(s)</b> RACZ ET AL.	
	<b>Examiner</b> Thien M. Le	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to \_\_\_\_\_.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 40-60 and 64-70. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/oph/index.jsp](http://www.uspto.gov/patents/init_events/oph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

a)  All    b)  Some    \*c)  None of the:

1.  Certified copies of the priority documents have been received.
2.  Certified copies of the priority documents have been received in Application No. 09/697,534.
3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in **ABANDONMENT** of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  **CORRECTED DRAWINGS** ( as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  **DEPOSIT OF and/or INFORMATION** about the deposit of **BIOLOGICAL MATERIAL** must be submitted. Note the attached Examiner's comment regarding **REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL**.

**Attachment(s)**

- |  |  |
|--|--|
| <ol style="list-style-type: none"> <li>1. <input type="checkbox"/> Notice of References Cited (PTO-892)</li> <li>2. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br/>Paper No./Mail Date <u>12/31/2013 (2 IDSs)</u></li> <li>3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material</li> <li>4. <input type="checkbox"/> Interview Summary (PTO-413),<br/>Paper No./Mail Date _____.</li> </ol> | <ol style="list-style-type: none"> <li>5. <input type="checkbox"/> Examiner's Amendment/Comment</li> <li>6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance</li> <li>7. <input type="checkbox"/> Other _____.</li> </ol> |
|--|--|

### **DETAILED ACTION**

The present application is being examined under the pre-AIA first to invent provisions.

The information disclosure statements filed on 12/31/2013 have been entered.

### ***Allowable Subject Matter***

Claims 40-60 and 64-70 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to disclose a handheld multimedia terminal comprising: a wireless interface, a non-volatile memory, a program store, a processor, a user interface, a display, and having the processor control codes as recited in claims 40. Claim 41 recites a data supply server having similar limitations as recited in claim 40. The prior art also fails to disclose a computer system and a method of providing and downloading multimedia contents having limitations as recited in claims 50, 57 and 64.

### ***Conclusion***


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thien M. Le whose telephone number is (571)272-2396. The examiner can normally be reached on Monday - Friday from 7:30am - 4:00pm.

Art Unit: 2887

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve S. Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thien M. Le/  
Primary Examiner, Art Unit 2887

<b>Search Notes</b>  	<b>Application/Control No.</b>  13438754	<b>Applicant(s)/Patent Under Reexamination</b>  HULST ET AL.
	<b>Examiner</b>  THIEN M LE	<b>Art Unit</b>  2887

CPC- SEARCHED		
Symbol	Date	Examiner


CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	380, 382, 492, 451, 486, 487	12/20/2012	LTM
updated	same as above	4/1/2013	LTM
updated	same as above	9/4/2013	LTM
updated	same as above	1/15/2014	LTM

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, review parent applications for double patenting	12/20/2012	LTM
EAST	4/1/2013	LTM
EAST	9/4/2013	LTM
EAST	1/15/2014	LTM

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
235	380,382	4/1/2013	LTM
updated	same as above	9/4/2013	LTM
updated	same as above	1/15/2014	LTM


--	--

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

CPC			Type	Version
Symbol				


CPC Combination Sets				
Symbol	Type	Set	Ranking	Version

NONE	(Assistant Examiner)	(Date)	<b>Total Claims Allowed:</b>	
/THIEN M LE/	Primary Examiner. Art Unit 2887	01/15/2014	O.G. Print Claim(s)	O.G. Print Figure
	(Primary Examiner)	(Date)	1	5

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

US ORIGINAL CLASSIFICATION				INTERNATIONAL CLASSIFICATION									
CLASS		SUBCLASS		CLAIMED				NON-CLAIMED					
235		380		G	0	6	K	5 / 00 (2006.01.01)					
<b>CROSS REFERENCE(S)</b>													
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)												
235	382												

NONE		<b>Total Claims Allowed:</b>	
		28	
(Assistant Examiner)	(Date)	O.G. Print Claim(s)	O.G. Print Figure
/THIEN M LE/ Primary Examiner. Art Unit 2887	01/15/2014	1	5
(Primary Examiner)	(Date)		

<b>Issue Classification</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant																<input type="checkbox"/> CPA		<input checked="" type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original						
1	40	20	56																		
5	41	21	57																		
6	42	22	58																		
7	43	23	59																		
8	44	24	60																		
9	45	25	64																		
10	46	26	65																		
11	47	27	66																		
12	48	28	67																		
13	49	2	68																		
14	50	3	69																		
15	51	4	70																		
16	52																				
17	53																				
18	54																				
19	55																				

NONE		<b>Total Claims Allowed:</b>	
		28	
(Assistant Examiner)	(Date)	O.G. Print Claim(s)	O.G. Print Figure
/THIEN M LE/ Primary Examiner. Art Unit 2887	01/15/2014	1	5
(Primary Examiner)	(Date)		



## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L2	1	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L3	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L4	1	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L5	0	L1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L6	2	L1 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L7	0	L1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L8	34588	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L9	1	L8 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L10	46036	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L11	3	L10 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L12	1	L9 and L11	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L13	0	code.clm. same present.clm.	US-PGPUB;	OR	OFF	2014/01/15

			USPAT; EPO; JPO; DERWENT			11:04
L14	3926	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L15	3	L14 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L16	1	L12 and L15	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L17	43898	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L18	1	L16 and L17	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L19	16717	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L20	0	L19 and L1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L21	3	(("8118221" or ("7942317" or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L22	3	L21 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L23	3	(("8118221" or ("7942317" or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L24	2	L23 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L25	2	L23 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L26	3	(("8118221" or ("7942317" or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L27	1	L26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L28	0	L27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L29	0	L27 and Mbyte.clm.	US-PGPUB;	OR	OFF	2014/01/15

			USPAT; EPO; JPO; DERWENT			11:04
L30	0	L26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L31	2941	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L32	63	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L33	100	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L34	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L35	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L36	1	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L37	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L38	1	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L39	0	L35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L40	2	L35 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L41	0	L35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L42	34588	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L43	1	L42 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04

L44	46036	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L45	3	L44 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L46	1	L43 and L45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L48	3926	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L49	3	L48 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L50	1	L46 and L49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L51	43898	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L52	1	L50 and L51	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L53	16717	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L54	0	L53 and L35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L55	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L56	3	L55 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L57	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L58	2	L57 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L59	2	L57 and status.clm. and mobile.clm.	US-PGPUB; USPAT;	OR	OFF	2014/01/15 11:04

			EPO; JPO; DERWENT			
L60	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L61	1	L60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L62	0	L61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L63	0	L61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L64	0	L60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L65	2941	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L66	63	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L67	100	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L68	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L69	582	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L81	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L82	1	L81 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L83	4	(("8336772") or ("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L84	2	L83 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L85	4	L83 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L86	4	L83 and processor.clm.	US-PGPUB; USPAT;	OR	OFF	2014/01/15 11:04

			EPO; JPO; DERWENT			
L87	1	L83 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L88	2	L83 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L89	2	L84 and L88	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L90	2	L89 and L85 and L86	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L91	1	L83 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L92	4	L83 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L93	2	L90 and L92	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L94	2	L93 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L95	4	L83 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L96	4	L83 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L97	2	L94 and L94	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L98	2	L94 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L99	2	L94 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L100	1	L94 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04

L101	2	L94 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L102	2	L101 and L99	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L103	4	L83 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L104	1	L83 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L105	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L106	0	L105 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:04
L107	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:04
L108	2	L107 and supplier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L109	2	((("6688789") or ("20070176003")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L110	6496	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L111	18881	light adj4 control adj4 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L112	607	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L113	1	L110 and L112	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L114	318	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L115	0	L114 and L110	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L116	0	L114 and 235/462.\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05

L117	0	L114 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L118	9427	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L119	64	L118 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L120	479	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L121	2	L120 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L122	21	L120 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L123	1980	(light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L124	2084	(illumination or light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L125	41	L124 and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L127	1020	(light or illumination) adj40 decreas\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L128	65	L126 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L129	70	((light or illumination) adj40 decreas\$4 adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L130	8	L126 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L131	1072	pulse\$4 adj20 decreas\$4 adj20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L132	10	L131 and flick\$4	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/01/15 11:05



			DERWENT			
L133	10	L131 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L134	108	(pulse\$4 adj20 decreas\$4 adj20 zero) and patient	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L135	1	L129 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L136	31	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L137	1019	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L138	13	L137 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L139	206997	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L140	47	L137 and L139	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L141	4383	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L142	4823	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L143	326	L142 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L144	2	L143 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L145	15	((flicker\$4 near30 gradual\$4 near30 zero))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L146	2492	((light or illumination) near20 pulse\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L147	27	L146 and "235"/\$.ccls.	US-PGPUB;	OR	OFF	2014/01/15

			USPAT; EPO; JPO; DERWENT			11:05
L148	3949	((light or illumination) near20 control near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L149	112	L148 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L150	4929	((light or illumination) near20 (width or control) near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L151	121	L150 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L152	1	L150 and "236"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L153	169	((light or illumination) near30 "off" near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L154	34	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L155	8175	(decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L156	10	L155 and (barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L157	517	light same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L158	532	(illumination or light) same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L159	112	L149 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L160	403	(illumination or light) same (decreas\$4 adj20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L161	15	L160 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05

L162	6809	((illumination or light) near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L163	100	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L164	4	L163 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L165	184	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L166	523111	l61and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L167	3	L165 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L168	497	((pulse\$1) near10 zero) same (scanner or reader)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L169	48	((pulse\$1) near10 zero) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L170	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L171	23	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L172	892	((light or illumination) adj20 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L173	747	((light or illumination) adj10 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L174	67	((light or illumination) adj10 (zero)) same strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L175	6	((light or illumination) adj10 (zero)) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L176	0	((zero) near20 pulse\$4 near20 ("off")) same strobe same power	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/01/15 11:05

			DERWENT			
L177	1110	((zero near20 pulse\$4 near20 ("off")) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L178	54	((zero near20 pulse\$4 near20 ("off")) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L179	121	((zero near20 pulse\$4 near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L180	73	((zero near20 (light or illumination) near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L181	593	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L182	301	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L183	0	L182 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L184	49	L182 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L185	814	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L186	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L187	46	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L188	20	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L189	191	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L190	3	(pulse\$1 near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L191	81	(pulse\$1 near20 (power) near20	US-PGPUB;	OR	OFF	2014/01/15

		(flick\$4 or flash)) and (scanner or barcode)	USPAT; EPO; JPO; DERWENT			11:05
L192	341	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L193	10	L192 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L194	13913	light near20 control\$4 near20 decrea\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L195	138	light near20 control\$4 near20 decrea\$4 near20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L196	911	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L197	4	L195 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L198	4987	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L199	14	L198 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L200	640	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L201	235	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L202	0	L201 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L203	32	L201 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L204	59	L112 and ((power or sleep) same zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L205	8891	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05

L206	9284	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L207	13	L206 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L208	1	("8302866").PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L209	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L210	2	L209 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L211	2	L209 and retrieving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L212	3	L209 and transmitting.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L213	3	L209 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L215	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L216	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L217	1	L216 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L218	0	L216 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L219	1	L216 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L220	0	L216 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L221	2	L216 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L222	0	L216 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/01/15 11:05

			DERWENT			
L223	34588	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L224	1	L223 and L216	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L225	46036	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L226	3	L225 and L216	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L227	1	L224 and L226	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L228	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L229	3926	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L230	3	L229 and L216	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L231	1	L227 and L230	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L232	43898	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L233	1	L231 and L232	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L234	16717	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L235	0	L234 and L216	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L236	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L237	3	L236 and user.clm.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/01/15 11:05

			DERWENT			
L238	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L239	2	L238 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L240	2	L238 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L241	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L242	1	L241 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L243	0	L242 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L244	0	L242 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L245	0	L241 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L246	2941	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L247	63	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L248	100	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L249	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L250	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L251	1	L250 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L252	0	L250 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L253	1	L250 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/01/15 11:05



		validation.clm. and program.clm.	DERWENT			
L254	0	L250 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L255	2	L250 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L256	0	L250 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L257	34588	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L258	1	L257 and L250	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L259	46036	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L260	3	L259 and L250	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L261	1	L258 and L260	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L262	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L263	3926	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L264	3	L263 and L250	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L265	1	L261 and L264	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L266	43898	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L267	1	L265 and L266	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05

L268	16717	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L269	0	L268 and L250	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L270	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L271	3	L270 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L272	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L273	2	L272 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L274	2	L272 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L275	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L276	1	L275 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L277	0	L276 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L278	0	L276 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L279	0	L275 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L280	2941	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L281	63	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L282	100	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L283	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05

L284	582	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L285	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L286	1	L285 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L287	4	(("8336772") or ("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L288	2	L287 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L289	4	L287 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L290	4	L287 and processor.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L291	1	L287 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L292	2	L287 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L293	2	L288 and L292	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L294	2	L293 and L289 and L290	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L295	1	L287 and multimedia.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L296	4	L287 and identifier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L297	2	L294 and L296	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L298	2	L297 and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L299	4	L287 and validation.clm.	US-PGPUB; USPAT;	OR	OFF	2014/01/15 11:05

			EPO; JPO; DERWENT			
L300	4	L287 and payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L301	2	L298 and L298	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L302	2	L298 and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L303	2	L298 and access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L304	1	L298 and selection.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L305	2	L298 and user.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L306	2	L305 and L303	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L307	4	L287 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L308	1	L287 and wireless.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L309	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L310	0	L309 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L311	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L312	2	L311 and supplier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L313	2	((("6688789") or ("20070176003")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L314	6496	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L315	18881	light adj4 control adj4 signal	US-PGPUB; USPAT;	OR	OFF	2014/01/15 11:05

			EPO; JPO; DERWENT			
L316	607	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L317	1	L314 and L316	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L318	318	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L319	0	L318 and L314	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L320	0	L318 and 235/462.\$\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L321	0	L318 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L322	9427	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L323	64	L322 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L324	479	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L325	2	L324 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L326	21	L324 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L327	1980	(light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L328	2084	(illumination or light) near30 decreas\$4 near30 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L329	41	L328 and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05

L331	1020	(light or illumination) adj40 decreases\$4 adj40 (zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L332	65	L330 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L333	70	((light or illumination) adj40 decreases\$4 adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L334	8	L330 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L335	1072	pulse\$4 adj20 decreases\$4 adj20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L336	10	L335 and flick\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L337	10	L335 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L338	108	(pulse\$4 adj20 decreases\$4 adj20 zero) and patient	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L339	1	L333 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L340	31	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L341	1019	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L342	13	L341 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L343	206997	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L344	47	L341 and L343	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L345	4383	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/01/15 11:05

			DERWENT			
L346	4823	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L347	326	L346 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L348	2	L347 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L349	15	((flicker\$4 near30 gradual\$4 near30 zero))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L350	2492	((light or illumination) near20 pulse\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L351	27	L350 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L352	3949	((light or illumination) near20 control near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L353	112	L352 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L354	4929	((light or illumination) near20 (width or control) near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L355	121	L354 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L356	1	L354 and "236"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L357	169	((light or illumination) near30 "off" near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L358	34	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L359	8175	(decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L360	10	L359 and (barcode)	US-PGPUB;	OR	OFF	2014/01/15

			USPAT; EPO; JPO; DERWENT			11:05
L361	517	light same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L362	532	((illumination or light) same (decreas\$4 near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L363	112	L353 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L364	403	((illumination or light) same (decreas\$4 adj20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L365	15	L364 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L366	6809	((illumination or light) near20 zero) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L367	100	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L368	4	L367 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L369	184	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L370	523111	l61and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L371	3	L369 and (barcode or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L372	497	((pulse\$1) near10 zero) same (scanner or reader)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L373	48	((pulse\$1) near10 zero) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L374	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05



L375	23	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L376	892	((light or illumination) adj20 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L377	747	((light or illumination) adj10 (zero)) and strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L378	67	((light or illumination) adj10 (zero)) same strobe	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L379	6	((light or illumination) adj10 (zero)) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L380	0	((zero) near20 pulse\$4 near20 ("off")) same strobe same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L381	1110	((zero) near20 pulse\$4 near20 ("off")) same power	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L382	54	((zero) near20 pulse\$4 near20 ("off")) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L383	121	((zero) near20 pulse\$4 near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L384	73	((zero) near20 (light or illumination) near20 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L385	593	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L386	301	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L387	0	L386 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L388	49	L386 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L389	814	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/01/15 11:05

			DERWENT			
L390	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L391	46	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L392	20	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L393	191	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L394	3	(pulse\$1 near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L395	81	(pulse\$1 near20 (power) near20 (flick\$4 or flash)) and (scanner or barcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L396	341	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L397	10	L396 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L398	13913	light near20 control\$4 near20 decrea\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L399	138	light near20 control\$4 near20 decrea\$4 near20 zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L400	911	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L401	4	L399 and (barcode\$1 or scanner)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L402	4987	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L403	14	L402 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L404	640	(LED\$1 or laser\$1 or light) near10	US-PGPUB;	OR	OFF	2014/01/15

		dim\$4 near10 gradual\$4	USPAT; EPO; JPO; DERWENT			11:05
L405	235	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L406	0	L405 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L407	32	L405 and scanner	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L408	59	L316 and ((power or sleep) same zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L409	8891	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L410	9284	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L411	13	L410 and "235"/\$.cls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L412	1	("8302866").PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L413	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L414	2	L413 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L415	2	L413 and retrieving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L416	3	L413 and transmitting.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L417	3	L413 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L419	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L437	4	((("8336772") or ("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L438	1	L437 and server.clm.	US-PGPUB;	OR	OFF	2014/01/15

			USPAT; EPO; JPO; DERWENT			11:05
L439	1	L437 and server.clm. and handheld.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L440	1	L437 and server.clm. and handheld.clm. and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L441	1	L437 and server.clm. and handheld.clm. and code.clm. and processor.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L442	1	L437 and server.clm. and handheld.clm. and code.clm. and processor.clm. and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L443	2363	(handheld or portable or mobile) same (purchas\$4) same (video\$1 or software or multimedia) same server	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L445	134	(handheld or portable or mobile) same (purchas\$4) same (video\$1 or software or multimedia) same server same request\$4 same payment\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L447	214	(handheld or portable or mobile) same (video\$1 or music\$1 or multimedia) same server same request\$4 same payment\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L449	90	"5861841"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L450	2	((("5682027") or ("5861841"))).PN.	US-PGPUB; USPAT	OR	OFF	2014/01/15 11:05
L451	2	"20120048926"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L452	1039	g07G1/0036.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L453	7257	g06q20/20.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05
L455	3	"20120080522"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/01/15 11:05

## EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L70	35055	code.clm. same request.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L71	4059	code.clm. same payment.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L72	16950	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L73	2889	memory same network same parameter\$1 same card	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L74	104	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L76	24050	(235/375,380,382,492,383,486,487).OCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L77	248	L72 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L78	564	L70 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L79	485	L71 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L80	21	L74 and L76	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:04
L420	35055	code.clm. same request.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L421	4059	code.clm. same payment.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L422	16950	code.clm. same selection\$1.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L423	2889	memory same network same parameter\$1 same card	US-PGPUB; USPAT;	OR	OFF	2014/01/15 11:05

			UPAD			
L424	104	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L425	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L426	24050	(235/375,380,382,492,383,486,487).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L427	248	L422 and L426	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L428	564	L420 and L426	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L429	485	L421 and L426	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L430	21	L424 and L426	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L431	0	"L26" and portable.clm. and carrier.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L432	852	"S113" and ((power or sleep) same zero)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L433	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L434	988	(portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L435	9428	(235/380,382).CCLS.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05
L436	106	L434 and L435	US-PGPUB; USPAT; UPAD	OR	OFF	2014/01/15 11:05

1/15/2014 11:19:57 AM

C:\Users\tle4\Documents\EAST\Workspaces\13438754.wsp

<p align="center"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p align="center">Sheet 1 of 4</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

U.S. PATENT DOCUMENTS				
Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	1-1	US-4200770	Apr-80	Hellman et al.
	1-2	US-4218582	Aug-80	Hellman et al.
	1-3	US-4272810	Jun-81	Gates et al.
	1-4	US-4405829	Sep-83	Rivest et al.
	1-5	US-4424414	Jan-84	Hellman et al.
	1-6	US-4463387	Jul-84	Hashimoto et al.
	1-7	US-4528643	Jul-85	Freeny, Jr.
	1-8	US-4731840	Mar-88	Mniszewski et al.
	1-9	US-4757534	Jul-88	Matyas et al.
	1-10	US-4782529	Nov-88	Shima
	1-11	US-4796220	Jan-89	Wolfe
	1-12	US-4803725	Feb-89	Horne et al.
	1-13	US-4809327	Feb-89	Shima
	1-14	US-4825306	Apr-89	Robers
	1-15	US-4868687	Sep-89	Penn et al.
	1-16	US-4868877	Sep-89	Fischer
	1-17	US-4878246	Oct-89	Pastor et al.
	1-18	US-4879747	Nov-89	Leighton et al.
	1-19	US-4905163	Feb-90	Garber et al.
	1-20	US-4926479	May-90	Goldwasser et al.
	1-21	US-4944006	Jul-90	Citta et al.
	1-22	US-4995082	Feb-91	Schnorr
	1-23	US-5005200	Apr-91	Fischer
	1-24	US-5130792	Jul-92	Tindell et al.
	1-25	US-5159634	Oct-92	Reeds, III
	1-26	US-5191573	Mar-93	Hair

Examiner Signature	/Thien Le/	Date Considered	01/14/2014
--------------------	------------	-----------------	------------

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

<p align="center"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p align="center">Sheet 2 of 4</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

U.S. PATENT DOCUMENTS				
Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	2-1	US-5214702	May-93	Fischer
	2-2	US-5220604	Jun-93	Gasser et al.
	2-3	US-5224163	Jun-93	Gasser et al.
	2-4	US-5224166	Jun-93	Hartman, Jr.
	2-5	US-5260788	Nov-93	Takano et al.
	2-6	US-5261002	Nov-93	Perlman et al.
	2-7	US-5276901	Jan-94	Howell et al.
	2-8	US-5315658	May-94	Micali
	2-9	US-5319705	Jun-94	Halter et al.
	2-10	US-5347580	Sep-94	Molva et al.
	2-11	US-5355302	Oct-94	Martin et al.
	2-12	US-5369705	Nov-94	Bird et al.
	2-13	US-5371794	Dec-94	Diffie et al.
	2-14	US-5388211	Feb-95	Hornbuckle
	2-15	US-5412717	May-95	Fischer
	2-16	US-5420927	May-95	Micali
	2-17	US-5497421	Mar-96	Kaufman et al.
	2-18	US-5509071	Apr-96	Petrie, Jr. et al.
	2-19	US-5519778	May-96	Leighton et al.
	2-20	US-5537475	Jul-96	Micali
	2-21	US-5557541	Sep-96	Schulhof et al.
	2-22	US-5581479	Dec-96	McLaughlin et al.
	2-23	US-5588060	Dec-96	Aziz
	2-24	US-5592664	Jan-97	Starkey
	2-25	US-5604804	Feb-97	Micali
	2-26	US-5606617	Feb-97	Brands

Examiner Signature	/Thien Le/	Date Considered	01/14/2014
--------------------	------------	-----------------	------------

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.



<p align="center"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p align="center">Sheet 3 of 4</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

U.S. PATENT DOCUMENTS				
Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	3-1	US-5636139	Jun-97	McLaughlin et al.
	3-2	US-5646992	Jul-97	Subler et al.
	3-3	US-5646998	Jul-97	Stambler
	3-4	US-5649187	Jul-97	Hornbuckle
	3-5	US-5666420	Sep-97	Micali
	3-6	US-5673316	Sep-97	Auerbach et al.
	3-7	US-5675734	Oct-97	Hair
	3-8	US-5706347	Jan-98	Burke et al.
	3-9	US-5710887	Jan-98	Chelliah et al.
	3-10	US-5745574	Apr-98	Muftic
	3-11	US-5765152	Jun-98	Erickson
	3-12	US-5796841	Aug-98	Cordery et al.
	3-13	US-5864620	Jan-99	Pettitt
	3-14	US-5892900	Apr-99	Ginter et al.
	3-15	US-5915025	Dec-99	Taguchi et al.
	3-16	US-5925127	Jul-99	Ahmad
	3-17	US-5982892	Nov-99	Hicks et al.
	3-18	US-5991399	Nov-99	Graunke et al.
	3-19	US-5999629	Dec-99	Heer et al.
	3-20	US-6064739	May-00	Davis
	3-21	US-6098056	Aug-00	Rusnak et al.
	3-22	US-6275936	Aug-01	Kyojima et al.
	3-23			
	3-24			
	3-25			
	3-26			

Examiner Signature	/Thien Le/	Date Considered	01/14/2014
--------------------	------------	-----------------	------------

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

<p align="center"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p align="center">Sheet 4 of 4</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	4-1	Smartflash LLC v. Apple Inc., Civil Action 6:13-CV-00447-MHS-KNM, Subpoena to Testify	
	4-2		
	4-3		
	4-4		
	4-5		
	4-6		
	4-7		

Examiner Signature	/Thien Le/	Date Considered	01/14/2014
--------------------	------------	-----------------	------------

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<p align="center"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p align="center">Sheet 1 of 1</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

U.S. PATENT DOCUMENTS				
Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	1-1	US-6226618	May 2001	Downs et al.
	1-2	US-6389538	May 2002	Downs et al.
	1-3			
	1-4			
	1-5			
	1-6			
	1-7			
	1-8			
	1-9			
	1-10			
	1-11			
	1-12			
	1-13			
	1-14			
	1-15			
	1-16			
	1-17			
	1-18			
	1-19			
	1-20			
	1-21			
	1-22			
	1-23			
	1-24			
	1-25			
	1-26			

Examiner Signature	/Thien Le/	Date Considered	01/14/2014
--------------------	------------	-----------------	------------


\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.


**UNITED STATES PATENT AND TRADEMARK OFFICE**

UNITED STATES DEPARTMENT OF COMMERCE  
**United States Patent and Trademark Office**  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

**BIB DATA SHEET**
**CONFIRMATION NO. 3525**

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.	
13/438,754	04/03/2012	235	2887	4037-0003	
<b>APPLICANTS</b> <b>INVENTORS</b> Patrick Sandor Racz, Saint Heller, UNITED KINGDOM; Hermen-ard Hulst, Amsterdam, NETHERLANDS;					
<b>** CONTINUING DATA *****</b> This application is a CON of 13/212,047 08/17/2011 PAT 8336772 which is a CON of 12/943,872 11/10/2010 PAT 8118221 which is a CON of 12/014,558 01/15/2008 PAT 7942317 which is a CON of 11/336,758 01/19/2006 PAT 7334720 which is a CON of 10/111,716 09/17/2002 ABN which is a 371 of PCT/GB2000/004110 10/25/2000					
<b>** FOREIGN APPLICATIONS *****</b> UNITED KINGDOM 9925227.2 10/25/1999					
<b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **</b> 04/16/2012					
Foreign Priority claimed <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No 35 USC 119(a-d) conditions met <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Verified and Acknowledged <u>/THIEN MINH LE/</u> <small>Examiner's Signature</small>	<input type="checkbox"/> Met after Allowance <small>Initials</small>	<b>STATE OR COUNTRY</b> UNITED KINGDOM	<b>SHEETS DRAWINGS</b> 17	<b>TOTAL CLAIMS</b> 28	<b>INDEPENDENT CLAIMS</b> 6
<b>ADDRESS</b> DAVIDSON BERQUIST JACKSON & GOWDEY LLP 4300 WILSON BLVD., 7TH FLOOR ARLINGTON, VA 22203 UNITED STATES					
<b>TITLE</b> DATA STORAGE AND ACCESS SYSTEMS					
<b>FILING FEE RECEIVED</b> 1591	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

<b>Index of Claims</b> 	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013	09/04/2013	01/15/2014				
1	40	✓	=	=	=				
5	41	✓	=	=	=				
6	42	✓	=	=	=				
7	43	✓	=	=	=				
8	44	✓	=	=	=				
9	45	✓	=	=	=				
10	46	✓	=	=	=				
11	47	✓	=	=	=				
12	48	✓	=	=	=				
13	49	✓	=	=	=				
14	50	✓	=	=	=				
15	51	✓	=	=	=				
16	52	✓	=	=	=				
17	53	✓	=	=	=				
18	54	✓	=	=	=				
19	55	✓	=	=	=				
20	56	✓	=	=	=				
21	57	✓	=	=	=				
22	58	✓	=	=	=				
23	59	✓	=	=	=				
24	60	✓	=	=	=				
	61	✓	-	-	-				
	62	✓	-	-	-				
	63	✓	-	-	-				
25	64	✓	=	=	=				
26	65	✓	=	=	=				
27	66	✓	=	=	=				
28	67	✓	=	=	=				
2	68		=	=	=				
3	69		=	=	=				
4	70		=	=	=				
	71								
	72								
	73								
	74								
	75								

<b>Index of Claims</b>  	<b>Application/Control No.</b> 13438754	<b>Applicant(s)/Patent Under Reexamination</b> HULST ET AL.
	<b>Examiner</b> THIEN M LE	<b>Art Unit</b> 2887

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/21/2012	04/01/2013	09/04/2013	01/15/2014				
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								
	101								
	102								
	103								
	104								
	105								
	106								



**PRIORITY DOCUMENT EXCHANGE**

**FAILURE STATUS REPORT**

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 9925227.2 to which priority is claimed has FAILED on 01/30/2014.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

[pdx@uspto.gov](mailto:pdx@uspto.gov) (email)

Priority Document Exchange Website: [http://www.uspto.gov/patents/process/file/pdx/pdx\\_index.jsp](http://www.uspto.gov/patents/process/file/pdx/pdx_index.jsp)



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/438,754	04/03/2012	Patrick Sandor Racz	4037-0003	3525

42624 7590 02/07/2014  
DAVIDSON BERQUIST JACKSON & GOWDEY LLP  
4300 WILSON BLVD., 7TH FLOOR  
ARLINGTON, VA 22203

EXAMINER
----------

LE, THIEN MINH

ART UNIT	PAPER NUMBER
----------	--------------

2887

MAIL DATE	DELIVERY MODE
-----------	---------------

02/07/2014

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.





UNITED STATES DEPARTMENT OF COMMERCE

U.S. Patent and Trademark Office

Address : COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

<b>APPLICATION NO./ CONTROL NO.</b>	<b>FILING DATE</b>	<b>FIRST NAMED INVENTOR / PATENT IN REEXAMINATION</b>	<b>ATTORNEY DOCKET NO.</b>
13/438,754	03 April, 2012	RACZ ET AL.	4037-0003

DAVIDSON BERQUIST JACKSON & GOWDEY LLP 4300 WILSON BLVD., 7TH FLOOR ARLINGTON, VA 22203	<b>EXAMINER</b>	
	Thien M. Le	
	<b>ART UNIT</b>	<b>PAPER</b>
	2887	20140204

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The information disclosure statement filed on 1/15/2014 has been entered.

/Thien M. Le/  
Primary Examiner, Art Unit 2887

<p align="center"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p align="center">Sheet 1 of 3</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

U.S. PATENT DOCUMENTS				
Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	1-1	US-5103392	Apr-91	Mori
	1-2	US-5530235	Jun-96	Stefik
	1-3	US-5629980	May-97	Stefik
	1-4	US-5634012	May-97	Stefik
	1-5	US-5638443	Jun-97	Stefik
	1-6	US-5715403	Feb-98	Stefik
	1-7	US-5790423	Aug-98	Lau
	1-8	US-5915019	Jun-99	Ginter
	1-9	US-5926624	Jul-99	Katz et al.
	1-10	US-5982891	Nov-99	Ginter et al.
	1-11	US-6055314	Apr-2000	Spies
	1-12	US-6170060	Jan-01	Mott et al.
	1-13	US-6223291	Apr-01	Puhl et al.
	1-14	US-6282653	Aug-01	Berstis et al.
	1-15	US-6367019	Apr-02	Ansell et al.
	1-16	US-6385596	May-02	Wiser et al.
	1-17	US-6434535	Aug-02	Kupka et al.
	1-18	US-6697948	Feb-04	Rabin et al.
	1-19	US-6829711	Dec-04	Kwok et al.
	1-20	US-7191153	Mar-07	Braitberg et al.
	1-21	US-7225160	May-07	Stefik et al.
	1-22	US-7233948	Jun-07	Shamoon et al.
	1-23	US-7249382	Jul-07	Kawell, Jr. et al.
	1-24	US-7263497	Aug-07	Wiser et al.
	1-25	US-7315829	Jan-08	Tagawa et al.
	1-26	US-7523072	Apr-2009	Stefik et al.

Examiner Signature	/Thien Le/	Date Considered	02/03/2014
--------------------	------------	-----------------	------------

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

<p align="center"><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p align="center">Sheet 2 of 3</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

U.S. PATENT DOCUMENTS				
Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	2-1	US-7636691	Dec-2009	Maari
	2-2			
	2-3			
	2-4			
	2-5			
	2-6			
	2-7			
	2-8			
	2-9			
	2-10			
	2-11			
	2-12			
	2-13			
	2-14			
	2-15			
	2-16			
	2-17			
	2-18			
	2-19			
	2-20			
	2-21			
	2-22			
	2-23			
	2-24			
	2-25			
	2-26			

Examiner Signature	/Thien Le/	Date Considered	02/03/2014
--------------------	------------	-----------------	------------

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

<p><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)</p> <p>Sheet 3 of 3</p>	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	3-1	Smartflash LLC v. Apple Inc., Civil Action 6:13-CV-00447-MHS-KNM, Defendants' Disclosure of Prior Art, dated Jan. 13, 2014	
	3-2		
	3-3		
	3-4		
	3-5		
	3-6		
	3-7		

Examiner Signature	/Thien Le/	Date Considered	02/03/2014
--------------------	------------	-----------------	------------

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	30	((("5103392") or ("5530235") or ("5629980") or ("5634012") or ("5638443") or ("5646992") or ("5715403") or ("5790423") or ("5915019") or ("5926624") or ("5982891") or ("6055314") or ("6142369") or ("6170060") or ("6223291") or ("6226618") or ("6282653") or ("6367019") or ("6385596") or ("6389538") or ("6434535") or ("6697948") or ("6829711") or ("7191153") or ("7225160") or ("7233948") or ("7249382") or ("7263497") or ("7523072") or ("7636691"))).PN.	US-PGPUB; USPAT	OR	OFF	2014/02/04 07:18
L2	13	l1 and multimedia	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:46
L3	25	l1 and payment\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:46
L4	19	l1 and wireless	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:46
L5	10	l2 and l3 and l4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:46
L6	3070	(payment\$1 near4 memory)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:56
L7	301713	communication near10 memory	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:56
L9	908	l6 and l7	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:56

L10	0	I9 and I1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 07:56
L11	7	I1 and handheld	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 08:55
L12	6	I5 and I11	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/02/04 08:56
S1	3	(("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/08 14:51
S2	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S3	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:12
S4	1	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:13
S5	0	S1 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25
S6	2	S1 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:25
S7	0	S1 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:33
S8	27343	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S9	1	S8 and S1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:37
S10	35059	code.clm. same receive.clm.	US-PGPUB;	OR	OFF	2012/07/08 15:38

			USPAT; EPO; JPO; DERWENT			
S11	3	S10 and S1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S12	1	S9 and S11	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:38
S13	0	code.clm. same present.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S14	3000	code.clm. same payment.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S15	3	S14 and S1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S16	1	S12 and S15	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:39
S17	36126	code.clm. same access.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:41
S18	1	S16 and S17	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S19	13678	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S20	0	S19 and S1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/08 15:42
S21	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2012/07/09 05:52
S22	3	S21 and user.clm.	US- PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/07/09 05:52

			DERWENT			
S23	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 07:46
S24	2	S23 and status.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S25	2	S23 and status.clm. and mobile.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 07:47
S26	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/07/09 09:13
S27	1	S26 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S28	0	S27 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S29	0	S27 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S30	0	S26 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:13
S31	2178	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S32	39	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:16
S33	61	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:35
S34	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/07/09 09:52
S35	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB;	OR	OFF	2012/10/22 14:25



			USPAT			
S36	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S37	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S38	1	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S39	0	S35 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S40	2	S35 and request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S41	0	S35 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S42	28666	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S43	1	S42 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S44	37012	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S45	3	S44 and S35	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S46	1	S43 and S45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S47	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2012/10/22 14:25

			DERWENT			
S48	3161	code.clm. same payment.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S49	3	S48 and S35	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S50	1	S46 and S49	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S51	37531	code.clm. same access.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S52	1	S50 and S51	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S53	14209	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S54	0	S53 and S35	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S55	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S56	3	S55 and user.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S57	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2012/10/22 14:25
S58	2	S57 and status.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S59	2	S57 and status.clm. and mobile.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S60	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB;	OR	OFF	2012/10/22 14:25

			USPAT			
S61	1	S60 and portable.clm. and carrier.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S62	0	S61 and byte\$1.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S63	0	S61 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S64	0	S60 and Mbyte.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S65	2322	memory same network same parameter\$1 same card	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S66	40	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S67	69	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S68	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:25
S69	542	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/10/22 14:39
S82	3	((("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 08:51
S83	1	S82 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 08:51
S84	3	((("8336772") or ("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 09:27
S85	1	S84 and memory.clm.	US-PGPUB;	OR	OFF	2012/12/20 09:39

			USPAT; EPO; JPO; DERWENT			
S86	3	S84 and interface.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S87	3	S84 and processor.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S88	0	S84 and display.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:40
S89	1	S84 and display\$4.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S90	1	S85 and S89	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S91	1	S90 and S86 and S87	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S92	0	S84 and multimedia.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:43
S93	3	S84 and identifier.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:44
S94	1	S91 and S93	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:44
S95	1	S94 and validation.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S96	3	S84 and validation.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:50
S97	3	S84 and payment.clm.	US- PGPUB;	OR	OFF	2012/12/20 09:51

			USPAT; EPO; JPO; DERWENT			
S98	1	S95 and S95	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S99	1	S95 and code.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S100	1	S95 and access.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:51
S101	0	S95 and selection.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S102	1	S95 and user.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S103	1	S102 and S100	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:52
S104	3	S84 and wireless	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S105	0	S84 and wireless.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 09:53
S106	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2012/12/20 11:53
S107	0	S106 and server.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 11:53
S108	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2012/12/20 15:00
S109	2	S108 and supplier.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:01

S110	2	((("6688789") or ("20070176003")).PN.	US-PGPUB; USPAT	OR	OFF	2012/12/20 15:30
S111	6083	image adj2 pickup adj2 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S112	17020	light adj4 control adj4 signal	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S113	559	(light adj4 control adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S114	1	S111 and S113	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:33
S115	301	(light adj4 control adj4 signal) same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S116	0	S115 and S111	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S117	0	S115 and 235/462.\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:34
S118	0	S115 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S119	8726	(light adj4 signal) same decreas\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S120	62	S119 and "235"/\$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:35
S121	441	(light adj4 signal) same decreas\$4 same zero	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:37
S122	2	S121 and "235"/\$.ccls.	US-PGPUB;	OR	OFF	2012/12/20 15:37

			USPAT; EPO; JPO; DERWENT			
S123	18	S121 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:38
S124	1836	(light) near30 decreas\$4 near30 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40
S125	1930	(illumination or light) near30 decreas\$4 near30 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40
S126	40	S125 and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:40
S127	923	(light or illumination) adj40 decreas\$4 adj40 (zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:43
S128	923	(light or illumination) adj40 decreas\$4 adj40 (zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:43
S129	60	S127 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:44
S130	63	((light or illumination) adj40 decreas\$4 adj40 (zero)) same pulse\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:44
S131	7	S127 and barcode\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:47
S132	1029	pulse\$4 adj20 decreas\$4 adj20 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:48
S133	9	S132 and flick\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:49
S134	8	S132 and barcode\$1	US- PGPUB;	OR	OFF	2012/12/20 15:51

			USPAT; EPO; JPO; DERWENT			
S135	99	(pulse\$4 adj20 decreas\$4 adj20 zero) and patient	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:53
S136	1	S130 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:57
S137	25	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:57
S138	945	((light or illumination) adj40 gradually) same pulse\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:58
S139	11	S138 and barcode\$1	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 15:58
S140	187291	image near5 (pickup or acquisition)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:00
S141	47	S138 and S140	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:00
S142	4072	((light or illumination) near20 level near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S143	4474	((light or illumination) near20 level\$1 near20 zero)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S144	261	S143 and flicker\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S145	0	S144 and barcode	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:03
S146	12	((flicker\$4 near30 gradual\$4 near30 zero))	US-PGPUB;	OR	OFF	2012/12/20 16:04



			USPAT; EPO; JPO; DERWENT			
S147	2343	((light or illumination) near20 pulse\$1 near20 zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:06
S148	24	S147 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:06
S149	3615	((light or illumination) near20 control near20 zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:08
S150	109	S149 and barcode	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:08
S151	4507	((light or illumination) near20 (width or control) near20 zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S152	117	S151 and barcode	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S153	1	S151 and "236"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:10
S154	162	((light or illumination) near30 "off" near30 zero near30 (pulse\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:11
S155	31	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:12
S156	7416	(decreas\$4 near20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:43
S157	8	S156 and (barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:43
S158	472	light same (decreas\$4 near20 zero) same power	US- PGPUB;	OR	OFF	2012/12/20 16:44

			USPAT; EPO; JPO; DERWENT			
S159	483	(illumination or light) same (decreas\$4 near20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S160	109	S150 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:44
S161	365	(illumination or light) same (decreas\$4 adj20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:45
S162	14	S161 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:46
S163	6180	((illumination or light) near20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:48
S164	86	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:49
S165	4	S164 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:49
S166	168	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50
S167	474725	l61and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50
S168	3	S166 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:50
S169	480	((pulse\$1) near10 zero) same (scanner or reader)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:51
S170	47	((pulse\$1) near10 zero) same (scanner or reader) same power	US- PGPUB;	OR	OFF	2012/12/20 16:51

			USPAT; EPO; JPO; DERWENT			
S171	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 16:55
S172	22	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:03
S173	842	((light or illumination) adj20 (zero)) and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S174	706	((light or illumination) adj10 (zero)) and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S175	61	((light or illumination) adj10 (zero)) same strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S176	5	((light or illumination) adj10 (zero)) same strobe same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:05
S177	0	((zero) near20 pulse\$4 near20 ("off")) same strobe same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:07
S178	1039	((zero) near20 pulse\$4 near20 ("off")) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:08
S179	53	((zero) near20 pulse\$4 near20 ("off")) same power same (saving or down)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:08
S180	116	((zero) near20 pulse\$4 near20 (control)) same power same (saving or down)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:10
S181	59	((zero) near20 (light or illumination) near20 (control)) same power same (saving or down)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:13
S182	511	((zero or "off") near10 (light or illumination) near10 (control)) same	US- PGPUB;	OR	OFF	2012/12/20 17:14

		power same (saving or down)	USPAT; EPO; JPO; DERWENT			
S183	260	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:14
S184	0	S183 and barcode	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:14
S185	37	S183 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:15
S186	716	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:16
S187	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:16
S188	39	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:17
S189	18	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:18
S190	177	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S191	3	(pulse\$1 near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S192	80	(pulse\$1 near20 (power) near20 (flick\$4 or flash)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:19
S193	304	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:21
S194	10	S193 and (barcode\$1 or scanner)	US- PGPUB;	OR	OFF	2012/12/20 17:21

			USPAT; EPO; JPO; DERWENT			
S195	12573	light near20 control\$4 near20 decrea\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S196	131	light near20 control\$4 near20 decrea\$4 near20 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S197	790	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S198	4	S196 and (barcode\$1 or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:23
S199	4145	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:26
S200	13	S199 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:26
S201	551	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:28
S202	207	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S203	0	S202 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S204	30	S202 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:29
S205	52	S113 and ((power or sleep) same zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:33
S206	7915	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US- PGPUB;	OR	OFF	2012/12/20 17:37

			USPAT; EPO; JPO; DERWENT			
S207	8295	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S208	11	S207 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/20 17:37
S209	1	("8302866").PN.	US- PGPUB; USPAT	OR	OFF	2012/12/20 17:44
S210	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2012/12/21 06:10
S211	2	S210 and request.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:11
S212	2	S210 and retrieving.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:11
S213	3	S210 and transmitting.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:11
S214	3	S210 and receiving.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 06:12
S215	913	(portable or mobile) near30 payment near30 memory	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 07:44
S216	16	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2012/12/21 07:46
S217	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S218	1	S217 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S219	0	S217 and identifier.clm. and processor.clm. and interface.clm. and	US- PGPUB;	OR	OFF	2013/04/01 09:39

		memory.clm. and payment.clm. and validation.clm. and display.clm.	USPAT; EPO; JPO; DERWENT			
S220	1	S217 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S221	0	S217 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S222	2	S217 and request.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S223	0	S217 and request.clm. and receive.clm. and present.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S224	30643	code.clm. same request.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S225	1	S224 and S217	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S226	40009	code.clm. same receive.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S227	3	S226 and S217	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S228	1	S225 and S227	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S229	0	code.clm. same present.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S230	3421	code.clm. same payment.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S231	3	S230 and S217	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S232	1	S228 and S231	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S233	39665	code.clm. same access.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S234	1	S232 and S233	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S235	15054	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S236	0	S235 and S217	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S237	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S238	3	S237 and user.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S239	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S240	2	S239 and status.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S241	2	S239 and status.clm. and mobile.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S242	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S243	1	S242 and portable.clm. and carrier.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S244	0	S243 and byte\$1.clm.	US- PGPUB;	OR	OFF	2013/04/01 09:39



			USPAT; EPO; JPO; DERWENT			
S245	0	S243 and Mbyte.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S246	0	S242 and Mbyte.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S247	2561	memory same network same parameter\$1 same card	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S248	48	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S249	78	memory same storing same card same ((payment or transaction) near10 data) same instructions	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S250	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S251	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S252	1	S251 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S253	0	S251 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and display.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S254	1	S251 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S255	0	S251 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm. same request.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S256	2	S251 and request.clm.	US- PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/04/01 09:39

			DERWENT			
S257	0	S251 and request.clm. and receive.clm. and present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S258	30643	code.clm. same request.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S259	1	S258 and S251	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S260	40009	code.clm. same receive.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S261	3	S260 and S251	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S262	1	S259 and S261	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S263	0	code.clm. same present.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S264	3421	code.clm. same payment.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S265	3	S264 and S251	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S266	1	S262 and S265	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S267	39665	code.clm. same access.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S268	1	S266 and S267	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/04/01 09:39

			DERWENT			
S269	15054	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S270	0	S269 and S251	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S271	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S272	3	S271 and user.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S273	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S274	2	S273 and status.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S275	2	S273 and status.clm. and mobile.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S276	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S277	1	S276 and portable.clm. and carrier.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S278	0	S277 and byte\$1.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S279	0	S277 and Mbyte.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S280	0	S276 and Mbyte.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S281	2561	memory same network same parameter\$1 same card	US- PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/04/01 09:39

			DERWENT			
S282	48	memory same network same parameter\$1 same card same ((payment or transaction) near10 data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S283	78	memory same storing same card same ((payment or transaction) near10 data) same instructions	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S284	26	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S285	550	"I37" and "I42"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S286	3	((("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S287	1	S286 and identifier.clm. and processor.clm. and interface.clm. and memory.clm. and payment.clm. and validation.clm. and program.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S288	4	((("8336772") or ("8118221") or ("7942317") or ("7334720"))).PN.	US-PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S289	2	S288 and memory.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S290	4	S288 and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S291	4	S288 and processor.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S292	1	S288 and display.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S293	2	S288 and display\$4.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S294	2	S289 and S293	US-PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S295	2	S294 and S290 and S291	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S296	1	S288 and multimedia.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S297	4	S288 and identifier.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S298	2	S295 and S297	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S299	2	S298 and validation.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S300	4	S288 and validation.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S301	4	S288 and payment.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S302	2	S299 and S299	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S303	2	S299 and code.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S304	2	S299 and access.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S305	1	S299 and selection.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S306	2	S299 and user.clm.	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S307	2	S306 and S304	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S308	4	S288 and wireless	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S309	1	S288 and wireless.dlm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S310	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S311	0	S310 and server.dlm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S312	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S313	2	S312 and supplier.dlm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S314	2	((("6688789") or ("20070176003")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S315	6162	image adj2 pickup adj2 signal	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S316	17444	light adj4 control adj4 signal	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S317	574	(light adj4 control adj4 signal) same decreas\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S318	1	S315 and S317	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S319	304	(light adj4 control adj4 signal) same zero	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S320	0	S319 and S315	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S321	0	S319 and 235/462.\$ccls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S322	0	S319 and "235"/\$.ccls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S323	8923	(light adj4 signal) same decreas\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S324	63	S323 and "235"/\$.ccls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S325	453	(light adj4 signal) same decreas\$4 same zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S326	2	S325 and "235"/\$.ccls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S327	19	S325 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S328	1874	(light) near30 decreas\$4 near30 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S329	1973	(illumination or light) near30 decreas\$4 near30 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S330	40	S329 and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S331	949	(light or illumination) adj40 decreas\$4 adj40 (zero)	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S332	949	(light or illumination) adj40 decreases\$4 adj40 (zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S333	61	S331 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S334	64	((light or illumination) adj40 decreases\$4 adj40 (zero)) same pulse\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S335	7	S331 and barcode\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S336	1042	pulse\$4 adj20 decreases\$4 adj20 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S337	9	S336 and flick\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S338	8	S336 and barcode\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S339	102	(pulse\$4 adj20 decreases\$4 adj20 zero) and patient	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S340	1	S334 and barcode\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S341	27	((light or illumination) adj40 gradually adj40 (zero)) same pulse\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S342	961	((light or illumination) adj40 gradually) same pulse\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S343	11	S342 and barcode\$1	US- PGPUB;	OR	OFF	2013/04/01 09:39



			USPAT; EPO; JPO; DERWENT			
S344	191877	image near5 (pickup or acquisition)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S345	47	S342 and S344	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S346	4159	((light or illumination) near20 level near20 zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S347	4577	((light or illumination) near20 level\$1 near20 zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S348	283	S347 and flicker\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S349	0	S348 and barcode	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S350	12	((flicker\$4 near30 gradual\$4 near30 zero))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S351	2387	((light or illumination) near20 pulse\$1 near20 zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S352	24	S351 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S353	3694	((light or illumination) near20 control near20 zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S354	109	S353 and barcode	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S355	4610	((light or illumination) near20 (width or control) near20 zero)	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S356	117	S355 and barcode	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S357	1	S355 and "236"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S358	164	((light or illumination) near30 "off" near30 zero near30 (pulse\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S359	33	((light or illumination) near30 (gradual\$4) near30 zero near30 (pulse\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S360	7603	(decreas\$4 near20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S361	9	S360 and (barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S362	482	light same (decreas\$4 near20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S363	496	((illumination or light) same (decreas\$4 near20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S364	109	S354 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S365	374	((illumination or light) same (decreas\$4 adj20 zero) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S366	14	S365 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S367	6332	((illumination or light) near20 zero) same power	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S368	86	((illumination or light) near20 zero) same (power adj5 (down or saving\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S369	4	S368 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S370	171	((pulse\$1) near20 zero) same (power adj5 (down or saving\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S371	486192	l61and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S372	3	S370 and (barcode or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S373	482	((pulse\$1) near10 zero) same (scanner or reader)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S374	47	((pulse\$1) near10 zero) same (scanner or reader) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S375	6	((pulse\$1) near10 decreas\$4 near10 width\$1 ) same (scanner or reader) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S376	22	((light or illumination) adj40 decreas\$4 adj40 (zero)) and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S377	856	((light or illumination) adj20 (zero)) and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S378	717	((light or illumination) adj10 (zero)) and strobe	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S379	62	((light or illumination) adj10 (zero)) same strobe	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S380	6	((light or illumination) adj10 (zero)) same strobe same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S381	0	((zero) near20 pulse\$4 near20 ("off")) same strobe same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S382	1059	((zero) near20 pulse\$4 near20 ("off")) same power	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S383	53	((zero) near20 pulse\$4 near20 ("off")) same power same (saving or down)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S384	118	((zero) near20 pulse\$4 near20 (control)) same power same (saving or down)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S385	61	((zero) near20 (light or illumination) near20 (control)) same power same (saving or down)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S386	526	((zero or "off") near10 (light or illumination) near10 (control)) same power same (saving or down)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S387	268	((zero or "off") near10 (light or illumination) near10 (control)) same (power near5 (saving or down))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S388	0	S387 and barcode	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S389	39	S387 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S390	743	((zero or "off") near10 (light or illumination) near10 (flick\$4))	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S391	1	((zero or "off") near10 (light or illumination) near10 (flick\$4)) same	US- PGPUB;	OR	OFF	2013/04/01 09:39

		(scanner or barcode)	USPAT; EPO; JPO; DERWENT			
S392	39	((zero or "off") near10 (light or illumination) near10 (flick\$4)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S393	18	(power near20 (down or saving) near20 (flick\$4)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S394	179	(power near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S395	3	(pulse\$1 near20 (down or saving) near20 (flick\$4 or flash)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S396	81	(pulse\$1 near20 (power) near20 (flick\$4 or flash)) and (scanner or barcode)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S397	318	light near20 control\$4 near20 gradual\$4 near20 ("off" or zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S398	10	S397 and (barcode\$1 or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S399	12896	light near20 control\$4 near20 decrea\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S400	132	light near20 control\$4 near20 decrea\$4 near20 zero	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S401	818	light near20 control\$4 near20 decrea\$4 near20 (zero or "off")	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S402	4	S400 and (barcode\$1 or scanner)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S403	4331	(LED\$1 or laser\$1 or light) near10 dim\$4 near10 ("off" or zero)	US- PGPUB;	OR	OFF	2013/04/01 09:39

			USPAT; EPO; JPO; DERWENT			
S404	13	S403 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S405	569	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S406	212	((LED\$1 or laser\$1 or light) near10 dim\$4 near10 gradual\$4) same (sleep or power)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S407	0	S406 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S408	30	S406 and scanner	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S409	53	S317 and ((power or sleep) same zero)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S410	8155	pulse near10 width\$1 near10 (dimming or decreasing or reducing)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S411	8538	pulse\$1 near10 width\$1 near10 (dimming or decreasing or reducing)	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S412	11	S411 and "235"/\$.cls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S413	1	("8302866").PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S414	3	((("8118221") or ("7942317") or ("7334720")).PN.	US- PGPUB; USPAT	OR	OFF	2013/04/01 09:39
S415	2	S414 and request.clm.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39

S416	2	S414 and retrieving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S417	3	S414 and transmitting.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S418	3	S414 and receiving.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S419	1012	(portable or mobile) near30 payment near30 memory	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S420	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/04/01 09:39
S438	4	((("8336772") or ("8118221") or ("7942317") or ("7334720")).PN.	US-PGPUB; USPAT	OR	OFF	2013/07/24 11:05
S439	1	S438 and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 11:05
S440	1	S438 and server.clm. and handheld.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 11:05
S441	1	S438 and server.clm. and handheld.clm. and code.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 11:06
S442	1	S438 and server.clm. and handheld.clm. and code.clm. and processor.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 11:06
S443	1	S438 and server.clm. and handheld.clm. and code.clm. and processor.clm. and interface.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 11:06
S444	2096	(handheld or portable or mobile) same (purchas\$4) same (video\$1 or software or multimedia) same server	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 12:58
S445	574	(handheld or portable or mobile) same (purchas\$4) same (video\$1 or software	US-PGPUB;	OR	OFF	2013/07/24 12:59

		or multimedia) same server same request\$4	USPAT; EPO; JPO; DERWENT			
S446	119	(handheld or portable or mobile) same (purchas\$4) same (video\$1 or software or multimedia) same server same request\$4 same payment\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 13:01
S447	457	(handheld or portable or mobile) same (video\$1 or software or multimedia) same server same request\$4 same payment\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 13:18
S448	184	(handheld or portable or mobile) same (video\$1 or music\$1 or multimedia) same server same request\$4 same payment\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 13:23
S449	621	(handheld or portable or mobile) same (video\$1 or music\$1 or multimedia) same server same payment\$1	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 13:34
S450	86	"5861841"	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 13:48
S451	2	((("5862027") or ("5861841"))).PN.	US- PGPUB; USPAT	OR	OFF	2013/07/24 13:48
S452	2	"20120048926"	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 14:06
S453	949	g07G1/0036.cpc.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 14:09
S454	6096	g06q20/20.cpc.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 14:14
S455	1556	((mobile) same (payment\$1) same card) and "455"/\$.ccls.	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 14:21
S456	2	"20120080522"	US- PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/07/24 14:26

## EAST Search History (Interference)

Ref	Hits	Search Query	DBs	Default	Plurals	Time
-----	------	--------------	-----	---------	---------	------



#				Operator		Stamp
S70	29199	code.clm. same request.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S71	3300	code.clm. same payment.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:34
S72	14468	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:35
S73	2284	memory same network same parameter\$1 same card	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S74	73	memory same storing same card same ((payment or transaction) near10 data) same instructions	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S75	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:38
S77	21580	(235/375,380,382,492,383,486,487).OCLS.	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:39
S78	212	S72 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S79	469	S70 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S80	404	S71 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S81	19	S74 and S77	US- PGPUB; USPAT; UPAD	OR	OFF	2012/10/22 14:40
S421	31139	code.clm. same request.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S422	3558	code.clm. same payment.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S423	15293	code.clm. same selection\$1.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S424	2521	memory same network same parameter\$1	US-	OR	OFF	2013/04/01

		same card	PGPUB; USPAT; UPAD			09:39
S425	82	memory same storing same card same ((payment or transaction) near10 data) same instructions	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S426	25	(IC adj2 card) same (mbyte\$1 or gbyte\$1) same capacity	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S427	22443	(235/375,380,382,492,383,486,487).CCLS.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S428	222	S423 and S427	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S429	499	S421 and S427	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S430	437	S422 and S427	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S431	19	S425 and S427	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 09:39
S432	0	"L26" and portable.clm. and carrier.clm.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
S433	783	"S113" and ((power or sleep) same zero)	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
S434	17	((portable or mobile) near30 payment near30 memory) and (Mbyte\$1 or Gbyte\$1)	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:24
S435	787	(portable or mobile) near30 payment near30 memory	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
S436	8880	(235/380,382).CCLS.	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25
S437	92	S435 and S436	US- PGPUB; USPAT; UPAD	OR	OFF	2013/04/01 10:25

2/ 4/ 2014 9:35:34 AM

C:\Users\tle4\Documents\EAST\Workspaces\13438754.wsp

**REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL  
(Submitted Only via EFS-Web)**

Application Number	13/438,754	Filing Date	2012-04-03	Docket Number (if applicable)	4037-0003	Art Unit	2887
First Named Inventor	Patrick Sandor Racz			Examiner Name	Thien Minh Le		

**This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.**  
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

**SUBMISSION REQUIRED UNDER 37 CFR 1.114**

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_

Other \_\_\_\_\_

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other \_\_\_\_\_

**MISCELLANEOUS**

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months \_\_\_\_\_  
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other \_\_\_\_\_

**FEES**

**The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 501860

**SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED**

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/ Michael R. Casey /	Date (YYYY-MM-DD)	2014-03-21
Name	Michael R. Casey	Registration Number	40294

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re PATENT Application of:	Confirmation No.:	3525	
Patrick Sandor Racz	Attorney Docket:	4037-0003	
Appl. S.N.:	13/438,754	Group Art Unit:	2887
Filing Date:	April 3, 2012	Examiner:	Le, Thien Minh
Title:	DATA STORAGE AND ACCESS SYSTEMS	Date:	03/21/2014

**INFORMATION DISCLOSURE STATEMENT**

Hon. Commissioner of Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

Pursuant to 37 C.F.R. § 1.56, the attention of the Patent and Trademark Office is hereby directed to the reference(s) listed on the attached PTO-1449. One copy of each non-U.S. Patent reference is attached. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the reference(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

The submission of any document herewith, which is not a statutory bar, is not intended that any such document constitutes prior art against any of the claims of the present application or is considered to be material to patentability as defined in 37 C.F.R. § 1.56(b). Applicants do not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference against the claims of the present application.

In re Application of: Patrick Sandor Racz  
Application S.N.: 13/438,754  
Page 2 of 2

This Information Disclosure Statement (IDS) is being filed within three (3) months of the U.S. filing date OR before the mailing date of a first Office Action on the merits after an RCE. No certification or fee is required.

<b>CHARGE STATEMENT:</b> Deposit Account No. 501860, order no. <b>4037-0003</b> .
The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 ( <u>missing or insufficiencies only</u> ) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/Order Nos. shown above, for which purpose a <u>duplicate</u> copy of this sheet is attached
<b>This CHARGE STATEMENT <u>does not authorize</u> charge of the <u>issue fee</u> until/unless an issue fee transmittal sheet is filed.</b>

CUSTOMER NUMBER <b>42624</b>
---------------------------------

Davidson Berquist Jackson & Gowdey LLP  
4300 Wilson Blvd., 7th Floor,  
Arlington Virginia 22203  
Main: (703) 894-6400 • FAX: (703) 894-6430

Respectfully submitted,

By: / Michael R. Casey /

---

Michael R. Casey  
Registration No.: 40,294

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 1 of 28

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	1-1	US-2002/0032059	2002/03/14	Sugimura et al.
	1-2	US-4367402	1983/01/04	Giraud et al.
	1-3	US-4677657	1987/06/30	Nagata et al.
	1-4	US-4755660	1988/07/05	Nakano
	1-5	US-4822984	1989/04/18	Remery et al.
	1-6	US-4827512	1989/05/02	Hirokawa et al.
	1-7	US-4885788	1989/12/05	Takaragi et al.
	1-8	US-4887234	1989/12/12	Iijima
	1-9	US-4910393	1990/03/20	Gercekci et al.
	1-10	US-4959788	1990/09/25	Nagata et al.
	1-11	US-4968873	1990/11/06	Dethloff et al.
	1-12	US-5122643	1992/06/16	Gamou et al.
	1-13	US-5126541	1992/06/30	Shinagawa
	1-14	US-5140517	1992/08/18	Nagata et al.
	1-15	US-5185798	1993/02/09	Hamada et al.
	1-16	US-5200600	1993/04/06	Shinagawa
	1-17	US-5212369	1993/05/18	Karlisch et al.
	1-18	US-5247163	1993/09/21	Ohno et al.
	1-19	US-5252812	1993/10/12	Nakamura
	1-20	US-5276903	1994/01/04	Shinagawa
	1-21	US-5283885	1994/02/01	Hollerbauer
	1-22	US-5285055	1994/02/08	Oonakahara et al.
	1-23	US-5293424	1994/03/08	Holtey et al.
	1-24	US-5349649	1994/09/20	Iijima
	1-25	US-5365047	1994/11/15	Yamaguchi
	1-26	US-5379344	1995/01/03	Larsson et al.

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.



**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 2 of 28

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	2-1	US-5401945	1995/03/28	Buschmann et al.
	2-2	US-5420912	1995/05/30	Kopp et al.
	2-3	US-5426432	1995/06/20	Sanemitsu
	2-4	US-5442704	1995/08/15	Holtey
	2-5	US-5511000	1996/04/23	Kaloi, et al.
	2-6	US-5511023	1996/04/23	Schrenk
	2-7	US-5523794	1996/06/04	Mankovitz et al.
	2-8	US-5557679	1996/09/17	Julin et al.
	2-9	US-5606143	1997/02/25	Young
	2-10	US-5610774	1997/03/11	Hayashi et al.
	2-11	US-5636276	1997/06/03	Brugger
	2-12	US-5664228	1997/09/02	Mital
	2-13	US-5686714	1997/11/11	Abe et al.
	2-14	US-5687398	1997/11/11	Martineau
	2-15	US-5737571	1997/04/07	Fukuzumi
	2-16	US-5763869	1998/06/09	Moll et al.
	2-17	US-5802325	1998/09/01	Le Roux
	2-18	US-5825875	1998/10/20	Ugon
	2-19	US-5825882	1998/10/20	Kowalski et al.
	2-20	US-5841979	1998/11/24	Schulhof, et al.
	2-21	US-5844281	1998/12/01	Kawan et al.
	2-22	US-5856699	1999/01/05	Drupsteen et al.
	2-23	US-5892975	1999/04/06	Barnes
	2-24	US-5896507	1999/04/20	Martineau
	2-25	US-5911031	1999/06/08	Young-Man Lee
	2-26	US-5943423	1999/08/24	Sead Muftic

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 3 of 28

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication/ Issue Date	Name of Patentee or Applicant of Cited Document
	3-1	US-5960082	1999/09/28	Haenel
	3-2	US-5963980	1999/10/05	Coulier et al.
	3-3	US-5972738	1999/08/24	Cesarie et al.
	3-4	US-5995965	1999/11/30	Bettina Experton
	3-5	US-6003113	1999/12/14	Hoshino
	3-6	US-6005942	1999/12/21	Chan et al.
	3-7	US-6032857	2000/03/07	Kitagawa et al.
	3-8	US-6289711 B1	2004/12/07	Kwok et al
	3-9	US-6314409 B2	2001/11/06	Schneck, et al.
	3-10	US-6449684	2002/09/10	MacSmith et al.
	3-11	US-6532518	2003/03/11	MacSmith et al.
	3-12	US-6697944 B1	2004/02/24	Jones et al.
	3-13	US-6880761 B1	2005/04/19	Ritter et al.
	3-14	US-8033458	2011/10/11	Racz
	3-15	US-8061598	2011/11/22	Racz
	3-16	US-8118221	2012/02/21	Racz
	3-17	US-8336772	2012/12/25	Racz
	3-18			
	3-19			
	3-20			
	3-21			
	3-22			
	3-23			
	3-24			
	3-25			
	3-26			

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 4 of 28

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication Date	Name of Patentee or Applicant of Cited Document	Notes
	4-1	CA 2294721	1998/12/23	Ritter et al.	
	4-2	EP 0159539 B1	1990/09/12	Siemens Aktiengesellschaft	PT/SOR
	4-3	EP 0162221 B1	1992/11/11	Yoshida et al.	
	4-4	EP 0275510 B1	1992/10/21	Abraham et al.	
	4-5	EP 0328289 B2	1998/03/04	Shinagawa	
	4-6	EP 0354793 B1	1996/10/23	Shinagawa	
	4-7	EP 0536792 B1	1998/03/18	Hayashi et al.	
	4-8	EP 0809221	1997/11/26	Poggio	
	4-9	EP 0819287 B1	1998/01/21	Heyns et al.	
	4-10	EP 0913789 A2	1999/05/06	Neilsen	
	4-11	EP 0949595 A2	1999/10/13	Pan et al.	
	4-12	EP 1003135 A1	2000/05/24	Sarradin	SOR
	4-13	EP 1004992 A2	2000/05/31	Chan et al.	
	4-14	GB 2082816 A	1982/03/10	Halpern	
	4-15	GB 2092353 B	1984/05/31	Chalmers	
	4-16	GB 2107500 B	1985/09/11	Bernstein	
	4-17	GB 2204973 A	1988/11/23	Steiner et al.	
	4-18	GB 2274009 B	1992/12/29	Payne	
	4-19	JP 10-269289	1998/10/09	Kouichi	SOR/T
	4-20	WO 01/031599	2001/05/03	Racz et al.	
	4-21	WO 9527955	1995/10/19	Hummerston et al.	
	4-22	WO 9619771	1996/06/27	Weiner	
	4-23	WO 9625724	1996/08/22	Heyns et al.	
	4-24	WO 97/02548	1997/01/23	Everett et al.	
	4-25	WO 9809257	1998/03/05	Lisimaque et al.	
	4-26	WO 9819237	1998/05/07	Wilkinson	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
FORM PTO-1449 (modified)

Sheet 5 of 28

Application No.	13/438,754
Filing Date	April 3, 2012
First Named Inventor	Patrick Sandor Racz
Group Art Unit	2887
Examiner Name	Le, Thien Minh
Attorney Docket No.	4037-0003
Confirmation No.	3525

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Document No.	Publication Date	Name of Patentee or Applicant of Cited Document	Notes
	5-1	WO 9825238	1998/06/11	Clewits	
	5-2	WO 9833343	1998/07/30	Lehmus	
	5-3	WO 9837526	1998/08/27	Everett et al.	
	5-4	WO 9843212	1998/10/01	Chan et al.	
	5-5	WO 9852152	1998/11/19	Richards et al.	
	5-6	WO 9852153	1998/11/19	Richards	
	5-7	WO 9852158	1998/11/19	Everett et al.	
	5-8	WO 9852159	1998/11/19	Everett et al.	
	5-9	WO 9852160	1998/11/19	Everett et al.	
	5-10	WO 9852161	1998/11/19	Richards	
	5-11	WO 9852162	1998/11/19	Everett et al.	
	5-12	WO 9852163	1998/11/19	Richards et al.	
	5-13	WO 9922516	1999/05/06	Sarfati	
	5-14	WO 9946682	1999/09/16	Lindley et al.	
	5-15	WO 9946727	1999/09/16	Bright	
	5-16	WO 9948250	1999/09/23	Higginson et al.	
	5-17	WO 9962210	1999/12/02	DiGiorgio et al.	
	5-18				
	5-19				
	5-20				
	5-21				
	5-22				
	5-23				
	5-24				
	5-25				
	5-26				

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525

Sheet 6 of 28

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	6-1	About MultiMedia Cards ( <a href="http://www.mmca.org/whatisa.htm">http://www.mmca.org/whatisa.htm</a> ), dated April, 23, 1999	
	6-2	Actiontec to Deploy Wave Systems' EMBASSY E-Commerce Technology in Home Networking and Modem Cards, May 11, 1999	
	6-3	Aladdin and Wave Complete Security Technology Integration, Jan. 27, 1998	
	6-4	Amendment 1 to SDMI Portable Device Specification, Part I, Version 1.0, Sep. 1999	
	6-5	An introduction to BPI statistics - Printed on 6/27/2000	
	6-6	Answers to Frequently Asked Questions About Smart Cards, 1996	
	6-7	Atmel and Wave Systems Corp. Partner to Provide Advanced "E-Commerce on a Chip" Solution, May 10, 1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 7 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	7-1	Automatic Fare Collection ( <a href="http://www.oti.co.il/automatic_fare_collection.html">http://www.oti.co.il/automatic_fare_collection.html</a> ), printed Jan. 5, 2000	
	7-2	Breakthrough For E-Commerce Over DTV Proven in Test with New Jersey Public Television, Mar. 28, 2000	
	7-3	Capital Broadcasting Unit, DTV Plus & WaveXpress Form Strategic Partnership to Explore & Deliver Broadcast E-commerce, Mar. 30, 2000	
	7-4	ChipCASH: Making stored value work, printed Aug. 18, 2000	
	7-5	Creative Nomad World ( <a href="http://www.nomadworld.com/products/welcome.html">http://www.nomadworld.com/products/welcome.html</a> ), printed on 11/22/99	
	7-6	Creative Secures MP3 Player, November 12, 1999	
	7-7	CREATIVE TECHNOLOGIES CHOOSES WAVE SYSTEMS CORP. FOR MICRO-TRANSACTION SELLING AND PURCHASING, dated March 12, 1997	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 8 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	8-1	Creative Unveils Next Generation Portable Digital Audio Player, October 6, 1999	
	8-2	Cyber-COMM Frequently Asked Questions (FAQ), printed Apr. 27, 2000	
	8-3	Cyber-COMM Selects Wave Systems to Provide Trusted E-Commerce Infrastructure in Europe, Sep. 29, 1999	
	8-4	Digital Rights Management - Printed on 10/17/2000	
	8-5	E-COMMERCE: Companies 'not investing enough', October 14, 1999	
	8-6	Electronic Purse ( <a href="http://www.oti.co.il/electronic_purse.html">http://www.oti.co.il/electronic_purse.html</a> ), printed Jan. 5, 2000	
	8-7	empeg car - Printed on 11/22/99	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 9 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	9-1	Emphasis on Internet ID and Authentication Central to the Smart Card Forum Strategic Direction for 2000, September 22, 1999	
	9-2	ePanorama - Card Technology Technology Page, printed May, 1, 2000	
	9-3	Ericsson demonstrates plug-in MP3 player for mobile phones at Telecom 99 ( <a href="http://www.mmca.org/Press/ericsson-mp3.htm">http://www.mmca.org/Press/ericsson-mp3.htm</a> ), October 9, 1999	
	9-4	FAQ for alt.technology.smartcards ( <a href="http://www.ioc.ee/atssc/faq.html">http://www.ioc.ee/atssc/faq.html</a> ), printed on 11/30/2000	
	9-5	Flash and EEPROM: the never-ending tradeoff - August 1997	
	9-6	Flash Card Market Will Boom To \$1.3 Billion By 2002, Predicts IDC - December 3, 1998	
	9-7	Frequently Asked Questions ( <a href="http://www.scia.org/knowledgebase/aboutSmartCards/faqs.htm">http://www.scia.org/knowledgebase/aboutSmartCards/faqs.htm</a> ), printed on 11/30/2000	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.



<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 10 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	10-1	Gadgets Galore from Comdex ( <a href="http://www.wired.com/news/mp3/0,1285,32573,00.html">http://www.wired.com/news/mp3/0,1285,32573,00.html</a> ), November 17, 1999	
	10-2	GlobalWave- Secure Digital Media Distribution; printed May 15, 2000	
	10-3	Growing Number of On-Line Users Turn Digital Content Into Cash Using MyPublish from Wave Systems, Feb. 22, 2000	
	10-4	Guide to the SDMI Portable Device Specification - Part 1, Version 1.0 (date unknown)	
	10-5	Heer, D.N.; Maher, D.P.; IEEE Transactions on Consumer Electronics, Volume: 41, Issue: 3, 1995, Pages: 869 - 874	
	10-6	Heer, D.N.; Maher, D.P.; Takahashi, R.; Proceedings of International Conference on Consumer Electronics, 1995, pgs. 382-383.	
	10-7	How DRM commerce works ( <a href="http://www.intertrust.com/main/technology/howdrmcworks.html">http://www.intertrust.com/main/technology/howdrmcworks.html</a> ) - archived on 10/18/2000	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 11 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	11-1	HP and Wave Systems to Bring Trust And Security to the PC, Oct. 27, 1998	
	11-2	HP Offers secure PC for ecommerce, available by at least Apr. 27, 2000	
	11-3	HP, RSA Data Security and Wave Systems to Enable Enhanced Security for E-Mail and Internet Transactions, Jan 20, 1999	
	11-4	IBM forays into digital music software, February 8, 1999	
	11-5	IGST to Incorporate Wave Systems' EMBASSY Technology in Multimedia Chips for Set-Top Boxes, Dec. 2, 1998	
	11-6	I-Jam's New MP3 Internet Music Player will use SanDisk Multimedia Cards to Download and Store Music - June 14, 1999	
	11-7	Industry Specific Smart Card Specifications ( <a href="http://www.scia.org/knowledgebase/aboutSmartCards/specs.html">http://www.scia.org/knowledgebase/aboutSmartCards/specs.html</a> ), printed on 11/30/2000	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 12 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	12-1	Internet and Smart Card Application Deployment ( <a href="http://www.smartcardcentral.com/technical/articles/jsourc/jsourc_080999.asp">http://www.smartcardcentral.com/technical/articles/jsourc/jsourc_080999.asp</a> ), archived August 1999	
	12-2	Internet Audio Portables: A Christmas Buying Guide, printed Jan. 5, 2000	
	12-3	Intertrust technology - archived on 10/18/2000	
	12-4	ITE to Embed Wave System Corp.'s Embassy Technology into Integrated Circuits, Nov. 9, 1998	
	12-5	JazPiper FAQ ( <a href="http://www.jazpiper.nl/en_ie/faq.htm">http://www.jazpiper.nl/en_ie/faq.htm</a> ), printed on 11/22/99	
	12-6	Joint Press Release by Infineon Technologies and Grundig - August 27, 1999	
	12-7	Joint Press Release by Infineon Technologies and Hitachi - April 22, 1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 13 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	13-1	Launch Discover New Music ( <a href="http://www.launch.com/music/mymusic/pvn_content/0,3349,,00.html">http://www.launch.com/music/mymusic/pvn_content/0,3349,,00.html</a> ), January 4, 2000	
	13-2	Liquid Audio signs with EMI, June 17, 1999, pp. 1-2	
	13-3	Major Companies Join Forces to Solve Security, Trust, and Privacy Issues in Electronic Business, Aug. 24, 1999	
	13-4	Microsoft Ups Commitment to Digital Media ( <a href="http://www.billboard.com/sites/archive/00/0526.asp">http://www.billboard.com/sites/archive/00/0526.asp</a> ), May 26, 2000	
	13-5	Ministry of Sound's Content Library to Become Available to RioPort Audience and Distribution Partners, November 15, 1999	
	13-6	More popular than Sex ( <a href="http://www.wired.com/news/business/0,1367,31834,00.html">http://www.wired.com/news/business/0,1367,31834,00.html</a> ), October 14, 1999	
	13-7	MP3 catalyzing Net music's future, April 27, 1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 14 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	14-1	MP3 device makers win key court ruling, June 15, 1999	
	14-2	MP3: on the road again, November 22, 1999	
	14-3	MP3s Anywhere You Are ( <a href="http://www.wired.com/news/mp3/0,1285,32109,00.html">http://www.wired.com/news/mp3/0,1285,32109,00.html</a> ), October 28, 1999	
	14-4	MultiMedia Card: The Storage Medium ( <a href="http://www.pontis.de/site_e/produkte/ca_mmc_e.htm">http://www.pontis.de/site_e/produkte/ca_mmc_e.htm</a> ), printed Jan. 4, 2000	
	14-5	Music a la Card ( <a href="http://www.mplayer3.com/site_e/ho_pl_e.htm">http://www.mplayer3.com/site_e/ho_pl_e.htm</a> ), printed on 11/22/99	
	14-6	Music Battle Takes to the Hill ( <a href="http://www.wired.com/news/politics/0,1283,32008,00.html">http://www.wired.com/news/politics/0,1283,32008,00.html</a> ), October 20, 1999	
	14-7	Music to Microsoft's Ears ( <a href="http://www.wired.com/news/culture/0,1284,32379,00.html">http://www.wired.com/news/culture/0,1284,32379,00.html</a> ), November 15, 1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 15 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	15-1	NATIONAL SEMICONDUCTOR® AND WAVE SYSTEMS TO DEVELOP CO-PROCESSOR-BASED SECURITY SOLUTIONS FOR E-COMMERCE, dated Sep. 15, 1999	
	15-2	Net music changing copyrights, April 27, 1999	
	15-3	New Media Age - p. 23 - November 18, 1999	
	15-4	PC Free and Wave Systems to Deliver Bundles "E-Commerce PC", June 9, 1999	
	15-5	PCT/GB00/04110, International Search Report mailed February 13, 2000	
	15-6	Personal Jukebox PJB-100 - Printed on 11/22/99	
	15-7	Piracy (RIAA Webpage: <a href="http://www.riaa.com/piracy/piracy.htm">http://www.riaa.com/piracy/piracy.htm</a> ), printed on 11/25/1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 16 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	16-1	Piracy Definitions - Printed on 6/27/2000	
	16-2	Portable MP3 Players and More ( <a href="http://www.pontis.de/site_e/produkte/sh_prl_e.htm">http://www.pontis.de/site_e/produkte/sh_prl_e.htm</a> ), printed Jan. 4, 2000	
	16-3	PortalPlayer Announces Collaboration with SanDisk Corporation to Enable New Classes of Consumer Electronic Devices for Music Playback - December 8, 1999	
	16-4	Prepaid smart card techniques: A brief introduction and comparison - dated 1994	
	16-5	Programming Plus Digital Content: A New Business Model for Television, printed Apr. 27, 2000	
	16-6	PSXAMP - Printed on 11/22/99	
	16-7	Reciprocal - Driving the content economy (date unknown)	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 17 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	17-1	Research and Intellectual Property ( <a href="http://www.intertrust.com/main/technology/research-ip.html">http://www.intertrust.com/main/technology/research-ip.html</a> ) - Printed on 10/18/2000	
	17-2	RIAA wins restraining order against MP3 recording device, RIAA Press Release - 10/16/1998	
	17-3	Rio 500 (from archive.org archived Nov 28, 1999 but original date unknown)	
	17-4	RIOPORT SELECTS MAGEX TO PROVIDE DIGITAL RIGHTS MANAGEMENT SOLUTION FOR DIGITAL AUDIO DELIVERY, PLAYBACK USING RIOPORT PLATFORM AND INTERTRUST TECHNOLOGY, November 15, 1999	
	17-5	RioPort Shows Secure Solution for Downloading and Playing Back Windows Media Format Music and Spoken Word Tracks from Internet to Desktop, November 15, 1999	
	17-6	RIOPORT, INC. COLLABORATES WITH MICROSOFT ON TECHNOLOGY TO SEAMLESSLY DELIVER SECURE DIGITAL AUDIO CONTENT TO A VARIETY OF EXTERNAL PLAYBACK DEVICES, November 10, 1999	
	17-7	Rioport: About us ( <a href="http://www.rioport.com/RioAbout/0,1202,,00.htm">http://www.rioport.com/RioAbout/0,1202,,00.htm</a> ), printed on 11/22/99	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.



<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 18 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	18-1	S3 hears sweet music with MP3 plans ( <a href="http://news.cnet.com/news/0-1006-200-1711701.html">http://news.cnet.com/news/0-1006-200-1711701.html</a> ), April 18, 2000	
	18-2	Samsung and Sony Announce Memory Stick Collaboration, <a href="http://www.samsung.com/news/samsung/2001/sec0803-20010803102150.html">http://www.samsung.com/news/samsung/2001/sec0803-20010803102150.html</a> , pp. 1-2, Aug. 3, 2001	
	18-3	Samsung Yepp Features ( <a href="http://www.samsungyepp.com/Yepp64.html">http://www.samsungyepp.com/Yepp64.html</a> ), archived Mar. 4, 2000	
	18-4	SanDisk Announces Development of the World's First Floppy Disk Adapter for Multimediacards, July 19, 1999	
	18-5	SanDisk Will Supply I&C with Multimediacards for new portable MP3 Internet Music Players, June 23, 1999	
	18-6	SanDisk Will Supply Maycom with 32 MB Multimediacard for Use with New Merit, April 27, 1999	
	18-7	Sarnoff and Wave Systems to Form inTelecast, April 19, 1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 19 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	19-1	SDMI announces portable device technology will be available ( <a href="https://www.sdmi.org/dscgl/ds.py/Get/File-646/nyc-99-09-24-press-release.htm">https://www.sdmi.org/dscgl/ds.py/Get/File-646/nyc-99-09-24-press-release.htm</a> ), 9/24/1999	
	19-2	SDMI approves technology selection, 11/12/1999	
	19-3	SDMI fact sheet, printed on 11/25/1999	
	19-4	SDMI FAQ (date unknown)	
	19-5	SDMI IDENTIFIES AUDIO WATERMARK TECHNOLOGY FOR NEXT GENERATION PORTABLE DEVICES FOR DIGITAL MUSIC, 8/9/1999	
	19-6	SDMI Member Company Statements On the SDMI Portable Device Specification Release (date unknown)	
	19-7	SDMI Participant List ( <a href="http://www.sdmi.org/participant_list.htm">http://www.sdmi.org/participant_list.htm</a> ), dated May 24, 2000	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 20 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	20-1	SDMI Portable Device Specification - Part 1, Version 1.0, dated July 8, 1999	
	20-2	SDMI Publishes Open Standard for Portable Devices, July 13, 1999	
	20-3	SDMI Working group structure ( <a href="http://www.sdmi.org/work_group_struct.htm">http://www.sdmi.org/work_group_struct.htm</a> ), updated June 1, 2000	
	20-4	Shaw, I., Cash on Delivery - Mobile Consumer Management Goes Back to Basics (1994)	
	20-5	Smart Card Forum - <a href="http://www.smartcardforum.org/aboutscf/backgrd.htm">http://www.smartcardforum.org/aboutscf/backgrd.htm</a> , printed Nov. 30, 2000	
	20-6	Smart Card Overview ( <a href="http://www.scia.org/knowledgebase/aboutSmartCards/primer.htm">http://www.scia.org/knowledgebase/aboutSmartCards/primer.htm</a> ), printed on 11/30/2000	
	20-7	Smart Cards on Line ( <a href="http://www.smartex.com">http://www.smartex.com</a> ), dated Aug. 18, 2000	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 21 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	21-1	Smartflash LLC et. al. v. Apple Inc., Case No. 6:13cv00447-MHS-KNM, Exhibit B to Defendants' Preliminary Invalidation Contentions	
	21-2	Smartflash LLC et. al. v. Apple Inc., Case No. 6:13cv00447-MHS-KNM, Exhibit E to Defendants' Preliminary Invalidation Contentions	
	21-3	Smartflash LLC et. al. v. Apple Inc., Case No. 6:13cv00447-MHS-KNM, Exhibit F to Defendants' Preliminary Invalidation Contentions	
	21-4	Smartflash LLC et. al. v. Apple Inc., Case No. 6:13cv00447-MHS-KNM, Exhibit H to Defendants' Preliminary Invalidation Contentions	
	21-5	Sonicnet Music News, ( <a href="http://partners.sonicnet.com/ap/rioreport/newstory.jhtml?id=620291">http://partners.sonicnet.com/ap/rioreport/newstory.jhtml?id=620291</a> ), pp.1-2, Jan 7. 2000	
	21-6	Standard Microsystems and Wave Systems Agree to Embed Wave's "WaveMeter" Technology in Standard Microsystems Integrated Circuits, May 28, 1998	
	21-7	T3 News, July, 1999, pgs. 29-30	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 22 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	22-1	Technology Standards Developed for Music Delivery System over Mobile Phones - December 9, 1999	
	22-2	The MP3 Place ( <a href="http://www.mp3hardware.com/clickman.shtml">http://www.mp3hardware.com/clickman.shtml</a> ), printed on 11/22/99	
	22-3	The ROS-Card: the audio storage media of the future ( <a href="http://www.mplayer3.com/site_e/ho_ros_e.htm">http://www.mplayer3.com/site_e/ho_ros_e.htm</a> ), printed Nov. 22, 1999	
	22-4	The storage medium: MultiMediaCard ( <a href="http://www.mplayer3.com/site_e/ho_mmc_e.htm">http://www.mplayer3.com/site_e/ho_mmc_e.htm</a> ), printed on 11/22/99	
	22-5	The technology behind the world's first consumer trial of mobile electronic cash, printed 9/25/1999	
	22-6	The top 50 bootlegged artists in the UK, printed 11/25/1999	
	22-7	The Trusted Client from Wave Systems Corp. Web Site ( <a href="http://www.wavesys.com/news/featuredstory.html">http://www.wavesys.com/news/featuredstory.html</a> ), printed May 15, 2000	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 23 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	23-1	The Trusted Client from Wave Systems Corp. Web Site ( <a href="http://www.wavesys.com/technology/embassytc1.html">http://www.wavesys.com/technology/embassytc1.html</a> ), archived May 20, 2000	
	23-2	The World Market in Review, archived Mar. 3, 2000	
	23-3	The World of Multos ( <a href="http://www.multos.com/multoglobe.ihtml">http://www.multos.com/multoglobe.ihtml</a> ), printed Jan. 5, 2000	
	23-4	THEGLOBE.COM and Wave Systems Offer Internet Industry's First e-Commerce Service for the Sale of Personal Digital Content, Apr. 22, 1999	
	23-5	There is a DIVA in my pocket - Printed on 11/22/99	
	23-6	Thomson Lrya ( <a href="http://www.vitaminic.co.uk/hardware/lyra.shtml">http://www.vitaminic.co.uk/hardware/lyra.shtml</a> ), printed on 11/22/99	
	23-7	Uskela, S., Services in Cellular Packet Data Networks, Masters Thesis, Helsinki University of Technology (Sept. 1999)	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 24 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	24-1	Verifides Technology - Secure Information Sharing via Technology Enforced Originator Control (date unknown)	
	24-2	Wave - Wave Digital Network (dated 2000)	
	24-3	Wave Systems and IBM to Collaborate on Technology for Accessing Digital Content, Dec. 18, 1997	
	24-4	Wave Systems and Sarnoff Corporation Announce Board of Directors for WaveXpress Joint Venture, Sep. 9, 1999	
	24-5	Wave Systems Announces Agreement with KISS Nordic A/S to Bundle Wave's E-Commerce System with KISS Nordic Multimedia Products, Aug. 28, 1999	
	24-6	Wave Systems Announces New Technology Enabling Secure Electronic Commerce Transactions in the PC, Oct. 27, 1998	
	24-7	Wave Systems Announces Support of SDMI Specification, July 13, 1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 25 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	25-1	Wave Systems Appoints Alan Chaplin Vice President of Entertainment Service, May 11, 1999	
	25-2	Wave Systems Continues US Momentum In Europe by Showcasing Digital Content Distribution and E-Commerce Technology with GlobalWave at Milia 2000, Feb. 16, 2000	
	25-3	Wave Systems Corp. Announces Three Pay-Per-Use CD-ROM Software Publishing Partners, Feb. 10, 1997	
	25-4	Wave Systems Corp. Debuts Micro-Transaction System for Purchasing Digital Content, Feb. 10, 1997	
	25-5	Wave Systems Corp. Enhances Consumer-Publisher Relationships with Upgraded Great Stuff Network Technology, Mar. 4, 1998	
	25-6	Wave Systems Corp. Forges Strategic Relationship With Leading Broadcast Systems Solution Provider, Apr. 7, 1998	
	25-7	Wave Systems Demonstrates Trusted Client Services and Applications at Comdex, Nov. 15, 1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.



<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 26 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	26-1	Wave Systems Introduces MyPublish Community E-Commerce Service, Apr. 22, 1999	
	26-2	Wave Systems Introduces WaveDirect E-Commerce Service for PC Users, June 1, 1999	
	26-3	Wave Systems Plans to Acquire N*Able Technologies, June 14, 1999	
	26-4	Wave Systems Reports 1998 Results, Apr. 1, 1999	
	26-5	Wave Systems Signs Letter of Intent with Lego Media International to Deliver Software by Satellite for Europe Online Networks, Aug. 28, 1999	
	26-6	Wave Systems To Integrate Sun Microsystem's Java Card Technology Into Consumer Devices to Extend EMBASSY E-Commerce Solutions, May 10, 1999	
	26-7	Wave Systems to Offer Interactive Magic Software Titles Through Innovative WaveMeter Distribution System, June 15, 1998	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
	Confirmation No.	3525
Sheet 27 of 28		

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	27-1	Wave Systems to Participate in Trusted Computing Platform, Oct. 11, 1999	
	27-2	WaveEnabled Trusted Client Applications, from Wave Systems Corp. Web Site ( <a href="http://www.wavesys.com/technology/embassytc2.html">http://www.wavesys.com/technology/embassytc2.html</a> ), archived May 26, 2000	
	27-3	Wave's Embassy Technology Demonstrated in Compaq Smart Card Readers at Windows 2000 Launch, Feb. 17, 2000	
	27-4	WaveSystems Supports IBM Initiative to Embed Security in the PC, Sep. 28, 1999	
	27-5	Which Net music technology will win, May 7, 1999	
	27-6	Who's Gonna Own the Music ( <a href="http://www.wired.com/news/culture/0,1284,31682,00.html">http://www.wired.com/news/culture/0,1284,31682,00.html</a> ), October 18, 1999	
	27-7	Worldwide music industry coordinates its strategy againts piracy, RIAA Press Release, 10/28/1999	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> FORM PTO-1449 (modified)	Application No.	13/438,754
	Filing Date	April 3, 2012
	First Named Inventor	Patrick Sandor Racz
	Group Art Unit	2887
	Examiner Name	Le, Thien Minh
	Attorney Docket No.	4037-0003
Sheet 28 of 28	Confirmation No.	3525

NON-PATENT REFERENCES			
Examiner Initials*	Cite No.	Non-patent Reference bibliographic information, where available	Notes
	28-1	www.thenetnow.co.uk - MP3 Players - p.144 - 145 (date unknown)	
	28-2	X-Card - The Pocket smart card reader/Euro converter (date unknown)	
	28-3	X-Collection - Handy-Sized Smart Card Reader (date unknown)	
	28-4	X-Sign (date unknown)	
	28-5	X-Smart - Smart Card Reader/Writer (date unknown)	
	28-6	YP-E32 ( <a href="http://yepp.co.kr/eng/pd.html">http://yepp.co.kr/eng/pd.html</a> ) - Printed on 11/22/99	
	28-7	Zappee ZMP 3000 ( <a href="http://www.zappee.com/html/body_mp3_hardware.html">http://www.zappee.com/html/body_mp3_hardware.html</a> ), printed on 11/22/99	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*Examiner: Initial if reference was considered, whether or not citation is in conformance with MPEP 609. Draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant. Notes: If identified, the following is provided: EA = English Abstract, T = Translation, PT = Partial Translation, SOR = Statement of Relevancy, PF = Patent Family.

(12)

(21) **2 294 721**

(22) **16.06.1997**

(51) Int. Cl.<sup>7</sup>: **H04Q 007/32, G06K 019/07,  
G07F 007/10**

(85) **13.12.1999**

(86) **PCT/CH97/00237**

(87) **WO98/58509**

(71) **SWISSCOM AG,  
Viktoriastrasse 21  
CH-3050, BERN, XX (CH).**

**RITTER, RUDOLF (CH).  
BOUQUET, HANSPETER (CH).  
HEUTSCHI, WALTER (CH).**

(72)

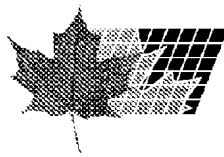
(74) **MACRAE & CO.**

(54) **CARTE A PUCE ET PROCEDE DE COMMUNICATION ENTRE UN DISPOSITIF EXTERNE ET UNE CARTE A PUCE**

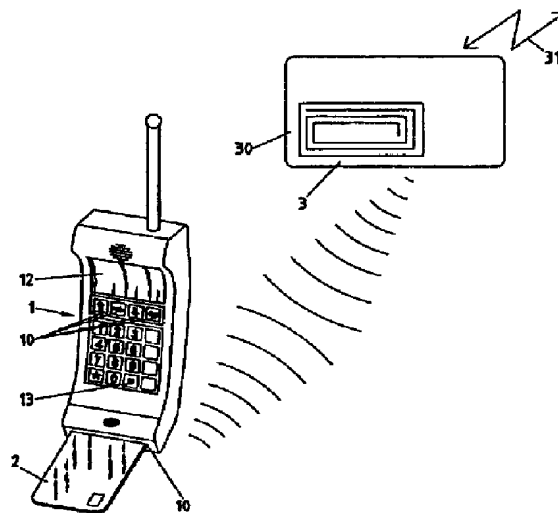
(54) **CHIP CARD AND METHOD FOR COMMUNICATION BETWEEN AN EXTERNAL DEVICE AND A CHIP CARD**

(57)

The invention relates to an SIM (Subscriber Identity Module ) chip card for GSM cellular telephones containing a data processing system (20) with memory elements (200). These memory elements enable the storage of data containing at least subscriber identification data in a telephone network. Electric contacts (24) on the surface of the chip card make it possible to exchange data between the said processing system (20) and a mobile communication station (1) into which the card can be removably inserted. The chip card furthermore contains at least one coil for establishing communication via radio waves between the said processing system and an external device (3) outside the said mobile communication station.



- (72) RITTER, RUDOLF, CH  
(72) BOUQUET, HANSPETER, CH  
(72) HEUTSCHI, WALTER, CH  
(71) SWISSCOM AG, CH  
(51) Int.Cl.<sup>7</sup> H04Q 7/32, G07F 7/10, G06K 19/07  
(54) **CARTE A PUCE ET PROCEDE DE COMMUNICATION ENTRE  
UN DISPOSITIF EXTERNE ET UNE CARTE A PUCE**  
(54) **CHIP CARD AND METHOD FOR COMMUNICATION  
BETWEEN AN EXTERNAL DEVICE AND A CHIP CARD**



(57) Cette carte à puce, qui fait partie d'un module d'identification d'abonné pour téléphones cellulaires de type GSM, contient des moyens de traitement de données (20), y compris des moyens de mémorisation (200) qui permettent de mémoriser des données contenant au moins les données d'identification d'un abonné à un réseau de télécommunications. Des contacts électriques (24) sur la surface de la carte à puce permettent d'échanger des données entre lesdits moyens de traitement de données (20) et une station mobile de communication (1) dans laquelle la carte peut être insérée de manière amovible. La carte à puce contient en outre au moins une bobine qui permet d'établir une communication par radio entre lesdits moyens de traitement de données et un dispositif externe (3) situé à l'extérieur de ladite station mobile de communication.

(57) The invention relates to an SIM (Subscriber Identity Module ) chip card for GSM cellular telephones containing a data processing system (20) with memory elements (200). These memory elements enable the storage of data containing at least subscriber identification data in a telephone network. Electric contacts (24) on the surface of the chip card make it possible to exchange data between the said processing system (20) and a mobile communication station (1) into which the card can be removably inserted. The chip card furthermore contains at least one coil for establishing communication via radio waves between the said processing system and an external device (3) outside the said mobile communication station.





**PCT**  
WELTORGANISATION FÜR GEISTIGES EIGENTUM  
Internationales Büro  
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

<p>(51) Internationale Patentklassifikation<sup>6</sup> : H04Q 7/32, G07F 7/10, G06K 19/07</p>	<p>A1</p>	<p>(11) Internationale Veröffentlichungsnummer: WO 98/58509</p> <p>(43) Internationales Veröffentlichungsdatum: 23. Dezember 1998 (23.12.98)</p>
<p>(21) Internationales Aktenzeichen: PCT/CH97/00237</p> <p>(22) Internationales Anmeldedatum: 16. Juni 1997 (16.06.97)</p> <p>(71) Anmelder (für alle Bestimmungsstaaten ausser US): GENERALDIREKTION PTT [CH/CH]; Viktoriastrasse 21, CH-3030 Bern (CH).</p> <p>(72) Erfinder; und</p> <p>(75) Erfinder/Anmelder (nur für US): RITTER, Rudolf [CH/CH]; Rossweidweg 8, CH-3052 Zollikofen (CH). BOUQUET, Hanspeter [CH/CH]; Kappelenring 49A, CH-3032 Hinterkappelen (CH). HEUTSCHLI, Walter [CH/CH]; Jungfrauweg 8, CH-3303 Jegensdorf (CH).</p> <p>(74) Anwalt: BOVARD AG; Optingenstrasse 16, CH-3000 Bern 25 (CH).</p>	<p>(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, KE, LS, MW, SD, SZ, UG), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Veröffentlicht</b> Mit internationalem Recherchenbericht. Mit geänderten Ansprüchen.</p>	

(54) Title: CHIP CARD AND METHOD FOR COMMUNICATION BETWEEN AN EXTERNAL DEVICE AND A CHIP CARD

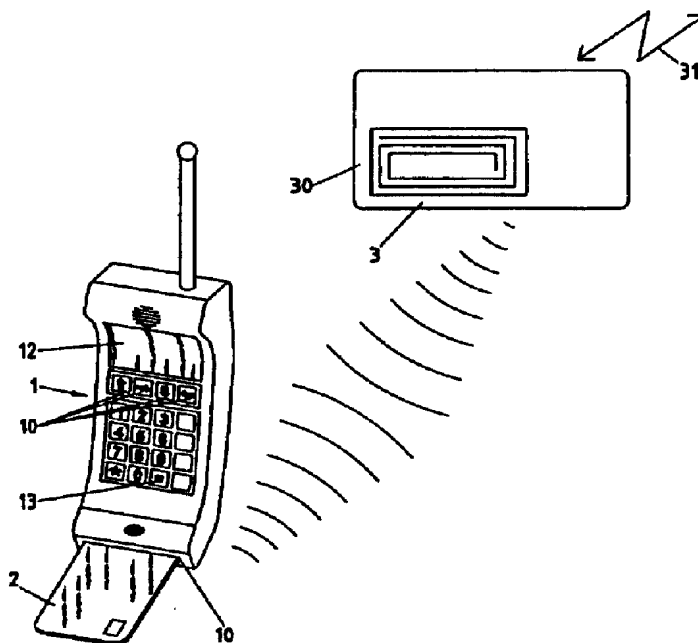
(54) Bezeichnung: CHIPKARTE UND VERFAHREN ZUR KOMMUNIKATION ZWISCHEN EINER EXTERNEN VORRICHTUNG UND EINER CHIPKARTE

(57) Abstract

The invention relates to an SIM (Subscriber Identity Module) chip card for GSM cellular telephones containing a data processing system (20) with memory elements (200). These memory elements enable the storage of data containing at least subscriber identification data in a telephone network. Electric contacts (24) on the surface of the chip card make it possible to exchange data between the said processing system (20) and a mobile communication station (1) into which the card can be removably inserted. The chip card furthermore contains at least one coil for establishing communication via radio waves between the said processing system and an external device (3) outside the said mobile communication station.

(57) Zusammenfassung

SIM (Subscriber Identity Module)-Chipkarte für GSM-Zellulartelefon, enthaltend Datenverarbeitungsmittel (20), welche Speichermittel (200) umfassen, die es erlauben, Daten zu speichern, welche mindestens Identifikationsdaten eines Abonnenten in einem Telekommunikationsnetz enthalten. Elektrische Kontakte (24) auf der Oberfläche der Chipkarte ermöglichen das Austauschen von Daten zwischen den genannten Verarbeitungsmitteln (20) und einer mobilen Kommunikationsstation (1), in welche die Karte in wegnehmbarer Weise eingeführt werden kann. Die Chipkarte enthält im weitem mindestens eine Spule, welche den Aufbau einer Kommunikation über Funkwellen zwischen den genannten Verarbeitungsmitteln und einer ausserhalb der genannten mobilen Kommunikationsstation befindlichen externen Vorrichtung (3) erlaubt.



## **Chipcard and Method for Communication Between an External Device and a Chipcard**

The present invention relates to a chipcard according to the preamble of the patent claim 1, to a mobile station according to the preamble of patent claim 7, to a device, capable of communicating with a chipcard  
5 according to the invention, as well as to various methods and applications of these methods to communication between a chipcard and an external device. More precisely, the present invention relates to the problem of communication between a chipcard and an external device, particularly a chipcard of the SIM-  
10 type, intended to be used, for instance, in a cellular phone, for example of the GSM-format.

In mobile telephone networks, such as, for example, the GSM-network (Global System for Mobile Communication), for instance, the identity of the subscribers is stored in a chipcard referred to as a SIM card (Subscriber  
15 Identity Module). The SIM card is removable, so that a user may receive the calls intended for him on the mobile device of his choice by moving the SIM card from one device to another. Furthermore, methods are known for loading the SIM card with a monetary amount in different ways as well as for charging telephone communication fees to this amount. Consequently, the mobile  
20 stations (MS), such as, for example, cellular telephones of the GSM type, are composed of two elements, the mobile device and the SIM chipcard.

Today there are two standard formats of SIM cards. The full-size format corresponds to the size of a credit card, while the plug-in format, which is adapted especially to the miniaturized portable telephones, has a size of  
25 approximately 25 mm by 10 mm. The functionality of cards in these two formats is identical.

Generally, SIM cards contain data processing means, in most cases a microcontroller integrated in a chip. These data processing means comprise, on the one hand, a zone with a read-/write-memory (intermediate) and/or read-  
30 only-memory, which makes it possible to store programs and/or data files, particularly identification data of the subscriber owning the card, as well as

calculating and processing means, capable of executing different algorithms, in particular algorithms enabling the execution of subscriber identification and communication encryption.

This architecture of the SIM cards, wherein certain aspects are  
5 standardized within the framework of the GSM-standard, is very "open" since various systems of value-added services (VAS) were considered, which systems are able to fully profit from the functionality of these cards. In particular, numerous services were considered which use the memory available on the SIM card and/or the processing possibilities of the microcontroller on the  
10 card for extending the functionality of the wireless telephone.

New data or new programs, necessary for the execution of these value-added services, may generally be loaded onto the card in one of the following three ways:

1) Through insertion of the card in a suitable read-/write-device for  
15 chipcards. The original data loaded on the card, i.e. prior to its delivery to a client is generally loaded in this fashion. However, owing to the fact that read-/write-devices for chipcards are not widespread, this method cannot be generally used in an easy fashion for updating or completing information registered on the card, after the card has been distributed. Furthermore, the  
20 card must be removed from the mobile station before it can be inserted into another device, which is not very practical, particularly in the case of the very small plug-in cards which cannot be handled very practically.

2) Through direct typing in of data on the keyboard of the mobile station. Owing to the heavily reduced size of keyboards normally used for  
25 mobile telephones and because of the limited number of keys, this approach is only appropriate for the entry of very short data, for instance a password or a yes-/no-type answer during execution of programs by the card's microcontroller, but by no means for the entry of complete programs into the SIM card.



3) The data and/or programs can be loaded remotely into the mobile station, for instance, in the form of short messages containing a header, which enables the mobile station to recognize the short message as such, and are then transferred by the mobile equipment into the card. This transmission can  
5 take place in both directions. The patent document EP689368, filed in the name of the applicant, describes a technique which makes it possible to remotely load data and programs into a mobile station in a transparent fashion. However, this type of transmission can only take place from another station, connected to the mobile radio network, for instance, from another mobile  
10 telephone. Moreover, the transmission can only take place at the cost of receiving a communication generally subject to fees in the mobile radio network.

The patent application PCT/CH96/00464, filed in the name of the applicant, describes a method for ordering products or information by means of  
15 a mobile station. A code unambiguously identifying a product and its supplier must be entered into the mobile station, and is then transmitted to the product supplier, together with identification data of the subscriber, by means of short messages via the mobile radio network. The product code must comprise a large number of alphanumeric characters, in order for the product and the  
20 product supplier to be identified unambiguously. Furthermore, control characters (parity) are necessary to recognize and correct possible errors in the product code. None of the means mentioned above prove to be really appropriate for entering this type of information into the mobile station in a comfortable way.

25 On the other hand, a certain number of new value-added services require that the data or programs stored in a SIM card may be accessed from an external device, for instance from another telephone.

Various patent documents, particularly documents classified in the group H04M-001/00 of the international patent classification system, describe  
30 systems which enable the entry of data, for example dial pulses or dial tones, into a telephone handset. However, these documents, for example DE2427527 or US4130738, generally require adaptations of the telephone handset and,

therefore, cannot be used for exchanging data with a conventional mobile station. Moreover, these documents allow only a one-way communication, generally from an external device to the telephone handset. This is particularly the case for the patent document EP0506544. Finally, these documents generally do not relate to  
5 the transmission of data or programs into the memory zone of a SIM chipcard inserted in a mobile station.

In the patent application WO 96/38814 a telephone card with contacts is described which is additionally provided with a wireless interface for another application, for example for use as a ticket. This card however contains no  
10 subscriber identification and cannot be used as a SIM card.

Described in the patent application GB 2 298 613 A is a SIM card with a first interface, provided with contacts, for connection to a mobile radio telephone, which has in addition a second interface, provided with contacts, for connection to an external device. Before this SIM card according to GB 2 298 613 can be  
15 connected to an external device, however, it has to be removed from the mobile radio telephone.

Described in the patent application GB 2 306 241 A is a receiving device which can receive chipcards in order to transmit data from a first chipcard to a second chipcard, or via a personal computer and a network connection to a  
20 distant station. Also according to GB 2 306 241 A, a chipcard cannot be inserted in a mobile radio telephone and in a receiving device at the same time.

Described in the patent application EP 555 992 A1 is an adapter for mobile radio telephones which can accept a SIM card and has a data interface and converting means in order to receive data, for example from a personal computer,  
25 to convert it into SMS (Short Message Service) format, and transmit it to the mobile radio telephone. The SMS card has to be removed from the mobile radio telephone in order to connect the adapter according to EP 555 992 A1 to the mobile radio telephone.

Described in the patent application DE 43 21 381 A1 is a device adapter,  
30 for example for a mobile radio telephone, which can be temporarily connected to the respective device via a card interface in order to load new versions of

4a

software programs into the device from a personal computer or from a memory contained in the device adapter. A card usually connected to the device, for example a SIM card, must be removed from the device in order to connect the adapter according to DE 43 21 381 A1 to this device.

Consequently, it is an object of this invention to propose a device and a method for communication, which are suitable for two-way transmission of data and programs to or from a SIM chipcard.

It is a further object of this invention to propose a telecommunications system which does not have the shortcomings of the systems of the prior art.

According to the invention, these objects are particularly achieved with the aid a chipcard having the elements of the characterizing portion of patent claim 1, a mobile station having the elements of the characterizing portion of patent claim 7, a data processing device having the elements of the characterizing portion of patent claim 14, and a method having the elements of the characterizing portion of one of the patent claims 20 or 26.

In particular, the objects of the invention are achieved with the aid of a chipcard, for instance a SIM chipcard having at least one wireless interface, which makes it possible for the card's processing means to communicate directly with an external device located outside the mobile communications device, neither the electrical contacts of the chipcard nor the mobile station being passed.

In a preferred embodiment of the invention, the wireless interface has at least one coil and, consequently, the direct communication between the SIM chipcard and an external device takes place through electromagnetic waves.

25

In this fashion, data can be directly written into the chipcard or read from the card by an external device, for example another wireless telephone or any data processing device whatsoever.

An advantage of the invention is that it can be applied without the  
5 necessity of any imperative changes of the mobile communication equipment.  
Thus, a chipcard having a wireless interface according to the invention can be distributed by a network administrator to those subscribers who have subscribed to a value-added service suitable for benefiting from the possibilities of these cards, and the card can be directly used by these  
10 subscribers by simply inserting it in a conventional mobile station.  
Consequently, it is not necessary to replace or change the existing equipment, except for the chipcards, which can be produced at very low cost.

The present invention also relates to various methods and services which can be applied thanks to the card according to the present invention.

15 The present invention will be better understood with the aid of the description, given by way of example and illustrated by the appended figures:

Figure 1 shows a schematic and perspectival view of a mobile station, in which a chipcard according to the invention is inserted, and of an external device according to the invention.

20 Figure 2 shows a schematic view of a chipcard according to the invention.

Although the description, given by way of example, relates particularly to the special case of a chipcard of the SIM-type (Subscriber Identity Module) used in combination with a portable telephone of the GSM-  
25 type, it is important to understand that the card may just as well be used in combination with any other type of mobile station, for instance with the GSM, PCN, NMT, TACS, PDC, DCS1800, or with any other standard of mobile communications, as well as with any type of chipcard used in a mobile communications network for storing subscriber identity information.

Figure 2 illustrates in schematic fashion an embodiment of a SIM chipcard according to the invention. The chipcard 2, in this example a card of the credit card format (full-size), has a conventional microcontroller 20 which is embedded in the plastic carrier 25 of the card and which is responsible for the SIM functionality of the card. The microcontroller 20 has a read-/write- and/or a read-only-memory zone 200 as well as a data processing zone 201, which are combined in a single integrated circuit. The microcontroller 20 is responsible for the application of the card's SIM functionality, as described, for instance, in the article "SIM Cards" by T. Grigorova and I. Leung, which was published in *Telecommunication Journal of Australia*, vol. 43, No. 2, 1993, pages 33 to 38, as well as for new functionality loaded onto the card at a later point in time. The chipcard also has contact means, for instance an area 24 with eight metallic contacts on the surface of the card, by means of which the card communicates with the mobile station 1, into which the card is inserted. The electrical energy supply of the card, or at least of the microcontroller 20, takes place through the communication station 1 with the aid of the contacts 24.

According to the invention, the chipcard 2 has a second integrated circuit 21 responsible for the direct communication with an external device. The second integrated circuit is connected with the microcontroller 20 via an interface 22. Moreover, the chipcard 2 has a coil 23 which is connected to the second integrated circuit 21 and embedded in the plastic carrier 25 of the chipcard. The coil 23 may be manufactured, for example, by coiling up a wire or by means of any other appropriate technique. Nowadays, integration of a coil into a chipcard is well mastered and is described, for instance, in the patent applications WO91/16718 and WO95/33246 (both in the name of Gustafson). In the case of a chipcard of the full-size format, the coil is preferably laminated in between two layers of plastic carriers 25 forming the card. In the case of a plug-in-SIM card, the coil can either be embedded into the plastic carrier, or be attached to the outside of this carrier by means of an adhesive, or by any other appropriate means.

Thanks to this interface 21, 23, the chipcard 2 inserted into a mobile station 1 may communicate directly with an external device 3, represented in a symbolic fashion and also provided with a coil or an antenna 30, via

electromagnetic waves, preferably via radio waves at a frequency close to approximately 120 kHz. The maximum communication distance depends on the characteristic of the coils 23, 30, as well as on the transmitting power, which is chosen such that too much strain on the energy supply of the station 1 and the card 2 can be avoided. For instance, a range of multiple meters can be achieved by means of conventional techniques without big problems. It is important to be careful that the receiving area 10 for the SIM card in the station 1 is not shielded electromagnetically around the coil so that a radio link can be established.

10 In this fashion, data and/or programs can be exchanged between the external device 3 and the chipcard 2 in both directions. Thereby, it becomes possible to remotely load data or programs into the memory 200 of the chipcard, to use or access this memory from an external device, or to establish any dialogue or monologue between the processing means 20, 21 on the card and any external device 3 suitable for this purpose in an easy way. The communication between the chipcard 2 and the external device 3 takes place without using the mobile radio network (GSM), to which the station 1 belongs.

In this example, the chipcard is provided with a conventional microcontroller 20, having storage means 200 and processing means 201, as well as with a communication module 21, which are implemented in the form of two separate integrated circuits. This arrangement makes it possible to use standard microcontrollers 20, which are available at low cost, and to add to them a specific communication module. However, one skilled in the art will realize that it is also possible to integrate the communication module 21 into the same integrated circuit as the microcontroller 20 or, for example, to implement a part of the read-/write and/or read-only-memory of the microcontroller 20 in the form of a separate integrated circuit.

In the same way as the microcontroller 20, the communication module 21 can be fed by the station 1 via contacts 24. In a preferred embodiment, the communication module is energetically independent of the microcontroller 20 and of the communication station 1, and it is supplied with energy through the external device 3 with the aid of the coil 23. In this case, a

storage capacitor, for the energy obtained via the coil 23, is preferably contained in the chipcard. A back-up battery (accumulator), fed by the station or via the coil 23, can also be present on the card. It is also possible to arrange two coils on the card 2, one for the actual communication with the external device 3 and the other for the energy supply of the module 21.

Depending on the application, the external device 3 may be any apparatus provided with an interface 30 that makes it possible to directly communicate with the card 2 via radio waves without using the mobile GSM radio network. In the simplest case, the external device 3 can consist of a further chipcard according to the invention, inserted into another mobile station 1. The invention thus makes it possible to exchange any type of data or programs which are stored in the SIM cards of the two apparatuses. Depending on the type of SIM card and depending on the administration programs of these two cards, it is possible, for instance, to transfer or copy programs and/or data from one card to the other, which programs and/or data extend the functionality of the card or provide access to new services. If the card contains a monetary amount from which communication fees are deducted, it is also possible to transfer the complete or partial remainder of the amount from one card to the other by means of an appropriate communication program and, thereby, load a chipcard with the amounts available on another card.

In an application variant of the invention, the external device 3 is a computer or a terminal provided with an appropriate radio interface 30. In this case, the device 3 is preferably provided with data entry means, not illustrated, for instance with a keyboard and with data display means, not illustrated, for instance with a display (screen). Furthermore, the device 3 is preferably connected to a communications network 31, for instance with an Intranet or with the Internet via a modem, not illustrated, or with any type of fixed or mobile communications network. Data or programs entered into device 3 can then be easily copied into the chipcard 2 via the radio interface 30, 23. In the opposite direction, the data stored in the chipcard can be transmitted to the display of the device 3, and can be displayed there.

An interactive dialogue, consisting of a sequence of communications in both directions, is also possible between the card 2 and a computer 3. A possible application of such a dialogue relates to the selection of an option from a menu, shown in the display of an external device 3, with the aid of a mobile telephone. In this case, the display of the device 3 shows a menu, for example a list of products or information proposed for sale. The user of a mobile station 1 according to the invention can control the position of a cursor in this menu by operating the cursor movement keys 13 on the keyboard of his mobile telephone. The cursor movement instructions are transmitted from the keyboard to the chipcard 2, and are sent from this card to the device 3 with the aid of the coil 3. To validate the selected menu option, for instance to order a product, the user uses a confirmation key on his keyboard, for instance the # key. The confirmation command is transmitted to the device 3 in the same fashion, which then executes a routine corresponding to the selected option. The executed routine can comprise, for example, the establishment of communication with the supplier in the fixed or mobile communications network 31, with which the device 3 is connected, for example via a modem, as well as the transmission of the order to this supplier. In a variant, the routine executed with the confirmation of the menu option includes the emission of a response via the interface 30 to the chipcard 2 an identification code of the selected product. At least a portion of the data received in this response, for instance the identification code of the ordered product, is then stored in the zone of the intermediate memory 200 of the chipcard 2. The application program loaded into the chipcard can then, for example, send a message to the product supplier, for instance a short message (SMS short message) containing this product identification code. Various other possibilities of product orders are described, inter alia, in the patent application PCT/CH96/00464.

Naturally, the chipcard 2 according to the invention not only can be used to control the position of an object, but also to control multiple characteristics of one or multiple objects, for instance position, color, shape, function, visibility, etc.

In the case where the menu in the display of the device 3 corresponds to an Intranet or Internet home page, for instance displayed by an



appropriate browser, the communication between the chipcard and the device 3 preferably contains instructions in the JAVA language (registered trademark by SUN MICROSYSTEMS) which can be directly interpreted by the said browser. Conversely, it is also desirable that the processing means 20, 21 on the card  
5 can also execute instructions in the Java language so that a directed communication is made possible based on instructions of this programming standard well known everywhere. Other preferably object-oriented languages, such as, for example, Corba or C++, could also be used.

The external device 3 could, for example, also be a monetary device,  
10 for instance a coin money machine, or an electronic cash ("e-cash") machine, or a cash register in a store. For the case where the external device 3 is a coin machine, the direct communication with the aid of the coils 23, 30 can make it possible, for example, to reload from the machine the monetary amount stored on the chipcard 2. The advantage consists in that the SIM card can be  
15 reloaded without having to be removed from the telephone handset 1 and without establishing a radio communication subject to a fee. A financial transaction may also take place in the opposite direction by debiting the monetary amount stored in the chipcard 2 with a given amount and by directly transmitting this given amount to the external device 3, for instance, a machine  
20 or a cash register in a department store, with the aid of the wireless interface according to the invention. A transaction of purchase payments in a store equipped with cash registers 3, provided with interfaces 30 for communicating with chipcards according to the invention, can thus comprise the following steps:

- 25 • Direct transmission of the amount to be paid by the cash register 3 to the chipcard 2.
- Temporary storage of this amount in the memory 200 of the SIM chipcard.
- Execution of a routine by the microcontroller 20, so that the  
30 amount to be paid is shown on the display 12 of the mobile station 1.

- In case of consent to the displayed figure, confirmation of this amount by the customer, for instance by pressing the # key.
- Direct transmission of this confirmation command to the device 3 with the aid of the interface 23-30.

5           For example, the monetary amount stored on the chipcard 2 can be charged instantaneously with the amount to be paid. If the monetary amount on the card 2 suffices to settle the transaction, the transaction amount can be debited to the card, and can be transferred to the device 3 via the interface 23, 30 according to any type of protocol and according to the same rules of  
10 security and confidentiality as have been proven, for example, for transactions of electronic cash.

          In a variant, the transaction amount can be transferred onto a bank account of the owner of the device 3 by any bank or financial institution of which the subscriber is a client. For that purpose, in the case where the amount  
15 shown on the display 12 is confirmed, the program loaded on the chipcard 2 can contain an instruction for emission of a SMS short message, containing a debit command, by the mobile station 1 or by the device 3 to a banking establishment.

          The external device 3 can also be an access control device, for  
20 instance a device of the electronic doorkeeper type which makes it possible to control entries and exits in protected locations, for example in a factory or within the fenced-in area of an amusement park. For this application, the chipcard 2 can be loaded with an electronic key stored in the memory 200. To gain access to a protected zone of the locality, it is thus necessary that a direct  
25 communication of the described type is established between the chipcard 2 and the device 3 with the aid of the coil 23, 30. Access to the restricted area is granted only if, based on this communication, it turns out that the electronic key stored in the card 2 is correct and that its owner has the right to penetrate the protected zone. The access method can include the emission: of a message by  
30 either the communication station 1 on the mobile radio network or by the access control device 3 on its own communications network 31, a message of

the SMS type, for instance intended for a central computer, not illustrated, which administers and registers the changes of place within the locality. Administration of the place changes can result, for instance, in billing or debiting the account of the subscriber with an amount depending on the entries  
5 that have taken place. In this application, it is advantageous that the electronic module is supplied electrically thanks exclusively to the coil 23, so that access is even possible when the batteries of the mobile station 1 are run down.

One skilled in the art will understand that these applications are merely given by way of non-restrictive examples. Expressed in more general  
10 terms, the invention relates to all types of methods which include a step of direct communication with a SIM chipcard and, if need be, a step of conventional communication via a conventional radio network.

In a variant embodiment of the invention, the communication of data stored on the chipcard 2 between *<sic. to>* an external device 3 takes place  
15 with the aid of an interface that is disposed in the mobile equipment 1 rather than directly on the chipcard 2. The communication can take place, for example, with the aid of an antenna, a coil or an infrared transceiver, integrated on the housing of the wireless telephone 1. However, this embodiment requires alterations of the apparatus 1 and, consequently, cannot be applied in an easy  
20 fashion by subscribers who are equipped with conventional communication stations 1 without this wireless interface.

### Claims

1. SIM chipcard (2) comprising:

data processing means (20) responsible for the card's SIM-  
functionality and containing storage means (200) which make it possible to  
5 store data, the said data containing at least identification data of a subscriber  
of a mobile telecommunications network;

electrical contacts (24) on the surface of the SIM chipcard, which  
make it possible to exchange data between the said processing means (20)  
and a mobile station (1), in which the SIM chipcard (2) may be inserted in a  
10 removable fashion;

at least one further interface which enables the data transmission  
between the said data processing means (20) and an external device (3);

characterized in that the said further interface is a wireless interface  
(21, 23), which makes it possible to transmit data between the said processing  
15 means (20) and an external device (3) located outside the mobile station (1)  
directly and without passing electrical contacts when the SIM chipcard is  
inserted in the mobile station (1), this contactless data transmission being  
controlled by the mobile station (1) via the said electrical contacts (24).

2. SIM chipcard according to the preceding claim, characterized in  
20 that the said wireless interface contains at least one coil (23), which enables  
the establishment of communication between the said processing means (20)  
and the said external device (3) via electromagnetic waves.

3. SIM chipcard according to the preceding claim, characterized in

that the said processing means comprise a microcontroller (20) responsible for the said SIM-functionality of the card, at least an electronic module (21) connected to the said coil (23) and responsible for the direct communication with the said external device (3), and an interface (22) between the said  
5 microcontroller and the said electronic module.

4. SIM chipcard according to the preceding claim, characterized in that the electrical power supply of the said electronic module and of the said coil is provided by the said mobile station (1) via the said electrical contacts (24).

10 5. SIM chipcard according to claim 3, characterized in that the electrical power supply of the said electronic module (21) and of the said coil (23) is provided by the said external device by interposing the said coil, so that radio communication between the SIM chipcard (2) and the external device (3) is possible even if the batteries of the mobile station (1) are run down.

15 6. SIM chipcard according to one of the preceding claims, characterized in that the processing means (20, 21) are capable of executing instructions in the Java language.

20 7. Mobile station (1) comprising means for communicating in a mobile telecommunications network and a receiving point (10) for inserting a removable SIM chipcard (2), which is intended for storing data containing at least the identification data of a subscriber of the said mobile telecommunications network,

25 characterized by at least one wireless interface (21, 23) enabling a data transmission between the said SIM chipcard (20), inserted in the mobile station, and an external device (3), located outside the mobile station (1), without using the said mobile telecommunications network, whereby this data transmission can be controlled by the mobile station (1).

8. Mobile station according to the preceding claim, characterized in

that the said wireless interface contains at least one coil (23), which makes it possible for the said SIM chipcard (2) to communicate with the said external device (3) via electromagnetic waves.

9. Mobile station according to the preceding claim, characterized in  
5 that the said coil (23) is integrated in the said SIM chipcard (2).

10. Mobile station according to claim 8, characterized in that it further comprises electrical batteries, and in that the said wireless interface (21, 23) can be supplied with energy by the said external device (3) by interposing the said coil (23) so that radio communication between the SIM chipcard (2)  
10 and the external device (3) is possible even if the said electrical batteries are run down.

11. Mobile station according to one of the claims 8 to 10, characterized in that the said receiving point (10) is not shielded electromagnetically to the outside.

15 12. Mobile station according to claim 7, characterized in that the said wireless interface contains at least one infrared transmitter-receiver on the housing of the said station.

13. Mobile station according to one of the claims 7 to 12, characterized in that it further comprises a confirmation key (11) and control  
20 means (13) for a cursor.

14. Mobile station according to one of the claims 7 to 13, characterized in that the said data transmission can be controlled with the keyboard of the mobile station (1).

15. Data processing device (3), characterized in that it contains a  
25 wireless interface (30), which makes it possible to communicate directly with a SIM chipcard (2) according to one of the claims 1 to 6, which SIM chipcard is inserted into a mobile station (1) according to one of the claims 7 to 14, without

using the said mobile radio network.

16. Data processing device according to the preceding claim,  
characterized in that the said interface contains at least a transmitter-receiver  
(30) which enables the establishment of communication with a SIM chipcard (2)  
5 according to one of the claims 2 to 6 via electromagnetic waves.

17. Data processing device according to one of the claims 14 or 15,  
characterized in that it contains the following: means for displaying a multiple-  
choice menu, and means for changing the position of a cursor in the said  
menu, respectively for executing a method corresponding to the choice made in  
10 the said menu, as the reaction to the cursor movement, respectively  
confirmation instructions which have been received at the said wireless  
interface.

18. Data processing device according to the preceding claim,  
characterized in that it contains an interface (31) of the Internet-/Intranet-type.

15 19. Data processing device according to one of the claims 15 to 18,  
characterized in that it is integrated in a monetary device.

20. Data processing device according to one of the claims 15 to 18,  
characterized in that it is integrated in an access control device.

20 21. Method for communication between an external device (3) and a  
mobile station (1) comprising means for communication in a mobile radio  
network and a receiving point (10) for inserting a removable SIM chipcard (2),  
intended for storing data containing at least identification data of a subscriber  
of the said mobile radio network,

25 characterized in that it comprises at least a step of direct  
communication between the said SIM chipcard (2) inserted into the mobile  
station and the said external device (3), without use of the said mobile radio

network; and

in that this direct communication may be controlled by the mobile station (1).

22. Method according to the preceding claim, characterized in that  
5 the said communication is bi-directional.

23. Method according to the preceding claim, characterized in that the said communication is communication via electromagnetic waves, which requires at least one coil (23), which is integrated in the said SIM chipcard.

24. Method according to one of the claims 21 to 23, characterized in  
10 that it comprises the following: at least a step of displaying a menu with multiple choice on a display of the said data processing device;

at least a step of selecting one of the options available for selection in the menu by the user of the said mobile station;

at least a step of communicating selection instructions, which are  
15 sent directly to the said external device by the said mobile station, without using the said mobile radio network;

at least a step of executing a method, corresponding to the choice made in the said menu, by the said external device.

25. Method according to one of the claims 21 to 24, characterized in  
20 that the said communication comprises the emission of at least one instruction in an object-oriented language, e.g. Java, by the said external device, whereby this instruction is intended to be executed by processing means (20, 21) in the SIM chipcard (2).

26. Method according to one of the claims 21 to 25 <sic. 24>,  
25 characterized in that the said communication comprises the emission of at least



one instruction in an object-oriented language, for example in the Java language, by the said SIM chipcard (2), whereby this instruction is intended to be executed by processing means in the said external device (3).

27. Method according to one of the claims 21 to 26, characterized in  
5 that the said communication <comprises> transmitting data between the said external device (3) and the said SIM chipcard (2), at least certain of which data are stored in the said SIM chipcard (2).

28. Method according to the preceding claim, characterized in that  
10 the said SIM chipcard stores a monetary amount usable with the said card, and in that the said data comprises indication of a reload-value for the said monetary amount.

29. Method according to the preceding claim, characterized in that it  
further comprises a subsequent step of emitting a short message, containing  
the said data, by the said mobile station.

15

20

1/1

FIG. 1

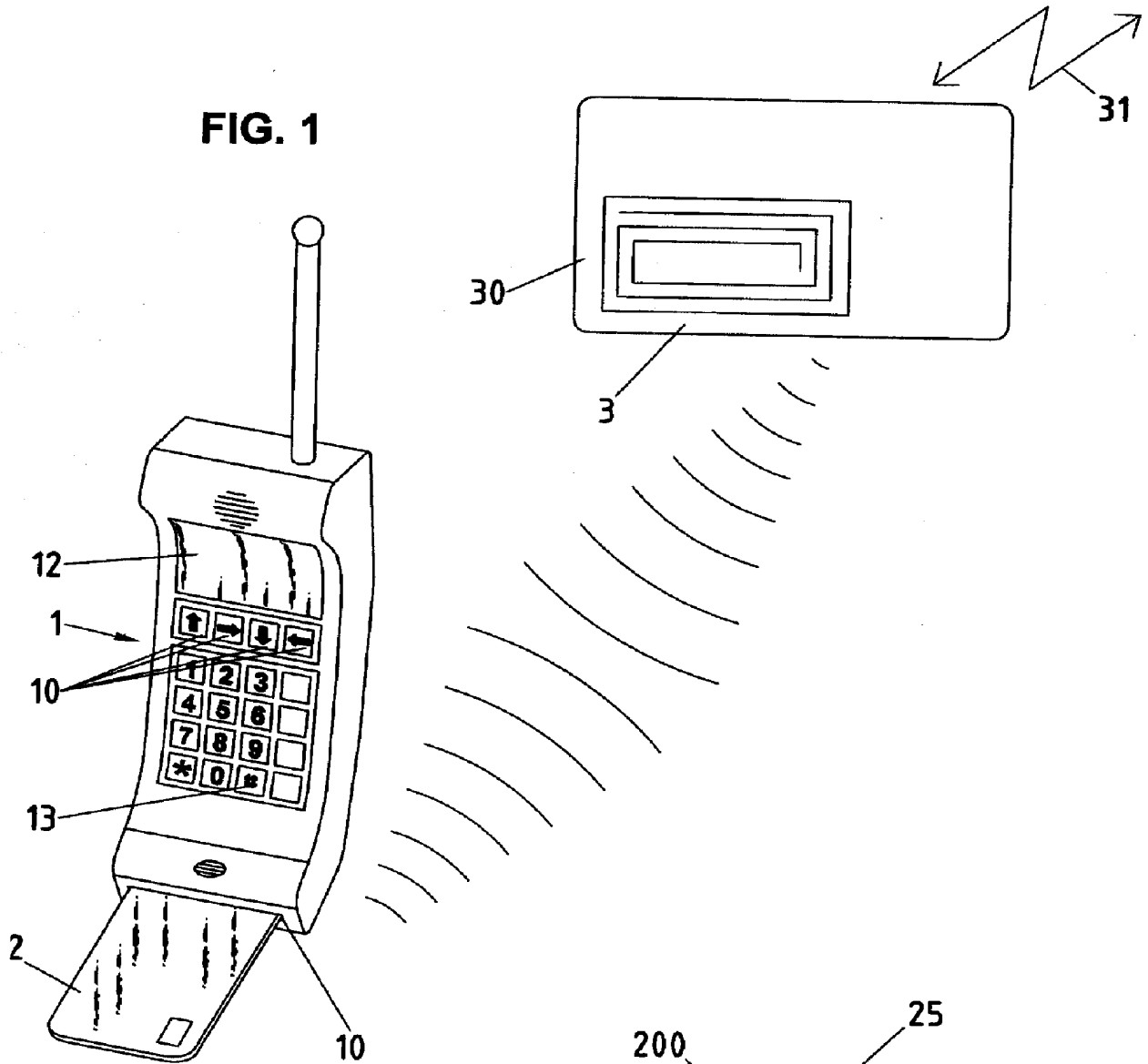
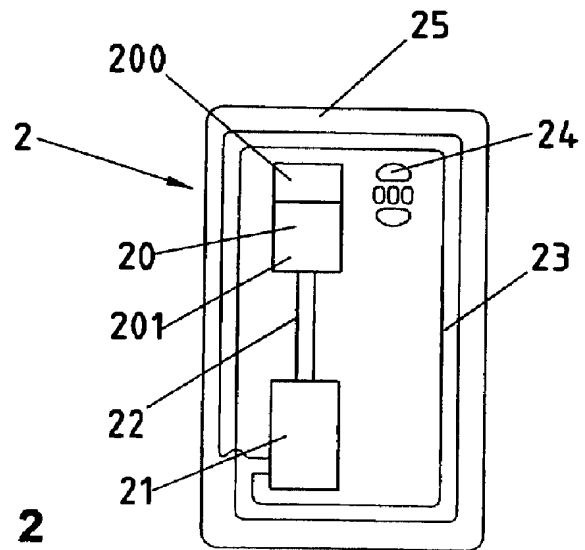


FIG. 2



STATEMENT OF RELEVANCY - EP 0159539

The English language claims begin in col. 7.

⑩



Europäisches Patentamt  
European Patent Office  
Office européen des brevets

⑪ Veröffentlichungsnummer:

**0 159 539**  
**B1**

⑫

## EUROPÄISCHE PATENTSCHRIFT

⑬ Veröffentlichungstag der Patentschrift: **12.09.90**

⑭ Int. Cl.<sup>5</sup>: **G 07 F 7/08, G 07 C 9/00**

⑮ Anmeldenummer: **85103258.1**

⑯ Anmeldetag: **20.03.85**

⑰ **Chipkartensystem.**

⑱ **Priorität: 04.04.84 DE 3412663**

⑲ **Patentinhaber: Siemens Aktiengesellschaft  
Wittelsbacherplatz 2  
D-8000 München 2 (DE)**

⑳ **Veröffentlichungstag der Anmeldung:  
30.10.85 Patentblatt 85/44**

㉑ **Erfinder: Albers, Hans-Erhard, Dipl.-Ing. (FH)  
Eichenring 39  
D-8551 Röttenbach (DE)  
Erfinder: Linneweh, Eckard, Ing. grad.  
Otto-Hahn-Strasse, 16,  
D-8056 Neufahrn, (DE)  
Erfinder: Müller, Dieter, Ing. grad.  
Mayrhofer Ring 32  
D-8031 Seefeld 2 (DE)**

㉒ **Bekanntmachung des Hinweises auf die  
Patenterteilung:  
12.09.90 Patentblatt 90/37**

㉓ **Benannte Vertragsstaaten:  
AT CH DE FR GB IT LI**

㉔ **Entgegenhaltungen:  
EP-A-0 032 193  
EP-A-0 058 029  
EP-A-0 061 373  
WO-A-82/03286  
WO-A-83/03694  
GB-A-2 020 869  
GB-A-2 028 555  
US-A-3 806 874  
US-A-4 001 550  
US-A-4 277 837**

**EP 0 159 539 B1**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99(1) Europäisches Patentübereinkommen).

Courier Press, Leamington Spa, England.

## Beschreibung

Die vorliegende Erfindung bezieht sich auf ein Chipkartensystem mit Chipkarten zur Verwendung als Geldersatz, als Ausweis bzw. als Speichermedium, bei dem eine einzige Chipkarte nacheinander für unterschiedliche Anwendungsfälle benutzbar ist, bei dem für die unterschiedlichen Anwendungsfälle unterschiedliche Bereiche eines in den Chip integrierten Speichers oder einer Funktionseinheit, vorgesehen sind, wobei für die Auswahl der unterschiedlichen Bereiche in Chip eine Auswahlerschaltung in dem Chip vorgesehen ist, für die eine bestimmte Auswahlprozedur festgelegt ist, durch welche sichergestellt werden kann, daß die für den betreffenden Anwendungsfall relevanten Bereiche und nur diese zugeordnet werden, daß für spezielle Anwendungsfälle als Funktionseinheit ein Prozessor vorgesehen ist, durch den die in den unterschiedlichen speziellen Anwendungsfällen erforderlichen Prozesse abgewickelt werden, wobei diese multifunktionale Chipkarte dazu geeignet ist, zusammen mit einer Eingabe-/Ausgabe-Einrichtung zu wirken, in der ein das Aktivieren ermöglichendes Kombinationsbedienelement vorgesehen ist und in die die Chipkarte einsteckbar ist und die für einen mobilen Einsatz zusätzlich eine Stromquelle enthält, und wobei die Eingabe-/Ausgabe-Einrichtung mit einer drahtlosen Sende-/Empfangs-Einrichtung zur Kommunikation mit einer ortsfesten Einrichtung verbindbar ist.

Bisher wurde für jeden Anwendungsfall eine eigene Chipkarte an die Benutzer ausgegeben. Die Folge davon war, daß ein Benutzer, der für unterschiedliche Anwendungsfälle entsprechende Chipkarten benutzt, eine Vielzahl derartiger Karten bei sich führen mußte. Abgesehen davon, daß die Vielzahl von Karten lästig ist, besteht die Möglichkeit der Verwechslung der Chipkarten. Bei Chipkarten nach dem Stand der Technik liegen die Kontakte zum Anschluß der Chipkarte an eine Lese-/Schreibeinrichtung offen, wodurch die Gefahr einer Verschmutzung, insbesondere mit öligen Stoffen, wie sie in Küche oder Werkstatt vorkommen, besteht. Die Folge davon ist eine schlechte Kontaktgabe und damit eine fehlerhafte Datenübertragung zwischen der Chipkarte und dem betreffenden Chipkarten-Terminal. Außerdem ist bisher ein Datentransfer nur dann möglich, wenn und solange die Chipkarte in das betreffende Terminal eingesteckt ist. Daraus resultiert beispielsweise, daß ein Datentransfer sogar bei einem reinen Lesevorgang, wie er beispielsweise beim Eingang in ein Betriebsgelände erforderlich ist, relativ lange dauert. Wenn sich beispielsweise bei Ankunft eines Verkehrsmittels vor dem Eingang eine Menschenschlange bildet, kann ein Lesevorgang mit Einstecken und Ausgeben von mehr als etwa einer halben Sekunde nicht mehr unbedingt in Kauf genommen werden. Eine Identifikationskarte nach dem Stand der Technik, mit der kommende Rufe in einer Telefon-Nebenstellenanlage an den Aufent-

haltsort des Karteninhabers nachgeführt werden sollen, muß der Karteninhaber beim Kommen und beim Gehen in das betreffende Terminal einstecken, um sich an- bzw. abzumelden. Abgesehen davon, daß er in einem gegebenenfalls großen Raum das Terminal suchen muß, besteht die Gefahr, daß er das Einstecken vergißt. Hat ein Raum mehrere Türen, so müßten. u.U. entsprechend viele Terminals installiert werden, was sehr aufwendig wäre.

Bei wichtigen Vorgängen, wie z.B. dem Zutritt zu geschützten Räumen, großen Geldgeschäften oder Zugang zu geschützten Daten, ist nicht nur die Berechtigung des Karteninhabers zu prüfen, sondern auch die Identität des Inhabers. Die dazu ausgegebene geheime, im allgemeinen vierstellige Personen-Identifizierungsnummer PIN ist schlecht zu merken (und für sehr wichtige Vorgänge trotzdem zu kurz). Sie wird deshalb von vielen Benutzern in der Nähe der Karte aufgeschrieben und ist somit beim Verlust der Karte leicht von Fremden zu finden. Ist andererseits die PIN von Inhaber frei wählbar, so werden leicht merkbare Ziffernfolgen gewählt (z.B. Geburtsdatum), die von einem Fremden leicht erraten werden können. Ferner muß sichergestellt werden, daß der Karteninhaber beim Eintippen der PIN nicht beobachtet werden kann, wodurch diese Fremden bekannt werden kann.

Bisher ist eine Verwendung einer Chipkarte als Speicher, beispielsweise für Telefonnummern, Notfallinformationen, Werkzeugprogramme, als Speicher für dezentrale Datenerfassung bei Lagerbestandsaufnahmen, Buchungsvorgängen, Terminabsprachen usw., der dezentral abgefragt und verändert werden kann, aber auch zu bestimmten Zeitpunkten mit einem zentralen Speicher verglichen und ggf. korrigiert oder auf den neuesten Stand gebracht werden kann, als Ersatz für Kleingeld, wobei bei Zahlungsvorgängen in Münzfernsprechern oder Automaten Teilbeträge eines vorbezahlten Betrags gebucht werden können, als Nachweis der Kreditwürdigkeit ggf. bis zu einem vorgegebenen Limit, das bei Zahlungsvorgängen auch vermindert werden kann, als Identifikationsmittel, bei dem zusätzlich die Zuordnung der Person zur Karte durch Eingabe der persönlichen Identifikationsnummer PIN über eine Tastatur am Chipkarten-Terminal oder durch "Lesen" des Fingerabdrucks überprüft werden kann usw. bekannt.

Aus der deutschen Patentanmeldung P 33 15 047.8 ist beispielsweise bereits eine integrierte Schaltung mit einem nichtflüchtigen Schreib-Lese-Speicher bekannt, die als ein Chip ausgebildet ist, der für den Einschluß in eine Ausweiskarte, nämlich eine Chipkarte, geeignet ist.

Aus "Betriebswirtschaftliche Blätter", Heft 2, Februar 1982, S. 33—35 (Verfasser: Wolfgang Starke) ist bereits die Verwendungsmöglichkeit der sog. ec-Karte als Multifunktionskarte bekannt.

Aus der US—A—4 277 827 ist ein Chipkartensystem bekannt, bei dem eine einzige Chipkarte unterschiedliche Speicherbereiche aufweist, die

durch eine Auswahl­schaltung entsprechend dem gewählten Anwendungsfall angesteuert werden. die multifunktionale Chipkarte ist dazu geeignet, zusammen mit einer Eingabe-/Ausgabe-Einrichtung zu wirken, in die die Chipkarte einsteckbar ist und die für einen mobilen Einsatz zusätzlich eine Stromquelle enthält. Die Eingabe-/Ausgabe-Einrichtung ist zur drahtlosen Kommunikation mit weiteren, z.B. ortsfesten Anlagen eingerichtet, wobei die den unterschiedlichen speziellen Anwendungsfällen zugeordneten erforderlichen Prozesse durch eine Prozessor abgewickelt werden.

Aus der GB—A—2 020 869 ist der Aufbau einer zur persönlichen Identifizierung dienenden, sowie für verschiedene andere Anwendungen einzusetzenden Datenträgerkarte, auf der ein Mikrocomputer sowie verschiedene Speicher samt Energieversorgung angeordnet sind, bekannt.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein Chipkartensystem zu schaffen, das multifunktional verwendbar ist und das die zuvor genannten Nachteile vermeidet.

Zur Lösung dieser Aufgabe wird ein neuartiges Chipkartensystem mit Chipkarten zur Verwendung als Geldersatz, als Ausweis bzw. als Speichermedium gemäß dem Oberbegriff des Patentanspruchs 1 vorgeschlagen, das erfindungsgemäß durch die in dessen kennzeichnenden Teil angegebenen Merkmale charakterisiert ist.

Vorteilhafte Weiterbildungen der Erfindung sind durch die in den Unteransprüchen angegebenen Merkmale gekennzeichnet.

Im folgenden wird die vorliegende Erfindung anhand mehrerer, Ausführungsbeispiele für die Erfindung betreffender Figuren im einzelnen erläutert.

Fig. 1 zeigt eine schematische Übersicht über das erfindungsgemäße Chipkartensystem mit einer in eine als Aufbewahrungstasche ausgebildeten Eingabe-/Ausgabe-Einrichtung eingesteckten Chipkarte und einer ortsfesten drahtlosen Sende-/Empfangs-Einrichtung.

Fig. 2 zeigt schematisch die Einteilung eines Chips für die erfindungsgemäße Chipkarte in verschiedene Funktionsbereiche.

Wie bereits erläutert, ist gemäß Fig. 1 eine Chipkarte 1 vorgesehen, die zwecks Aufbewahrung und Schutz gegen widrige äußere Einflüsse in eine als Aufbewahrungstasche, vorzugsweise Plastiktasche; ausgebildete Eingabe-/Ausgabe-Einrichtung 2 gesteckt ist. Die gezeigte Eingabe-/Ausgabe-Einrichtung 2 enthält ein Sendeorgan und ein Empfangsorgan sowie zumindest ein Bedienungselement. Die als ortsfestes Terminal dienende drahtlose Sende-/Empfangs-Einrichtung 3 enthält ebenfalls ein Sendeorgan und ein Empfangsorgan und ist zur Kommunikation mit einer ortsfesten Einrichtung verbindbar. Die drahtlose Datenübertragung in Richtung von der Sende-/Empfangs-Einrichtung 3 zu der Eingabe-/Ausgabe-Einrichtung 2 und umgekehrt kann vorzugsweise mittels Infrarotwellen durchgeführt werden. In diesem Fall sind die Sende- und Empfangsorgane jeweils Infrarotsende- bzw.

Empfangsdioden. Die Eingabe-/Ausgabe-Einrichtung 2 enthält außerdem eine für ihre eigene Stromversorgung und die notwendige Stromversorgung für die in sie eingesteckte Chipkarte 1 erforderliche Stromquelle (nicht gezeigt). Der Chip in der Chipkarte 1 weist für die unterschiedlichen Anwendungsfälle unterschiedliche Bereiche eines in dem Chip integrierten Speichers  $1_1, 1_2 \dots 1_n$ , eine für die Auswahl der unterschiedlichen Bereiche notwendige Auswahl­schaltung 121 sowie für spezielle Anwendungsfälle als Funktionseinheit einen Prozessor 12 auf (vgl. Fig. 2). Das ortsfeste Terminal in Form der drahtlosen Sende-/Empfangs-Einrichtung 3 enthält bei Vorhandensein mehrerer mobiler Einrichtungen in dem betreffenden Ortsbereich eine Einrichtung, die in an sich bekannter Weise und ggf. nach einer Prioritätsliste einen Mehrfachzugriff steuern kann.

Das Bedienungselement in der Eingabe-/Ausgabe-Einrichtung 2 kann gemäß einer vorteilhaften Weiterbildung der Erfindung ein Kombinationsbedienungselement sein, mittels dessen das Aktivieren der eingesteckten Chipkarte vorzunehmen ist und das außerdem einen Fingerabdrucksensor darstellt. Für spezielle Anwendungsfälle bleibt die Eingabe-/Ausgabe-Einrichtung 2 in ihrem empfangsbereiten Zustand und sendet auf den Empfang eines Signals von dem ortsfesten Terminal hin, mit dem dieses eine Anwendungs­information überträgt, automatisch die benötigte Nachricht.

Der in der Chipkarte 1 enthaltene Speicher ist vorzugsweise als Halbleiterspeicher ausgebildet, der nichtflüchtig speichert und elektrisch programmierbar ist. Vorzugsweise wird für den Chip innerhalb der Chipkarte die EPROM-Technologie verwendet.

Die mit dem erfindungsgemäßen Chipkartensystem durchzuführenden Prozesse betreffen folgende Funktionen:

- Verschlüsselung bzw. Entschlüsselung der zu sendenden bzw. zu empfangenden Daten
- Authentizitätsprüfung
- Datensicherung gegen Übertragungsfehler und
- Verarbeitung einer Fingerabdruckinformation.

Zum Auswählen bestimmter Funktionsbereiche in dem Chip wird ein sog. Dialogverfahren durchgeführt. Zum Auswählen und Einschalten aller relevanten und nur dieser Bereiche innerhalb des Chips, die für einen bestimmten Anwendungsfall erforderlich sind, wird ein spezielles Verfahren durchgeführt, das innerhalb der Chipkarte durch den dafür vorgesehenen Prozessor 12 gesteuert wird. Im Zustand des Eingestecktseins der Chipkarte 1 in die Plastikeinstecktasche wird erfindungsgemäß eine spezielle Prozedur zum Aktivieren, nämlich zum Einschalten der Stromquelle für die Chipkarte 1 und die Sende-/Empfangs-Einrichtung 2 durchgeführt.

Die Datenübertragung kann gemäß einer andern Weiterbildung der Erfindung auch über Mikrowellen abgewickelt werden.

Zusammenfassend ist festzustellen, daß durch

das neuartige Chipkartensystem folgende Vorteile gegeben sind:

—Ein Datenaustausch ist wegen des verwendeten breitbandigen Kanals schnell abzuwickeln,

—das Einstecken der Karte in ein Terminal, wie es herkömmlicherweise zu erfolgen hat, entfällt,

—die Personenidentifizierungsnummer PIN kann an einem geeigneten Ort eingegeben werden, an dem eine Beobachtung durch Unbefugte nicht möglich ist.

Zum Schutz der zu übertragenden Daten gegen ein "Abhören" während einer Infrarot- oder Mikrowellenübertragung können die an sich bekannten Verfahren der Nachrichtenverschlüsselung verwendet werden. Soll außerdem auch vermieden werden, daß das System von Unbefugten benutzt wird, kann außerdem eine Authentizitätsprüfung vorgenommen werden.

#### Patentansprüche

1. Chipkartensystem mit Chipkarten zur Verwendung als Geldersatz, als Ausweis bzw. als Speichermedium, bei dem eine einzige Chipkarte (1) nacheinander für unterschiedliche Anwendungsfälle benutzbar ist, bei dem für die unterschiedlichen Anwendungsfälle unterschiedliche Bereiche eines in den Chip integrierten Speichers ( $1_1, 1_2 \dots 1_n$ ) oder einer Funktionseinheit vorgesehen sind, wobei für die Auswahl der unterschiedlichen Bereiche im Chip eine AuswahlSchaltung (121) in dem Chip vorgesehen ist, für die eine bestimmte Auswahlprozedur festgelegt ist, durch welche sichergestellt werden kann, daß die für den betreffenden Anwendungsfall relevanten Bereiche und nur diese zugeordnet werden, daß für spezielle Anwendungsfälle als Funktionseinheit ein Prozessor (12) vorgesehen ist, durch den die in den unterschiedlichen speziellen Anwendungsfällen erforderlichen Prozesse abgewickelt werden, wobei diese multifunktionale Chipkarte (1) dazu geeignet ist, zusammen mit einer Eingabe-/Ausgabe-Einrichtung (2) zu wirken, in der ein das Aktivieren ermöglichendes Kombinationsbedienungsselement vorgesehen ist und in die die Chipkarte (1) einsteckbar ist und die für einen mobilen Einsatz zusätzlich eine Stromquelle enthält, und wobei die Eingabe-/Ausgabe-Einrichtung (2) mit einer drahtlosen Sende-/Empfangs-Einrichtung (3) zur Kommunikation mit einer ortsfesten Einrichtung verbindbar ist, dadurch gekennzeichnet, daß der Prozessor (12) in an sich bekannter Weise in den Chip eingebaut ist, daß diese ortsfeste Einrichtung ihrerseits eine Einrichtung enthält, die bei Vorhandensein mehrerer mobiler Einrichtungen in dem betreffenden Ortsbereich in an sich bekannter Weise und ggf. nach einer Prioritätsliste einen Mehrfachzugriff steuert, und daß für spezielle Anwendungen die Eingabe-/Ausgabe-Einrichtung (2) im empfangsbereiten Zustand bleibt und auf den Empfang eines Signals von der ortsfesten Station hin, mit der diese eine Anwendungsinformation überträgt, automatisch die benötigte Nachricht sendet.

2. Chipkartensystem nach Anspruch 1, dadurch

gekennzeichnet, daß die Eingabe-/Ausgabe-Einrichtung (2) als Plastiktasche ausgebildet ist, in der die Chipkarte (1) ständig getragen wird, wodurch eine Verschmutzung der empfindlichen äußeren Kontaktstellen der Chipkarte (1) vermeidbar ist, und daß das Kombinationsbedienungsselement in der Eingabe-/Ausgabe-Einrichtung (2) vorgesehen ist, mittels dessen das Aktivieren vorzunehmen ist und das außerdem einen Fingerabdrucksensor darstellt.

3. Sende- und Empfangseinrichtung für das Chipkartensystem nach Anspruch 1, dadurch gekennzeichnet, daß die Kommunikation über Infrarotwellen abgewickelt wird.

4. Sende-/Empfangseinrichtung für das Chipkartensystem nach Anspruch 1, dadurch gekennzeichnet, daß die Kommunikation über Mikrowellen abgewickelt wird.

5. Chipkartensystem nach Anspruch 1, dadurch gekennzeichnet, daß der Speicher ein Halbleiterspeicher ist.

6. Chipkartensystem nach Anspruch 5, dadurch gekennzeichnet, daß der Halbleiterspeicher nichtflüchtig speichert und elektrisch programmierbar ist.

7. Chipkartensystem nach Anspruch 1 und 6, dadurch gekennzeichnet, daß für den Chip die E<sup>2</sup>PROM-Technik vorgesehen ist.

8. Chipkartensysteme nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Prozesse folgende Funktionen betreffen:

—Verschlüsselung bzw. Entschlüsselung der zu sendenden bzw. zu empfangenden Daten

—Authentizitätsprüfung

—Datensicherung gegen Übertragungsfehler

—Verarbeitung der Fingerabdruckinformation.

#### Revendications

1. Système à cartes à puces, comportant des cartes à puces destinées à être utilisées à la place d'argent, en tant que cartes d'identité ou en tant que support de mémoire, et dans lequel une seule carte à puce (1) peut être utilisée successivement pour différents cas d'utilisation, et dans lequel, pour les cas d'utilisation différents, il est prévu des zones différentes d'une mémoire ( $1_1, 1_2 \dots 1_n$ ), intégrée dans une puce, ou une unité fonctionnelle, et dans lequel pour la sélection des différentes zones de la puce, il est prévu, dans cette dernière, un circuit d'évaluation (121), pour lequel est fixée une procédure déterminée de sélection, grâce à laquelle on peut être certain que les zones afférentes au cas d'utilisation considéré et seulement ces zones sont associées, et dans lequel, pour des cas d'application particuliers, il est prévu, en tant qu'unité fonctionnelle, un processeur (12), au moyen duquel les processus nécessaires pour les différents cas d'utilisation particuliers sont exécutés, et dans lequel cette carte à puce multifonctionnelle (1) est appropriée pour coopérer avec un dispositif d'entrée/sortie (2), dans lequel un élément de commande de combinaison permettant l'activation est prévu et dans lequel la carte à puce (1) peut être enfilée

et qui contient en outre une source de courant, pour une utilisation mobile, et dans lequel le dispositif d'entrée/sortie (2) peut être relié à un dispositif d'émission/réception (3) sans fil pour communiquer avec un dispositif fixe, caractérisé par le fait que le processeur (12) est monté de façon connue en soi dans la puce, que ce dispositif fixe contient pour sa part un dispositif qui, lors de la présence de plusieurs dispositifs mobiles dans l'environnement considéré, commande d'une manière connue en soi et éventuellement selon une liste de priorités, un accès multiple et que pour des applications particulières, le dispositif d'entrée/sortie (2) reste pour l'état à la réception et émet automatiquement l'information nécessaire, lors de la réception, à partir du poste fixe, d'un signal, avec lequel l'information d'utilisation est transmise.

2. Système à cartes à puces suivant la revendication 1, caractérisé par le fait que le dispositif d'entrée/sortie (2) est réalisé sous la forme d'une poche plastique, dans laquelle la carte à puce (1) est disposée à demeure, ce qui permet d'éviter un salissement des plaques extérieures sensibles de contact de la carte à puce (1), et que dans le dispositif d'entrée/sortie (2) est disposé l'élément de commande de combinaison, à l'aide duquel l'activation doit être réalisée et qui représente en outre un capteur d'empreintes digitales.

3. Dispositif d'émission/réception pour le système à cartes à puces suivant la revendication 1, caractérisé par le fait que la communication est exécutée au moyen d'ondes de rayonnement infrarouge.

4. Dispositif d'émission/réception pour le système à cartes à puces suivant la revendication 1, caractérisé par le fait que la communication est réalisée à l'aide de microondes.

5. Système à cartes à puces suivant la revendication 1, caractérisé par le fait que la mémoire est une mémoire à semi-conducteurs.

6. Système à cartes à puces selon la revendication 5, caractérisé par le fait que la mémoire à semi-conducteurs utilise une mémorisation non volatile et est programmable électriquement.

7. Système à cartes à puces suivant les revendications 1 et 6, caractérisé par le fait que pour la puce, on utilise la technique E<sup>2</sup>PROM.

8. Système à cartes à puces suivant les revendications précédentes, caractérisés par le fait que les processus concernent les fonctions suivantes:

- codage et décodage des données devant être émises ou reçues,
- contrôle d'authenticité,
- sécurité des données vis-à-vis de défauts de transmission,
- traitement de l'information d'empreintes digitales.

#### Claims

1. Chip card system with chip cards for use as a money substitute, as an identity card or as a storage medium, with which a single chip card (1) can be used successfully for different application

cases, with which different areas of money (1, 1<sub>2</sub> . . . 1<sub>n</sub>), integrated into the chip, or of a function unit are provided for the different application cases, a selection circuit (121) being provided in the chip for the selection of the different areas in the chip, for which circuit a certain selection procedure is fixed, by which it can be ensured that the areas relevant for the application case concerned and only these are assigned, that a processor (12), by which the processes necessary for the different specific application cases are executed, is provided for specific application cases as a function unit, this multifunctional chip card (1) being suitable to act together with an input/output device (2), in which a combination control element permitting activation is provided and into which the chip card (1) can be inserted and which additionally contains a power source for mobile use, and the input/output device (2) being connectable to a wireless transmitting/receiving device (3) for communication with a stationary device, characterized in that the processor (2) is fitted in the chip in a way known per se, in that this stationary device for its part contains a device which, if a plurality of mobile devices are present in the local area concerned, controls a multiple access in a way known per se and, if appropriate, according to a priority list, and in that the input/output device (2) remains in the ready-to-receive state for specific applications and, in response to the reception of a signal from the stationary station, with which the latter transmits an item of application information, automatically sends the required message.

2. Chip card system according to Claim 1, characterized in that the input/output device (2) is designed as a plastic wallet in which the chip card (1) is permanently carried, whereby the soiling of the sensitive outer contact points of the chip card (1) can be avoided, and in that the combination control element, by means of which activation is to be performed and which, in addition, represents a fingerprint sensor, is provided in the input/output device (2).

3. Transmitting/receiving device for the chip card system according to Claim 1, characterized in that communication is performed via infrared waves.

4. Transmitting/receiving device for the chip card system according to Claim 1, characterized in that communication is performed via microwaves.

5. Chip card system according to Claim 1, characterized in that the memory is a semiconductor memory.

6. Chip card system according to Claim 5, characterized in that the semiconductor memory stores in a non-volatile manner and is electrically programmable.

7. Chip card system according to Claims 1 and 6, characterized in that the E<sup>2</sup>PROM technique is provided for the chip.

8. Chip card system according to one of the preceding claims, characterized in that the processes concern the following functions:



9

**EP 0 159 539 B1**

10

—encoding or decoding of the data to be transmitted or to be received  
—authenticity checking

—data security against transmission errors  
—processing of fingerprint information.

5

10

15

20

25

30

35

40

45

50

55

60

65

6

FIG 1

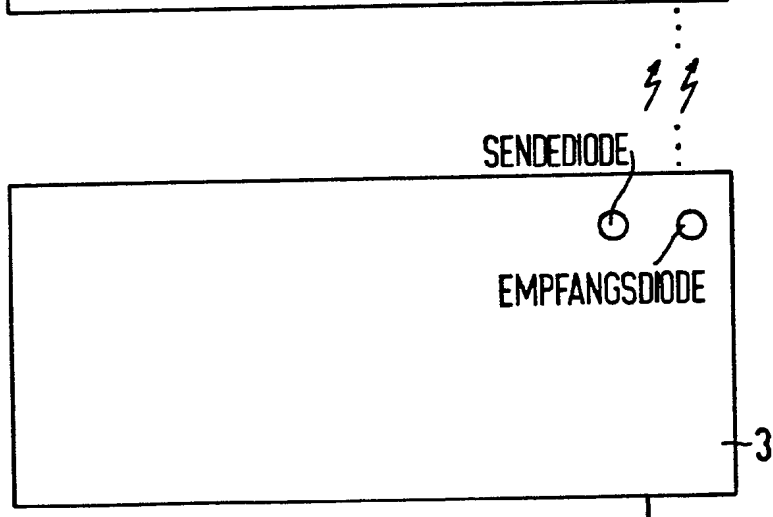
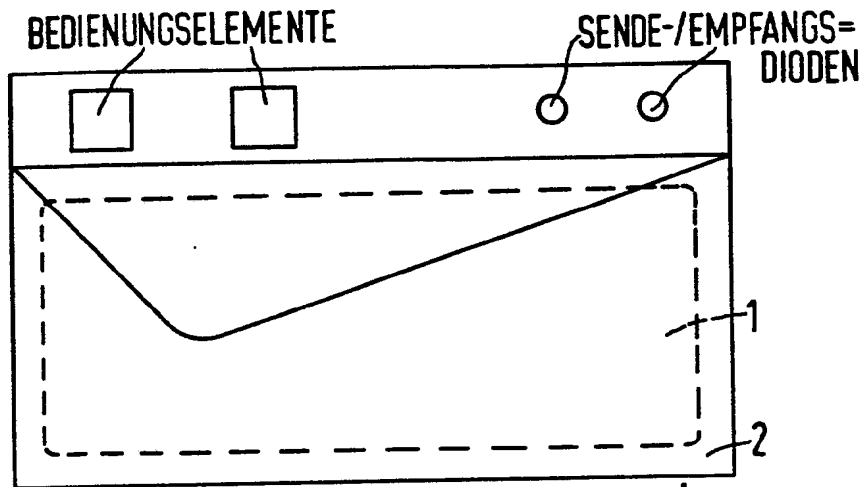
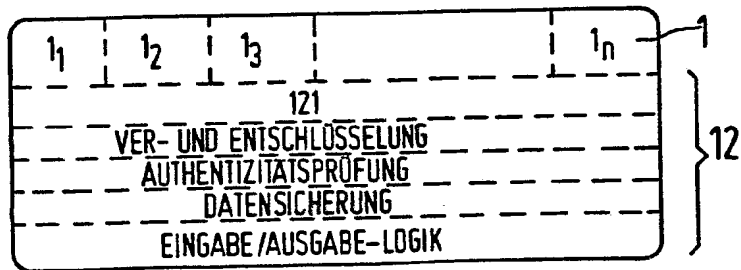
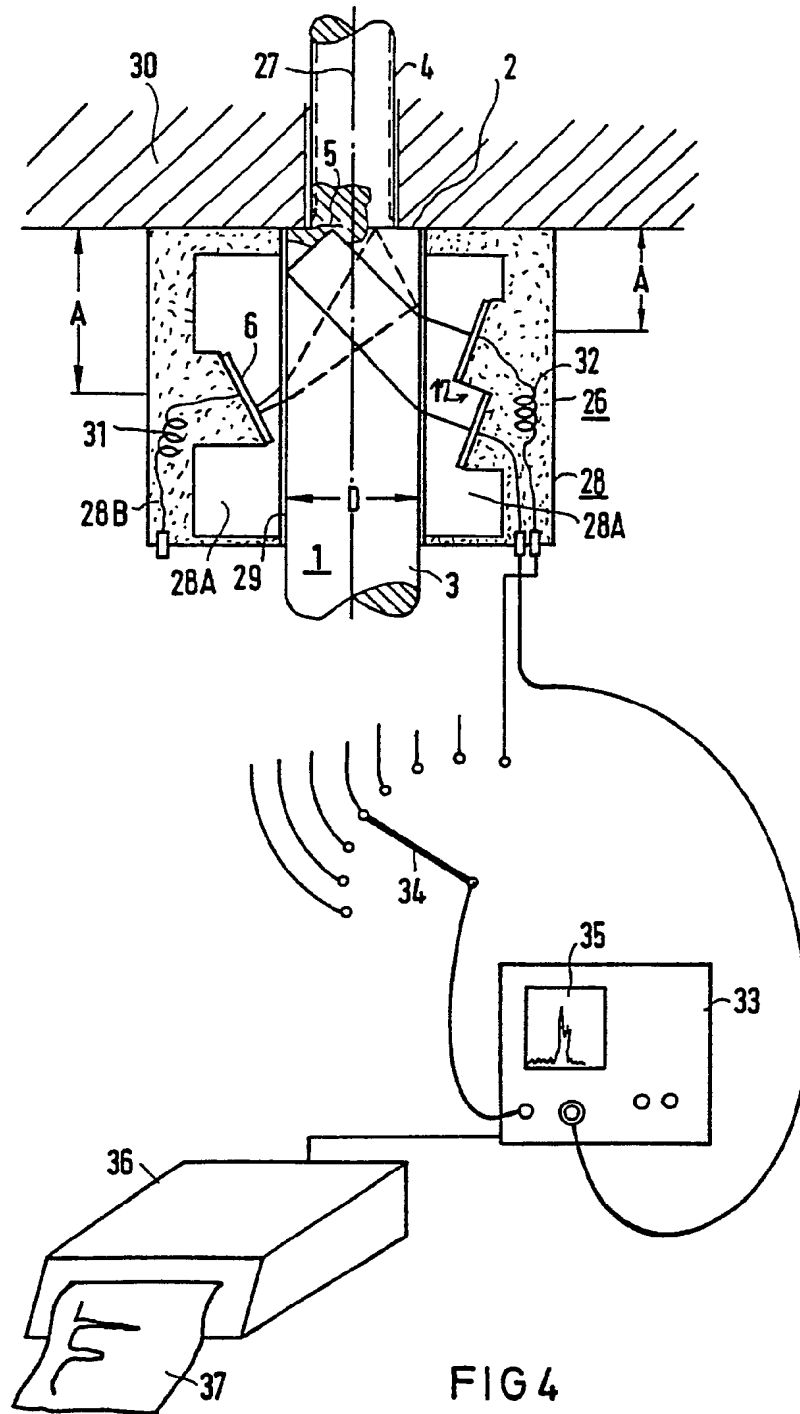


FIG 2





19



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



11 Publication number:

**0 162 221 B1**

12

### EUROPEAN PATENT SPECIFICATION

45 Date of publication of patent specification: **11.11.92** 51 Int. Cl.<sup>5</sup>: **G07F 7/10**

21 Application number: **85103117.9**

22 Date of filing: **18.03.85**

54 **Financial transaction processing system using on IC card.**

30 Priority: **19.03.84 JP 53949/84**  
**21.03.84 JP 54966/84**

43 Date of publication of application:  
**27.11.85 Bulletin 85/48**

45 Publication of the grant of the patent:  
**11.11.92 Bulletin 92/46**

84 Designated Contracting States:  
**AT BE CH DE FR GB IT LI LU NL SE**

56 References cited:  
**WO-A-83/03018**  
**DE-A- 3 222 288**  
**FR-A- 2 471 003**  
**GB-A- 2 011 671**

**PATENT ABSTRACTS OF JAPAN, vol. 5, no. 64 (P-59)[736], 30th April 1981; & JP-A-56 14 369 (FUJITSU K.K.) 12-02-1981**

**NEUES AUS DER TECHNIK, nos. 4/5, 15th September 1980, page 2, Würzburg, DE; "Kreditkarte mit Tastenfeld (und Wieder-gabeanordnung)"**

73 Proprietor: **OMRON TATEISI ELECTRONICS CO.**  
**10, Tsuchido-cho Hanazono Ukyo-ku Kyoto 616(JP)**

72 Inventor: **Yoshida, Shinya Omron Tateisi Electronics Co.**  
**10, Tsuchido-Cho Hanazono Ukyo-ku Kyoto-shi Kyoto-fu(JP)**  
Inventor: **Nagata, Masanori Omron Tateisi Electronics Co.**  
**10, Tsuchido-Cho Hanazono Ukyo-ku Kyoto-shi Kyoto-fu(JP)**

74 Representative: **WILHELMS, KILIAN & PARTNER Patentanwälte**  
**Eduard-Schmid-Strasse 2 W-8000 München 90(DE)**

**EP 0 162 221 B1**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid (Art. 99(1) European patent convention).

## Description

The present invention relates to an IC (Integrated Circuit) card and a financial transaction processing system using the IC card, and particularly, relates to an IC card capable of storing, prior to transaction, data necessary for transaction with financial bodies such as a bank and a credit company.

Presently, a magnetic card such as so-called cash card and credit card has been widely used for payment, deposit, transfer and the like through an online system in the financial bodies such as a bank and a credit company. Data for identifying a customer, such as a secret number, is magnetically stored in the magnetic card. When a transaction is performed, a customer goes to a bank at which he has a bank account, with such magnetic card, and inserts his card into a terminal such as an Automatic Teller Machine (ATM) and a cash dispenser (CD) installed therein and enters into the terminal data necessary for transactions such as a secret number, a kind of transaction and a transaction amount by operating inputting means such as a keyboard in accordance with predetermined procedures. The information of secret number read out by the terminal and information of each of transactions entered into the terminal by a customer are transmitted to a center of the bank, and in response to these informations, a center file is renewed and then an instruction for performing the transaction is provided to the terminal. Thus, any transaction is performed between the customer and the terminal.

Recently, kinds of transactions by means of an online system tend to include a transaction, such as a transfer, which is not so often used, and in consideration of recent social circumstances, it can be expected that such kind of transaction is progressively increased. Since the presently used magnetic card has only a function identifying a customer, the customer must determine transaction data such as kind of transaction and transaction amount at the time of performing a transaction and enter the same into a terminal, which means that there are increased selecting factors and operating procedures for the client in operating the terminal. Therefore, since it is expected that some customer encounters some difficulty, displaying means such as CRT is, as auxiliary means, provided in the terminal so that the procedure or order of transaction and selecting factors can be displayed to the customer. However, such auxiliary means have the limitation to some extent and, particularly, a customer who is not so familiar with terminal has difficulty in making transaction operations within a short time period, resulting in inefficiency of transaction processing.

In addition, such a conventional magnetic card is sometimes subjected to unfair use through theft, loss and the like. Such unfair use is usually made by a transaction terminal such an ATM and CD without any person in charge thereof. Of course, even in such a case, a secret number must be known to such unfair user. However, the information stored in a conventional magnetic card can be easily decoded and it is likely that such secret number tends to comprise a date of birthday, a telephone number and the like, of the customer, and hence an unfair user can easily assume such secret number. Therefore, a conventional magnetic card has a problem relating to security.

A financial transaction processing system according to the preamble of claim 1 is known from WO-A-83 03 018.

The invention is as claimed in claim 1.

Accordingly, a primary object of the present invention is to provide an integrated circuit card which can reduce load for transaction processing on the terminal side and can enhance security for transaction.

Another object of the present invention is to provide a financial transaction processing system using an integrated circuit card, which can reduce load for transaction processing on a terminal side and can enhance the security for transaction.

A primary advantage of the present invention is that the data necessary for transaction can be stored in advance in an integrated circuit card, prior to transaction processing.

A further advantage of the present invention is that after an integrated circuit card is inserted into a terminal the number of operating procedures can be largely decreased and a time period required for transaction is also reduced so that efficiency of transaction processing can be increased, because a customer can surely enter the data necessary for transaction into his integrated circuit card for storage before he goes to a bank.

Still further advantage of the present invention is that a secret relating to transaction can be completely kept since the data relating to transaction can be entered when he is alone.

In addition, a further advantage of the present invention is that even if an IC card happens to be owned by an unfair user through theft, loss and the like, it is difficult to read out the data of secret number and the like and hence the IC card is never unfairly used, since the transaction data such as secret number which may cause unfair use by the others can be erased after completion of transaction.

A still further advantage of the present invention is that a customer can know a previous transaction record through the IC card by erasing only a portion of data such as secret number after com-

pletion of transaction and by keeping the remaining transaction data unerased.

A still further advantage of the present invention is that, since the data necessary for transaction can be stored in advance, together with a desired effective time period data and the transaction processing can be permitted within the effective time period in a terminal, it is impossible to perform transaction such as payment transaction after lapse of the set effective time period, even if the IC card happens to be owned by an unfair user through theft, loss and the like, and hence an unfair use by the others can be prevented.

These objects and other objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings.

Fig. 1 is a schematic block diagram showing an electrical structure of an integrated circuit card;

Fig. 2 is a perspective view of an integrated circuit card;

Fig. 3 is a memory map of an integrated circuit card;

Fig. 4 is a flow diagram explaining a transaction data storing operation of an integrated circuit card;

Fig. 5 is a schematic block diagram showing an electric structure of a terminal for use with an integrated circuit;

Fig. 6 is a memory map of a terminal for use with an integrated circuit card shown in Fig. 5;

Fig. 7 is a flow diagram explaining a transaction data reading operation in a financial transaction processing system;

Fig. 8 is a flow diagram explaining a transaction processing of a terminal for use with an integrated circuit card;

Fig. 9 is a flow diagram explaining a transaction processing of a terminal for use with an integrated circuit card of an embodiment of the present invention;

Fig. 10 is a memory map of an integrated circuit card of another embodiment of the present invention;

Fig. 11 is a flow diagram explaining a transaction data storing operation of an integrated circuit card of another embodiment of the present invention;

Fig. 12 is a memory map of a terminal for use with an integrated circuit card of another embodiment of the present invention;

Fig. 13 is a flow diagram explaining a transaction processing of a terminal for use with an integrated circuit card of another embodiment of the present invention.

Fig. 1 is a schematic block diagram showing an electric structure of an IC card.

The IC card has the same size and configuration as a conventional magnetic card such as a cash card and a credit card, and contains at least an IC memory such as a read only memory and a random access memory, a central processing unit made of an integrated circuit, and a plurality of, usually eight, contacts for communicating with a terminal. In a conventional magnetic card, storage capacity is rather small and it is easy to decode stored information. The feature of an IC card is that, as compared with a conventional magnetic card, a storage capacity is large and security is excellent because stored information can be made not to be decoded by the others by using a program which can not be easily read out. In addition, the IC card itself can provide some request to the terminal.

Referring to Fig. 1, an input/output port having an input/output line terminal 8 is connected through a data bus 9 to a central processing unit (CPU) 2, a read only memory (ROM) 3, a random access memory (RAM) 4, a display 5 and a keyboard 6. An electric power is supplied from a battery 7 to the input/output port 1, the central processing unit 2, the read only memory 3, the random access memory 4, the display 5 and the keyboard 6. The input/output port 1 is used for communicating with a terminal, (see Fig. 5), for use in the IC card in transaction processing. The ROM 3 stores fixed data relating to transaction processing, such as an ID number, a bank number, a branch number, an account number and an effective time period, and a program for transaction processing. The RAM 4 stores data necessary for each transaction, such as a secret number and transaction amount. The keyboard 6 is used for entering the data necessary for each transaction into the RAM 4. The display 5 displays the entered data to a user.

Fig. 2 is a perspective view of an IC card. Referring to Fig. 2, on a front surface panel of an IC card body 10, a power switch 11, a keyboard 12 including a plurality of touch keys, a liquid crystal display 13 and a plurality of contacts 14 are provided. The power switch 11 is used for supplying a power to each of constituent elements of the IC card shown in Fig. 1. The keyboard 12 is used for entering the data necessary for transaction processing into the IC card so that the data is stored in the ROM 4. The liquid crystal display 13 displays the above described entered data to a user. The contacts 14 are used for electrically connecting to the terminal when the IC card is inserted into the terminal.

Fig. 3 is a diagram showing a memory map of the IC card, which comprises a storage region in a read only memory and a storage region in a random access memory. The storage region in the ROM comprises a program storage area, an ID

number storage area, a bank number storage area, a branch number storage area, an account number storage area, and an effective time period storage area. The storage region in the RAM comprises a secret number storage area, a deposit (credit) storage area, a payment storage area, a transaction number storage area, a bank-to-be-transferred area, an account-to-be-transferred area, and a transfer amount area.

Fig. 4 is a flow diagram explaining a specific operation program for entering transaction information and storing the same, prior to transaction processing, the program being stored in the ROM 3 of the IC card.

Now, referring to Figs. 1 to 4, a specific operation of the IC card when the IC card transaction data is entered will be described. The embodiment shown in Fig. 4 indicates a situation where a kind of transaction (referred to as "a transaction number" hereinafter), a secret number and a transaction amount are stored in the IC card, prior to transaction processing.

Before going to a bank at which a client has a bank account, he enters into his own IC card the above described transaction data, that is, the transaction number, the secret number and the transaction amount whenever and wherever he wishes to do so. First, the customer turns a power switch 11 of the IC card on (step S1). As a result, a power is supplied from the battery 7 to each of constituent elements of the IC card shown in Fig. 1. Then, the customer operates the keyboard 12 to select a desired transaction number, that is, the kind of transaction, to enter the same into the IC card (step S2). In this embodiment, it is assumed that the transaction number 1 denotes a payment processing, the transaction number 2 denotes a deposit processing, and the transaction number 3 denotes a transfer processing. The selected transaction number is stored in the transaction number storage area in the RAM 4 (step S3). In addition, the following data entering and storing operations are performed based on the program corresponding to the selected transaction number, stored in program storage area of the ROM 3.

If and when the customer selects the transaction number 1 (payment) (step S4), he first enters his secret number using the keyboard 12 (step S5). The secret number is stored in the secret number storage area of the RAM 4 (Fig. 3) in the IC card (step S6). Subsequently, the customer further enters an amount of payment using the keyboard 12 (step S7). The data of the payment amount is stored as well in the payment storage area of the RAM 4 (step S8). As a result, storing transaction data for payment processing is completed and then a power supply of IC card is automatically turned off in accordance with a program (step S9).

If and when the transaction number 2 (deposit) is selected (step S10), the customer enters an amount of deposit using the keyboard 12. The data of such amount is stored in the deposit storage area of the RAM 4 (step S12). As a result, the transaction data storage for deposit processing is completed, and then the power supply of the IC card is automatically turned off (step S13).

If and when the transaction number 3 (transfer) is selected (step S14), the customer first enters his secret number by using the keyboard 12 (step S15). The secret number is stored in the secret number storage area of the RAM (step S16). Subsequently, the customer enters the bank number to be transferred and the amount number thereof by using the keyboard 12 (step S17). Such data is also stored in the corresponding areas of the RAM 4 (step S18). In addition, the customer enters an amount of transfer using the keyboard 12 (step S19). The amount data is also stored in the transfer amount area of the RAM 4 (step S20). As a result, storing the data relating to transfer processing is completed and then a power supply of IC card is automatically turned off (step S21). Each of the data entered by the keyboard 12 is displayed in the liquid crystal display 13 each time the data is entered, so that the customer can confirm whether the entered data is correct or not.

As described in the foregoing, according to the present embodiment, a transaction number, a secret number, and a transaction amount can be securely stored in advance in the IC card, prior to transaction processing.

Fig. 5 is a schematic block diagram showing an electric structure of a terminal communicating with an IC card shown in Figs. 1 to 4. Referring to Fig. 5, an IC card reader 15 is a unit for communication through the input/output port 1 and the contacts 14 of the IC card as inserted. A cathode ray tube (CRT) 16 is a unit for displaying procedures of transaction and the like to a customer. A keyboard 17 is a unit which a customer communicate with the terminal, if necessary. A slip issuing machine 18 receives permission of payment from a center and issue a slip. A paper receiving portion 19 includes unit for receiving papers the customer inserts on deposit and counting the number thereof. A paper discharging portion 20 includes a unit for discharging papers to the customer. A bankbook printing portion 21 prints the transaction record on the entered bankbook when the bankbook is inserted into the terminal together with the IC card. Each of these units is connected to a control 22 through internal data buses, so that the control 22 can control operations of these units. In addition, the control 22 is also connected to a central processing unit of a center (not shown) for each bank through a line control 23 and a

input/output terminal 24.

Fig. 6 is a diagram showing a memory map of a terminal for use with the IC card as shown in Fig. 5.

Fig. 7 is a flow diagram explaining a specific reading operation of a financial transaction processing system, that is, explaining a specific reading operation between the IC card shown in Fig. 1 and the terminal shown in Fig. 5.

Referring to Figs. 5 to 7, a specific reading operation of the financial transaction processing system will be described. Reading of the IC card is performed by means of half duplex communication system, which is the same as communication between a terminal and a center CPU.

First, the IC card which is the one embodiment as shown in Figs. 1 to 4 is entered into a terminal for use with the IC card, which is shown in Fig. 5 and installed in a bank (step S22). Then, an electric power is supplied to each of constituent elements of the IC card shown in Fig. 1 and the CPU 2 generates a card insert command based on the program stored in the ROM 3 and transmits the command to the IC card reader 15 of the terminal through the input/output port 1 (step S23). Upon receipt of the command by the terminal (step S24), the terminal generates an ID number request command and transmits the same to the IC card (step S25). Then, in the IC card, the central processing unit 2 receiving the ID number request command from the terminal through the input/output port 1 (step S26) transmits the ID number stored in the storage region of the ROM 3, as shown in Fig. 3, to the IC card reader 15 of the terminal through the input/output port 1 (step S27). The terminal receives such ID number (step S28) and generates a bank number request command and transmits the same to the IC card (step S29). Then, in the IC card, the central processing unit 2 receiving the bank number request command from the terminal through the input/output port 1 (step S30) transmits the bank number stored in the storage region of the ROM 3 as shown in Fig. 3 to the IC card reader 15 of the terminal through the input/output port 1 (step S31). The terminal receives such bank number (step S32) and generates an effective time period data request command and transmits the same to the IC card (step S33). Then, in the IC card, the CPU 2 receiving the effective time period data requesting command from the terminal through input/output port 1 transmits the effective time period data stored in the storage region of the ROM 3 as shown in Fig. 3 to the IC card reader of the terminal through the input/output port 1 (steps S35 and S36). As described in the foregoing, the fixed data relating to transaction, which is stored in the ROM 3 in the IC card, is first read out by the terminal. Then, the terminal generates an RAM

storage contents requesting command for requesting the transaction data stored in advance in the RAM 4 in accordance with the respective programs and transmits the same to the IC card (step S37). Correspondingly, in the IC card, the central processing unit 2 receiving the RAM storage contents requesting command from the terminal through the input/output port 1 (step S38) transmits the RAM storage contents stored in the storage region of the RAM 4 as shown in Fig. 3, that is, the transaction data such as transaction number, a secret number, a transaction amount and a bank-to-be-transferred, to the IC card reader 15 of the terminal through the input/output port 1 (steps S39 and S40). The IC card completed its role by transmitting the RAM storage contents to the terminal and then a power supply is turned off in accordance with program and, upon completion of transaction processing, the IC card is returned to the customer from the terminal (step S41).

Fig. 8 is a flow diagram explaining a specific transaction processing operation of the terminal from insertion of the IC card to termination of transaction processing.

Now, referring to Figs. 1 to 8, a specific transaction processing of the terminal will be described.

From the IC card inserted into the terminal by a customer (step S42), the data relating to transaction is read out from the ROM 3 and RAM 4 shown in Fig. 7 (steps S43 and S44). First, the terminal confirm the fixed data inherent to the specific bank, such as ID number, a bank number, an effective time period data read out from the ROM 3 (steps S45, S46 and S47) and if and when any of inconsistencies occurs, the content stored in the RAM 4 of the IC card is erased (step S48) and the IC card is returned to the customer (step S49). If and when all of the requirements are satisfied, the following transaction processing is performed in accordance with a predetermined kind of transaction.

If and when the customer sets in advance a transaction number 1 (payment) (step S50), it is determined whether the secret number read out from the RAM 4 of the IC card is correct or not (step S51). If correct, the terminal transmits to the CPU of the center for each bank the transaction data read out from the ROM 3 and RAM 4 of the IC card (step S52) in response to the data as transmitted to the center, the center retrieves and renews the corresponding file and provides an instruction of permission for payment to the terminal. Upon receipt of this instruction (step S53), the terminal instructs a slip issuing machine 18 to issue a payment slip and instruct the paper discharging portion 20 to discharge the necessary papers to the client (step S54). After completion of payment to a customer, the contents stored in the RAM 4 of the IC card are erased for security (step S55) and



the IC card is returned to the customer in accordance with the program (step S56) and then the transaction is completed.

If and when the customer presets in advance a transaction number 2 (deposit) (step S57), the customer inserts papers to be deposited to the paper receiving portion 19 (step S58). The paper receiving portion 19 counts the number of the papers (step S59) and determines whether the counted amount coincides with the amount stored in advance in the RAM 4 of the IC card (step S60). If these amounts coincide with each other, the terminal transmits to the center CPU of the bank the transaction data read out from the ROM 3 and RAM 4 of the IC card (step S61). Thus, the center retrieves and renews the corresponding file in accordance with the transmitted data. As a result, a deposit transaction processing is terminated and then the content of transaction stored in the RAM 4 of the IC card is erased (step S62) and the IC card is returned to the customer in accordance with the program (step S63).

If and when the customer presets the transaction number 3 (transfer) (step S64), it is determined whether the secret number read out from the RAM 4 of the IC card is correct or not (step S65). If correct, the terminal transmits to the center CPU of the bank the transaction data read out from the ROM 3 and RAM 4 of the IC card (step S66). The center CPU communicates with the bank to be transferred, in response to the data such as the bank to be transferred and the account number thereof, and an amount of transfer which are entered in advance. As a result, the transfer transaction is completed (step S67), and the content of transaction stored in the RAM 4 of the IC card is erased (step S68) and the IC card is returned to the customer in accordance with the program (step S69).

As described in the foregoing, in accordance with the present embodiment, a transaction number, a secret number and a transaction amount, which are entered through the terminal in transaction processing in a conventional system, can be securely entered in advance into an IC card, so that a customer can keep a secret of transaction. Particularly, if the transaction number is set as deposit or transfer, an unfair user can not use the IC card for the purpose of payment and hence a good security is obtained. In addition, an operating time period when a customer can handle or operate a terminal can be decreased and hence efficiency of transaction processing can be improved.

Fig. 9 is a flow diagram explaining a transaction processing of a terminal for use with an IC card, which is an embodiment of the present invention. The embodiment shown in Fig. 9 is the same as the financial transaction processing system as

described referring to Figs. 1 to 8, except for the following points.

More particularly, whereas in the steps S55, S62 and S68 of Fig. 8, the storage contents of the RAM 4 of the IC card are all erased, in the flow diagram of Fig. 9, only a secret number is erased in the steps S70 and S71, instead of the steps S60 and S68, and erasing the storage contents of the RAM 4 in the step S62 is not performed.

More specifically, if and when a customer sets in advance a transaction number 1 (payment) (step S50), only the secret number out of a contents stored in the RAM 4 of the IC card is erased for safety in response to a command from a terminal when payment processing to a customer is completed (step S70) and the IC card is returned to a customer in accordance with the program (step S56) and the transaction is completed.

If and when a customer sets in advance a transaction number 2 (deposit) (step S57), the transaction contents stored in the RAM 4 of IC card are never erased after the completion of deposit transaction and the IC card is returned to a customer in accordance with a program (step S63) and a transaction is completed.

If and when a customer sets in advance a transaction number 3 (transfer) (step S64), only a secret number out of the transaction contents stored in the RAM 4 of the IC card is erased, for safety, in response to a command from the terminal (step S71), after completion of transfer transaction (step S67), and the IC card is returned to a customer in accordance with a program (step S69) and the transaction is completed.

As described in the foregoing, in accordance with the present embodiment, after completion of transaction, a secret number stored in the IC card can be erased, so that unfair use can be prevented, and other transaction record relating to transaction amount and the like can be left in the IC card.

Fig. 10 is a memory map of an IC card of another embodiment of the present invention, Fig. 11 is a flow diagram explaining a transaction data storing operation of the IC card, Fig. 12 is a memory map of a terminal for communicating with the IC card and Fig. 13 is a flow diagram explaining a transaction processing of the terminal.

The embodiment shown in Figs. 10 to 13 is the same as the financial transaction processing system shown in Figs. 1 to 8, except for the following points.

As shown in the step S72 of Fig. 11, a customer sets a second effective time period and enters the data thereof into the IC card. Meanwhile, in the present embodiment, an effective time period so far described as a fixed data is particularly referred to as a first effective time period. The second effective time period is determined in con-

sideration of the time interval from the time of the data entrance to the arrival to a bank. That is, first the time when transaction will be completed is expected and then the second effective time period is set so that the period can lapse after completion of transaction. As shown in Fig. 10, the second effective time period is stored in the storage region of the RAM 4 of the IC card (step S73).

In case where a transaction processing is performed using an IC card in which the above described second effective time period is stored, it is determined in the terminal whether the time when the transaction in question is being performed is in the second effective time period stored in the RAM 4 of the IC card, as shown in the step S74 of Fig. 13. If and when the second effective time period lapses, the contents stored in the RAM 4 of the IC card are erased (step S48) and the IC card is returned to a customer (step S49). If and when the second effective time period does not lapse, a transaction processing is performed in accordance with the kind of transaction as set in advance.

As described in the foregoing, in accordance with the present embodiment, security for transaction can be increased by setting the desired effective time period, because even if the IC card happens to be owned by an unfair user through theft, loss and the like, the unfair use can not be realized if the effective time period lapses.

Meanwhile, although in the above described embodiments, a transaction number, a secret number and a transaction amount are stored in advance in an IC card, it may be possible to make an IC card store only a transaction number prior to transaction processing and then to enter a secret number and a transaction amount by using a terminal at the time of transaction processing, and, in addition, it may be also possible to make the IC card store a secret number and a transaction amount, prior to the transaction processing and then enter a transaction number using a terminal at the time of transaction.

## Claims

1. A financial transaction processing system comprising: an integrated circuit card for use in financial transaction processing, including
  - first storing means (4) for storing data necessary for the financial transaction processing;
  - second storing means (3) containing a program of processing procedures for performing the financial transaction;
  - data entering means (6) for entering said data necessary for financial transaction processing into said first storing means;
  - data display means (5) for displaying said entered data; and

data processing means (2) for processing said entered data in accordance with said program stored in said second storing means; terminal means for communicating with said integrated circuit card, including

data reading means (15) for reading out the data stored in said first storing means; and

transaction processing means (22) for performing said financial transaction in accordance with said read data, characterized by

said terminal means comprising transaction termination detecting means for detecting termination of said transaction processing, and

data erasing means (step S70 and step S71) responsive to the output of said transaction termination detecting means for erasing a portion of the data stored in said first storing means (4), said erased data including a secret number.

2. A financial transaction processing system in accordance with claim 1, wherein said integrated circuit card includes third storing means (step S73) for storing an effective time period of the data necessary for financial transaction processing, the data of the effective time period being entered by said data entering means (6), said terminal means includes
  - effective time period reading means for reading said effective time period stored in said third storing means, and
  - effective time period detecting means (step S74) for detecting that the time when transaction is now being performed is within said effective time period,
  - said data reading means being responsive to the output of said effective time period detecting means for reading the data stored in said first storing means (4).

## Patentansprüche

1. Verarbeitungseinrichtung für finanzielle Transaktionen mit
  - einer IC-Karte zur Verwendung bei der Finanztransaktionsverarbeitung, welche aufweist
    - erste Speichermittel (4) zum Speichern von für die Finanztransaktionsverarbeitung notwendigen Daten,
    - zweite Speichermittel (3), welche ein Programm für Verarbeitungsabläufe zur Durchführung der Finanztransaktion enthalten,
    - Dateneingabemittel (6) zum Eingeben der für die Finanztransaktionsverarbeitung notwendigen Daten in die ersten Speichermittel,
    - Datenanzeigemittel (5) zum Anzeigen der

einggegebenen Daten, und

Datenverarbeitungsmittel (2) zum Verarbeiten der eingegebenen Daten gemäß dem in den zweiten Speichermitteln gespeicherten Programm;

mit Terminalmitteln zum Informationsaustausch mit der IC-Karte, welche aufweisen

Datenlesemittel (15), zum Auslesen von in den ersten Speichermitteln gespeicherten Daten, und

Transaktionsverarbeitungsmittel (22) zur Durchführung der Finanztransaktion gemäß den gelesenen Daten, dadurch gekennzeichnet, daß

die Terminalmittel

Transaktionsbeendigungsfeststellmittel zum Feststellen einer Beendigung der Transaktionsverarbeitung, und

Datenlöschmittel (Schritt S70 und Schritt S71), die auf die Ausgabe der Transaktionsbeendigungsfeststellmittel ansprechen, zum Löschen eines Teils der in den ersten Speichermitteln (4) gespeicherten Daten, wobei die gelöschten Daten eine Geheimnummer enthalten.

2. Einrichtung zur Verarbeitung einer finanziellen Transaktion nach Anspruch 1, bei welcher die IC-Karte dritte Speichermittel (Schritt S73) zum Speichern einer wirksamen Zeitdauer der für die Finanztransaktionsverarbeitung nötigen Daten aufweist, wobei die Daten der effektiven Zeitdauer mit den Eingabemitteln (6) eingegeben werden, wobei die Terminalmittel

Lesemittel für die effektive Zeitdauer zum Lesen der in den dritten Speichermitteln gespeicherten effektiven Zeitdauer, und

Feststellungsmittel (Schritt S74) für die effektive Zeitdauer zum Feststellen, daß die Zeit, zu der die Transaktion gerade durchgeführt wird, innerhalb der effektiven Zeitdauer liegt, enthalten,

wobei die Datenlesemittel auf die Ausgabe der Feststellungsmittel für die wirksame Zeitdauer mit dem Lesen der in den ersten Speichermitteln (4) gespeicherten Daten ansprechen.

## Revendications

1. Un système de traitement de transactions financières comprenant : une carte à circuit intégré à utiliser dans le traitement de transactions financières incluant

un premier moyen de mémoire (4) pour mémoriser des données nécessaires pour le traitement de transactions financières;

un deuxième moyen de mémoire (3)

contenant un programme de procédures de traitement pour effectuer la transaction financière;

un moyen d'entrée de donnée (6) pour entrer dans ledit premier moyen de mémoire lesdites données nécessaires au traitement de transactions financières;

un moyen d'affichage de données (5) pour afficher ladite entrée de données; et

un moyen de traitement de données (2) pour traiter lesdites données entrées conformément audit programme mémorisé dans ledit deuxième moyen de mémorisation;

un moyen de terminal pour communiquer avec ladite carte à circuit intégré, incluant

un moyen de lecture de données (15) pour lire les données mémorisées dans ledit premier moyen de mémoire; et

un moyen de traitement de transactions (22) pour effectuer ladite transaction financière conformément auxdites données lues, caractérisé en ce que

ledit moyen de terminal comprend

un moyen de détection d'achèvement de transactions pour détecter l'achèvement dudit processus de transactions, et

un moyen d'effacement de données (étape S70 et étape S71) sensible à la sortie dudit moyen de détection d'achèvement de transactions pour effacer une partie des données mémorisées dans ledit premier moyen de mémoire (4), lesdites données effacées incluant un numéro secret.

2. Un système de traitement de transactions financières selon la revendication 1, dans lequel la carte à circuit intégré inclut un troisième moyen de mémoire (étape S73) pour mémoriser un laps de temps effectif des données nécessaires pour le traitement de transactions financières, les données du laps de temps effectif étant entrées par ledit moyen d'entrée de données (6),

ledit moyen de terminal inclut

un moyen de lecture de laps de temps effectif pour lire ledit laps de temps effectif mémorisé dans ledit troisième moyen de mémoire, et

un moyen de détection de laps de temps effectif (étape S74) pour détecter que le temps où la transaction est actuellement en cours d'exécution se trouve à l'intérieur dudit laps de temps effectif,

ledit moyen de lecture de données étant sensible à la sortie dudit moyen détecteur de laps de temps effectif pour lire les données mémorisées dans ledit premier moyen de mémoire (4).

FIG. 1

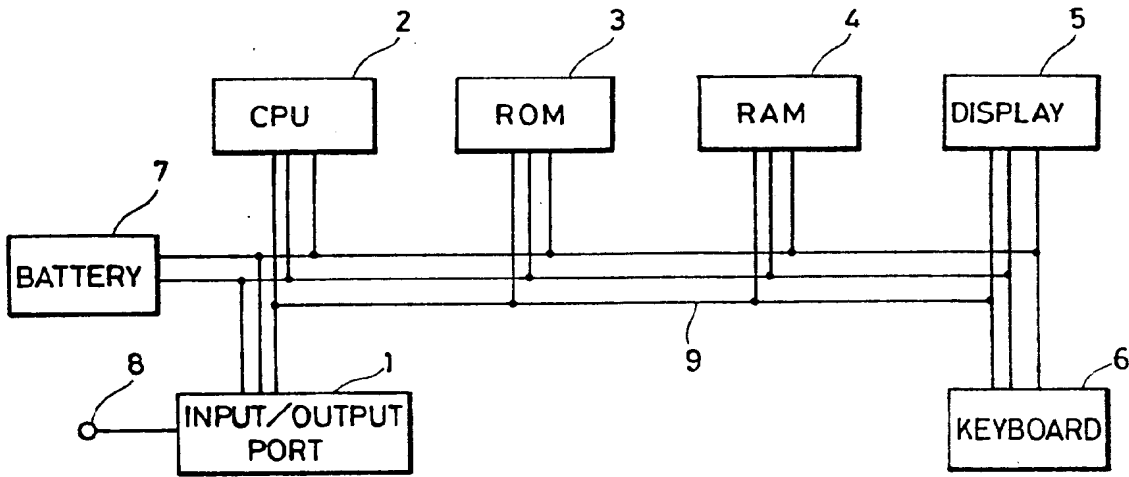


FIG. 2

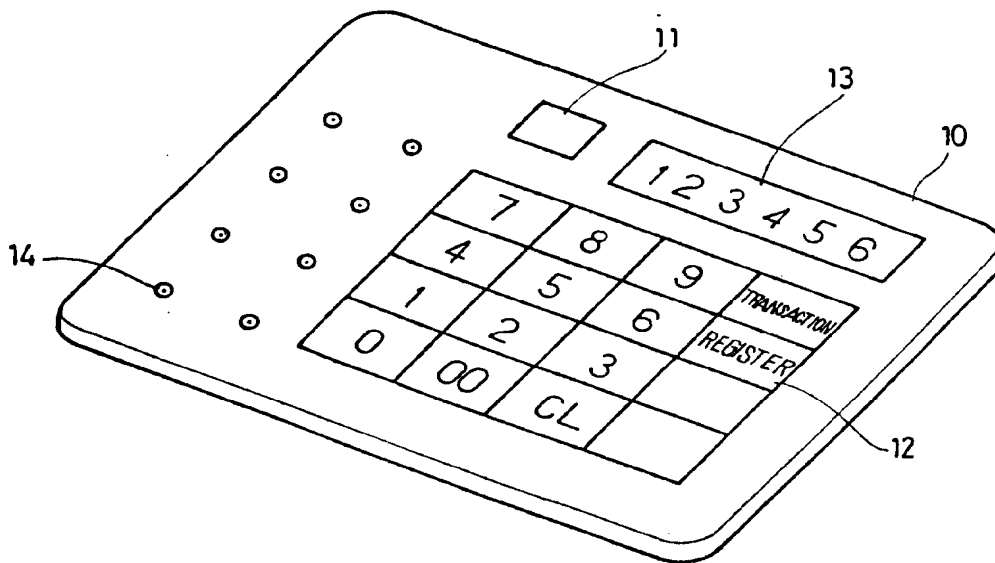


FIG. 3

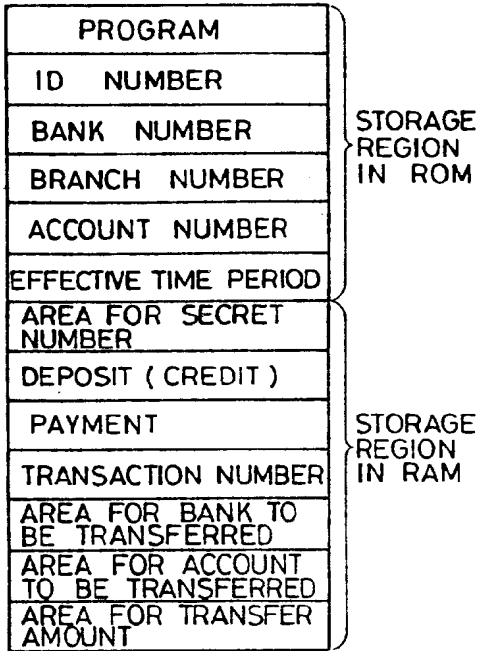


FIG. 6

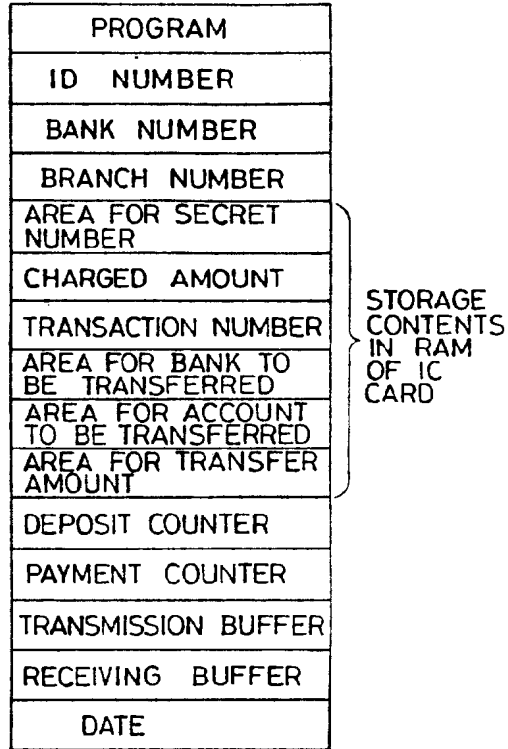


FIG. 5

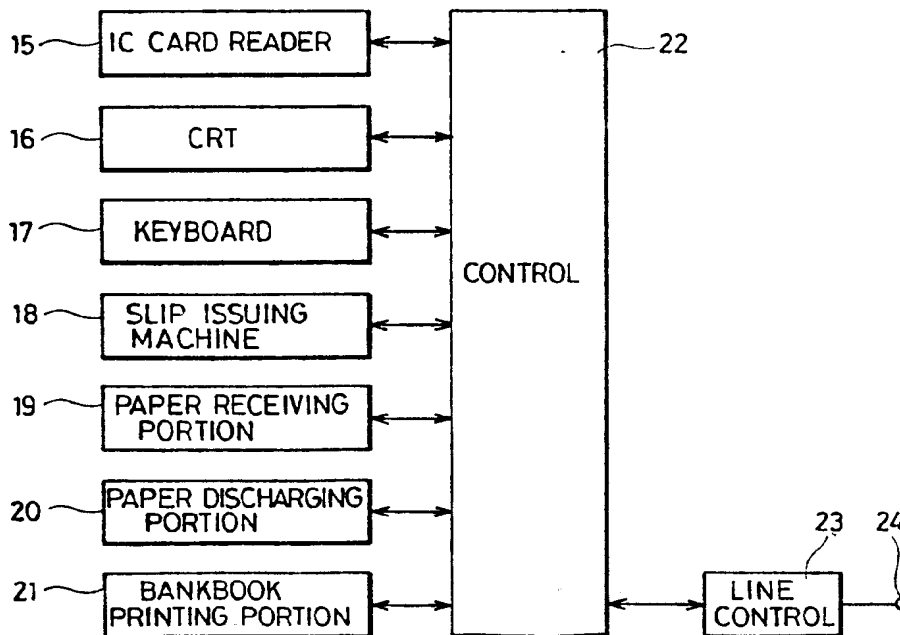


FIG. 4

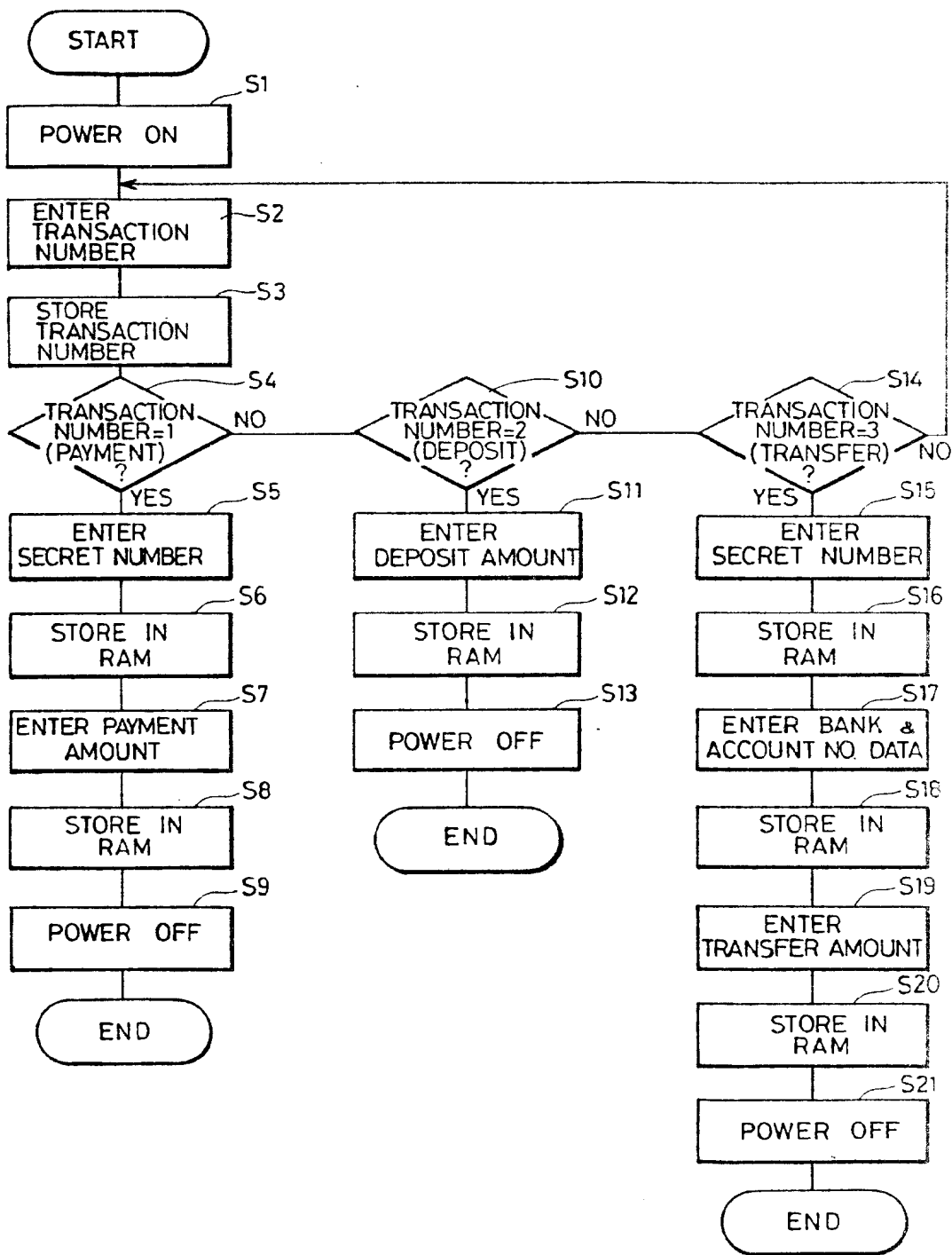


FIG. 7

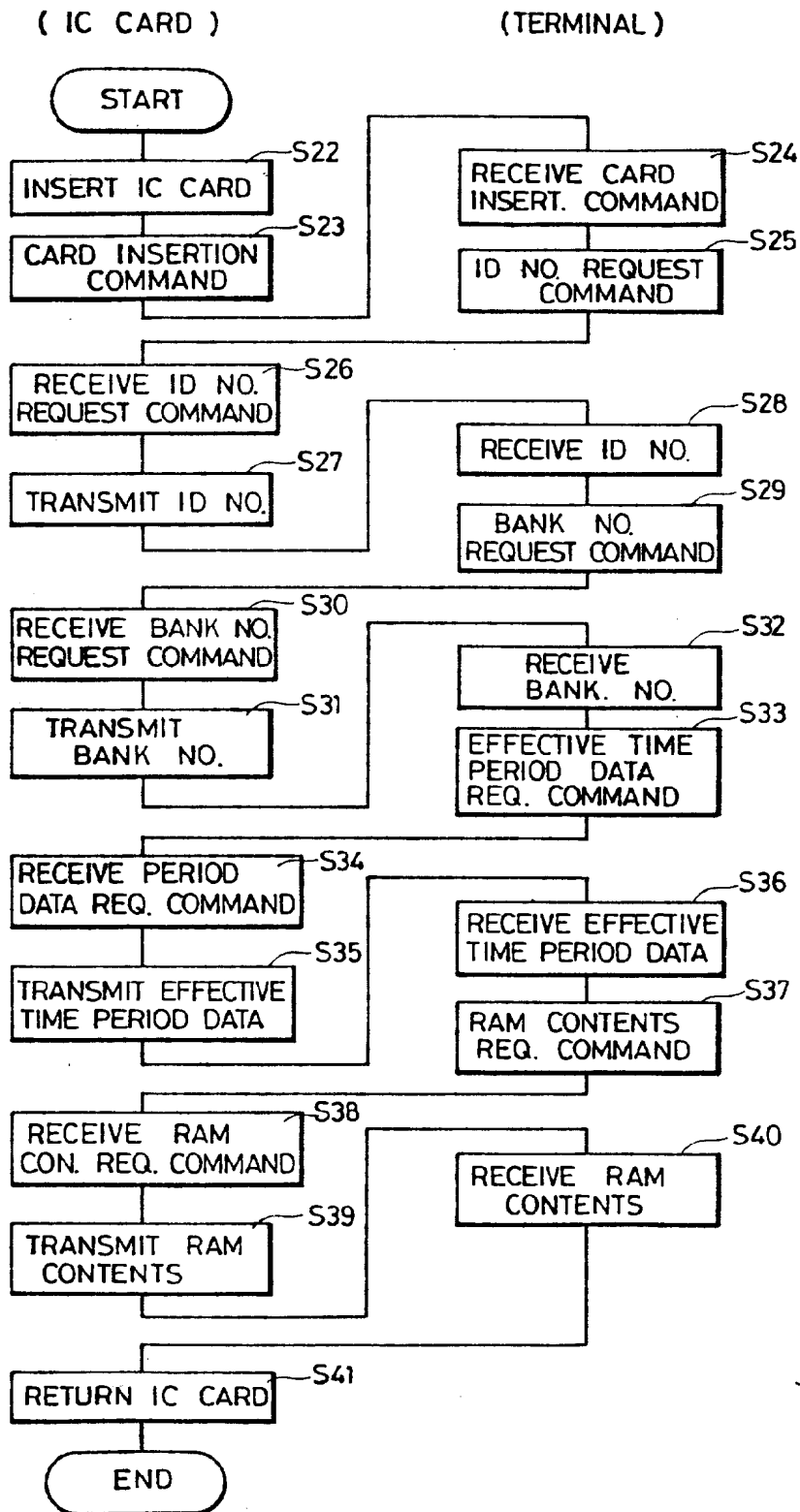


FIG. 8A

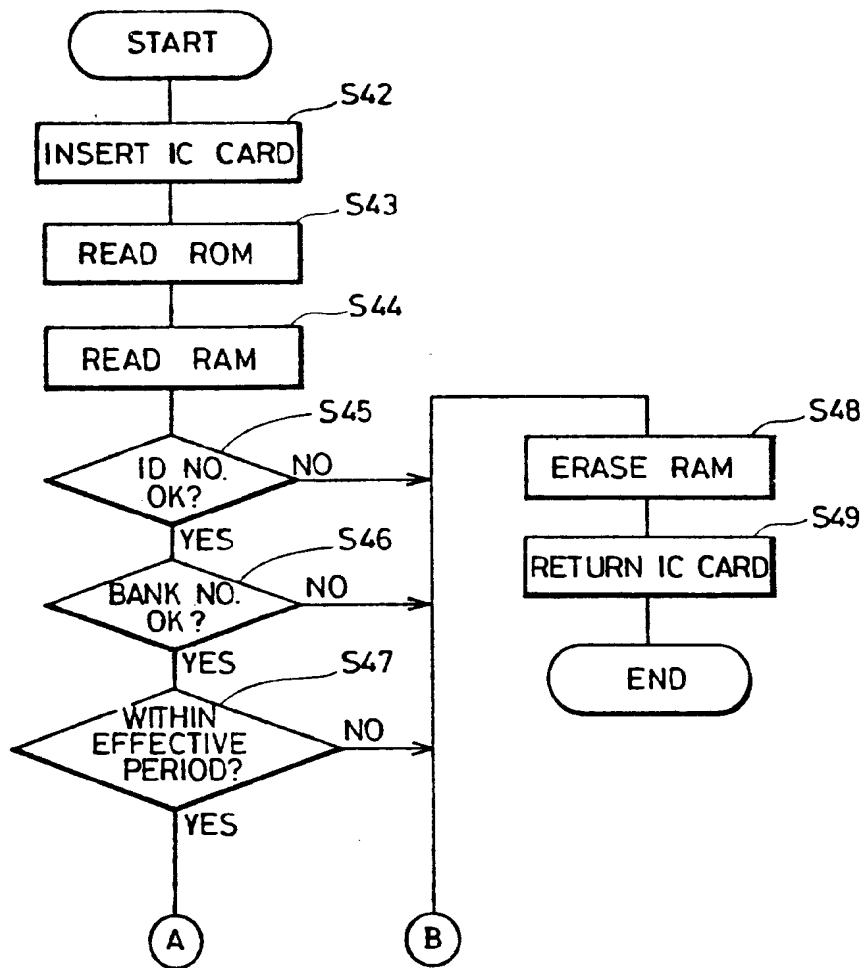




FIG. 8B

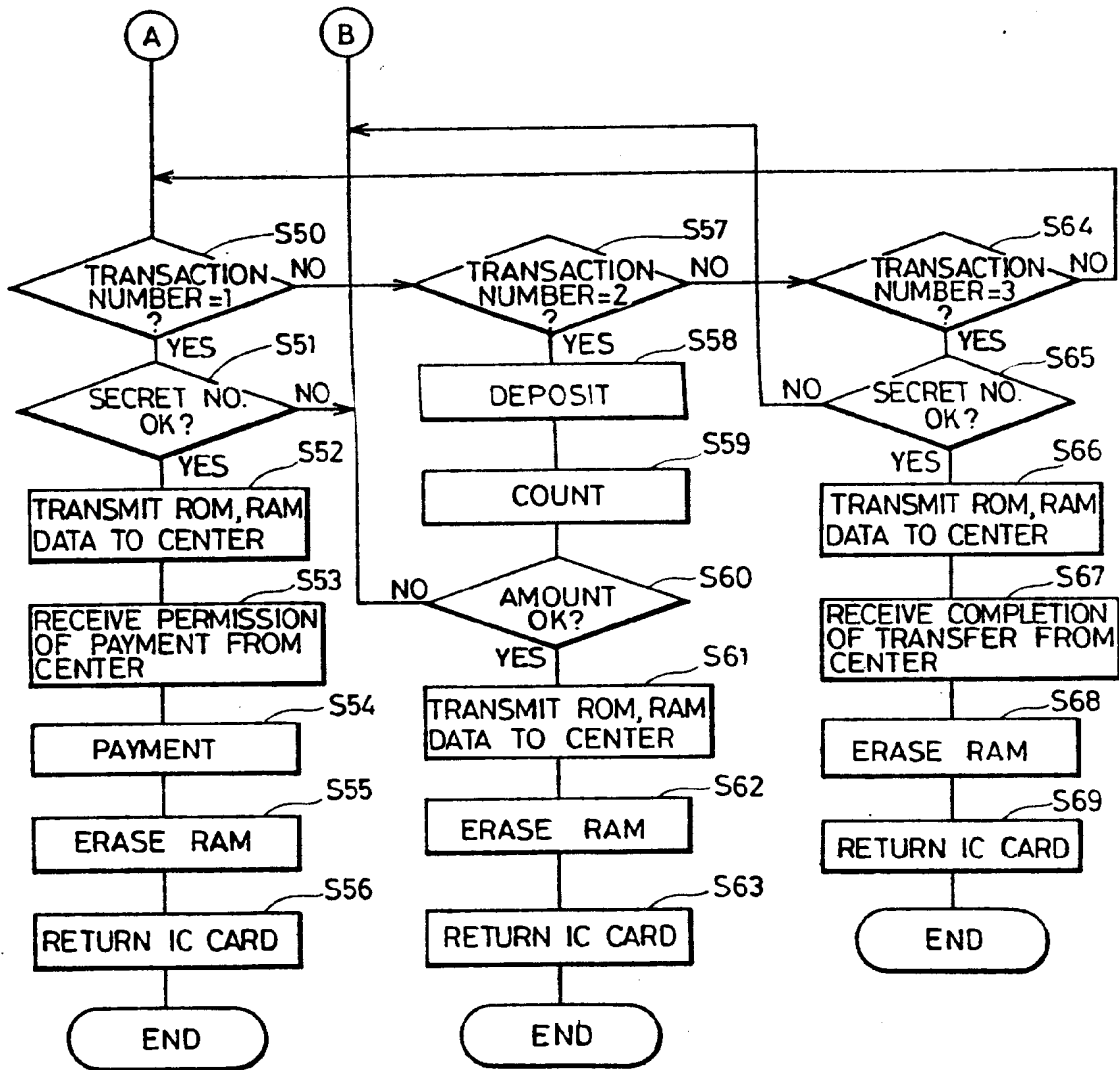


FIG. 9

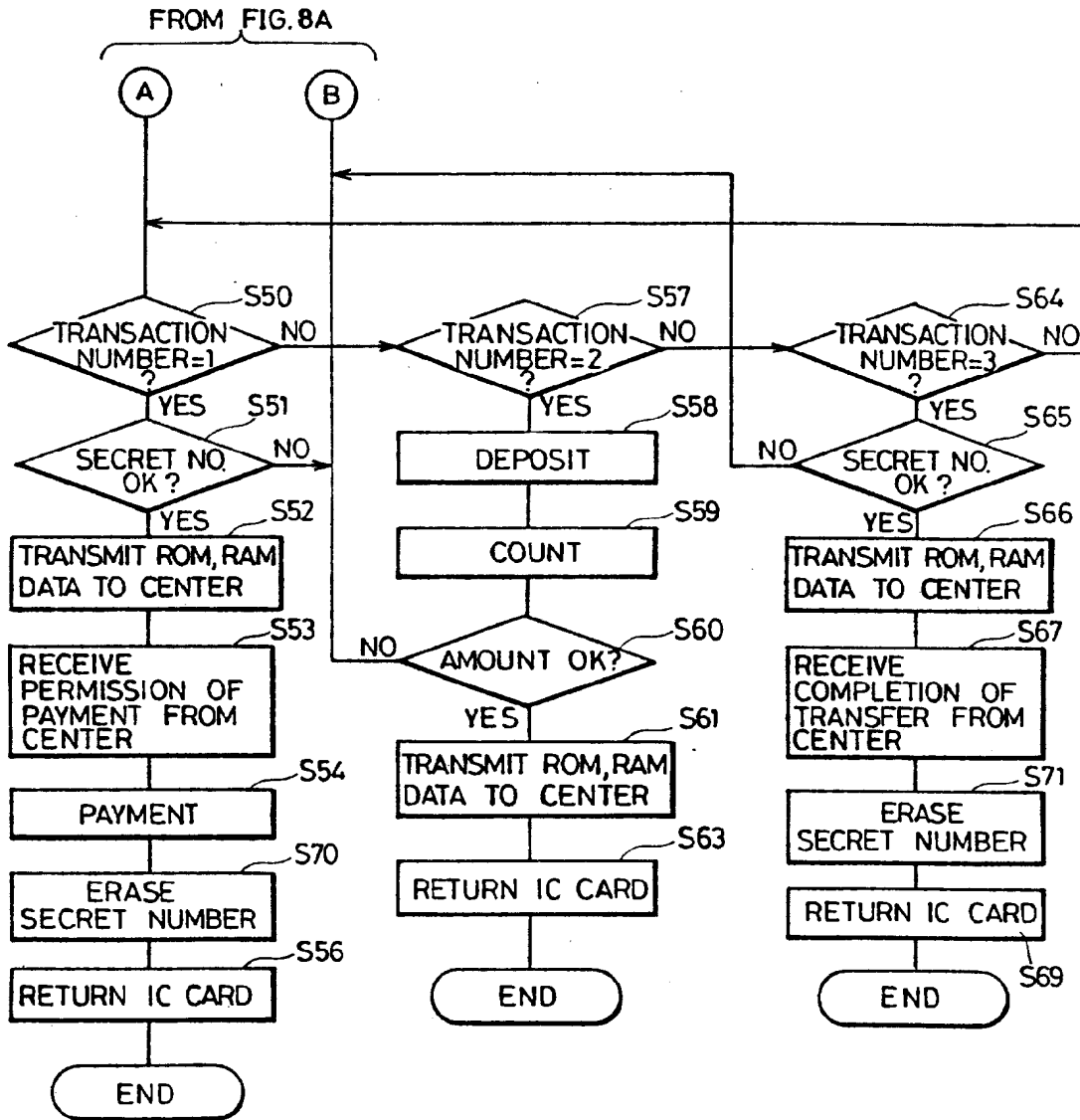


FIG. 10

PROGRAM
ID NUMBER
BANK NUMBER
BRANCH NUMBER
ACCOUNT NUMBER
FIRST EFFECTIVE TIME PERIOD
AREA FOR SECRET NUMBER
DEPOSIT (CREDIT)
PAYMENT
TRANSACTION NUMBER
SECOND EFFECTIVE TIME PERIOD
AREA FOR BANK TO BE TRANSFERRED
AREA FOR ACCOUNT TO BE TRANSFERRED
AREA FOR TRANSFER AMOUNT

STORAGE REGION IN ROM

STORAGE REGION IN RAM

FIG. 12

PROGRAM
ID NUMBER
BANK NUMBER
BRANCH NUMBER
AREA FOR SECRET NUMBER
CHARGED AMOUNT
TRANSACTION NUMBER
SECOND EFFECTIVE TIME PERIOD
AREA FOR BANK TO BE TRANSFERRED
AREA FOR ACCOUNT TO BE TRANSFERRED
AREA FOR TRANSFER AMOUNT
DEPOSIT COUNTER
PAYMENT COUNTER
TRANSMISSION BUFFER
RECEIVING BUFFER
DATE

CONTENTS OF STORAGE OF RAM OF IC CARD

FIG. 11

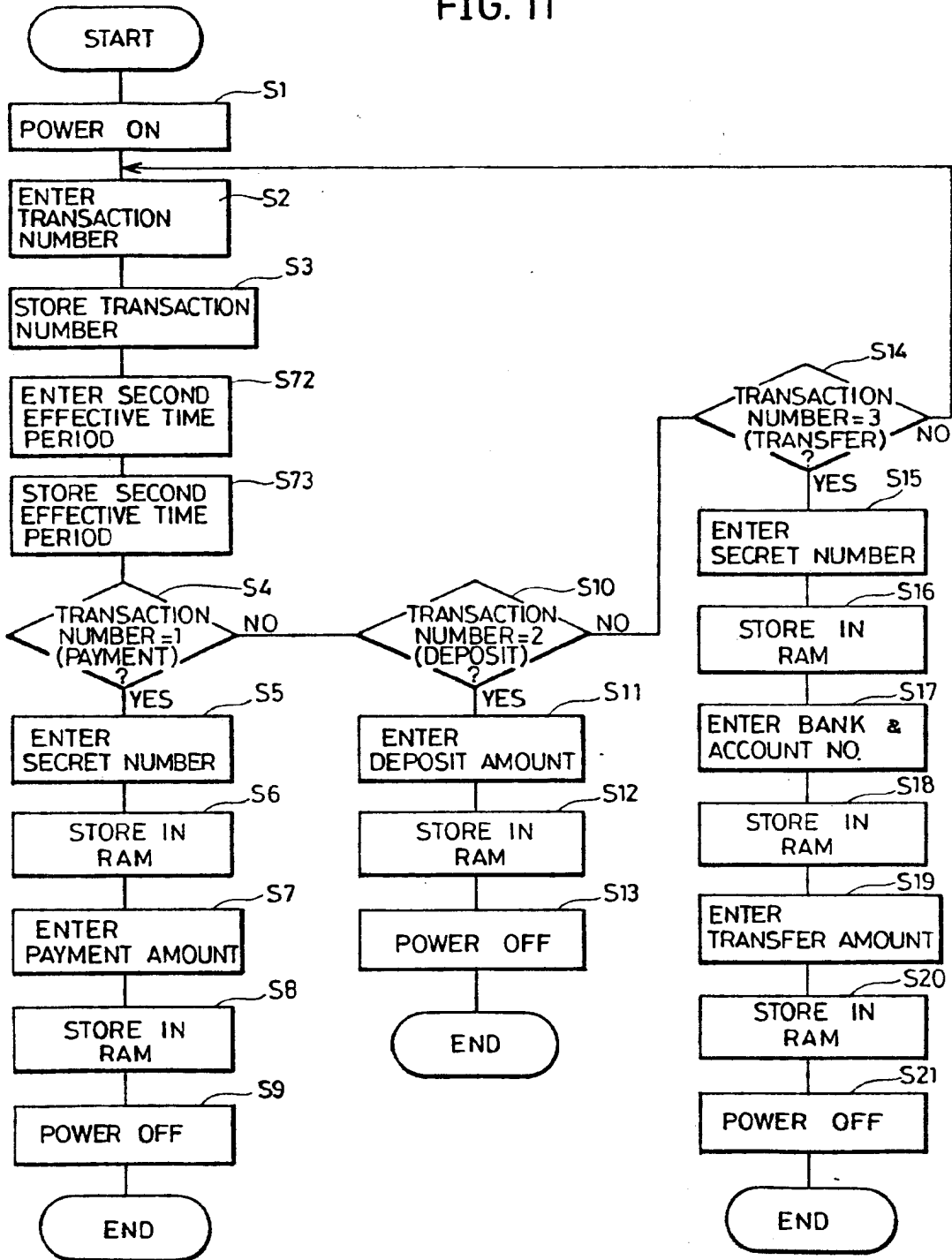
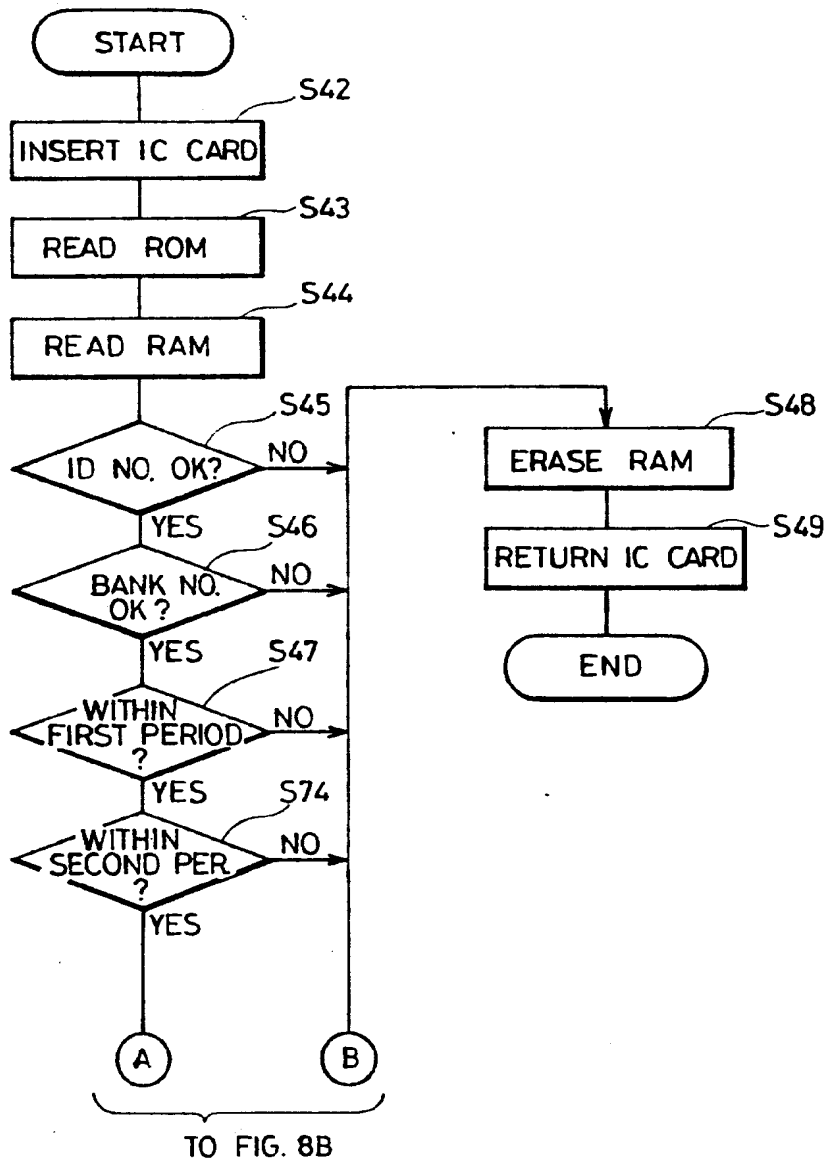


FIG. 13



19



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



11

Publication number:

**0 275 510 B1**

12

**EUROPEAN PATENT SPECIFICATION**

45

Date of publication of patent specification: **21.10.92**

51

Int. Cl.<sup>5</sup>: **G07F 7/10**

21

Application number: **87118815.7**

22

Date of filing: **18.12.87**

54

**Smart card having external programming capability and method of making same.**

30

Priority: **20.01.87 US 4501**

43

Date of publication of application:  
**27.07.88 Bulletin 88/30**

45

Publication of the grant of the patent:  
**21.10.92 Bulletin 92/43**

84

Designated Contracting States:  
**DE FR GB IT**

56

References cited:  
**EP-A- 0 217 281**  
**WO-A-87/05420**  
**US-A- 4 613 937**

73

Proprietor: **International Business Machines Corporation**  
**Old Orchard Road**  
**Armonk, N.Y. 10504(US)**

72

Inventor: **Abraham, Dennis George**  
**5795 Gettysburg Dr.**  
**Concord, NC 28025(US)**  
Inventor: **Double, Glen Paul**  
**8834 High Ridge Lane**  
**Concord, NC 28025(US)**  
Inventor: **Neckyfarow, Steven William**  
**2609 Lawton Bluff Rd.**  
**Matthews, NC 28105(US)**  
Inventor: **Rohland, William Stanley**  
**4234 Rotunda Rd.**  
**Charlotte, NC 28226(US)**  
Inventor: **Tung, Min-Hsiung George**  
**10309 Ben Franklin Ct.**  
**Matthews, NC 28105(US)**

74

Representative: **Herzog, Friedrich Joachim,**  
**Dipl.-Ing. et al**  
**IBM Deutschland GmbH, Patentwesen und**  
**Urheberrecht, Schönaicher Strasse 220**  
**W-7030 Böblingen(DE)**

**EP 0 275 510 B1**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid (Art. 99(1) European patent convention).

## Description

### Background of the Invention

#### Technical Field

The present invention relates to improvements in portable cards carrying processors and memory thereon, of the type referred to in the industry as "smart cards" or "integrated circuit cards" or chip-cards". More particularly, the present invention relates to improvements in the manufacturing process for such cards and the resultant card, whereby the cards are manufactured at least partially "blank" or without application program loaded therein and later customized, or loaded with the appropriate application programs.

#### Background Art

Numerous disclosures of smart cards and systems for using such cards are known in the prior art. These smart card are represented, by way of example by those described in U. S. Patents 3,702,464 to Castrucci and 4,007,355 to Moreno. In such smart cards application programs are stored in read-only-storage within the card, fully and unalterably fixed on the card at the time of initial manufacturing. Such read-only-storage is characterized by the limitation that the application program must be determined and loaded into the smart card upon its initial fabrication (during the manufacturing process). Once the program has been loaded, the slightest change in the program requires that at least the chip, if not the entire card must be scrapped.

This technique of manufacturing smart cards with application programs fixed in unalterable read-only-storage also means that the entire application program development process must precede any smart card manufacturing. This leads to sequential development and manufacturing, meaning a relatively long period from conception of an application program for a smart card until it is available in a completed smart card. As a result, it is necessary to "bread-board" an application program in something other than a smart card itself, and such bread-board may require yet another step in the development process, with an instrument or tool other than the final product. Further, the simulation of the application program may require addition software to allow the simulation, for example, of a terminal for communicating with the bread-boarded application program.

A card having a fixed program and no capability to be changed has an advantageous effect in avoiding certain other limitations and disadvantages, however. For example, if the program is

changeable and fixed into a memory which is initially in a variable state, it may be difficult to determine whether the memory includes an application program loaded in it. A second example of a limitation and disadvantage avoided by a card with a fixed and unchangeable program is that security against unauthorized access and modification to the data is not required in the card having fixed, unchangeable memory.

Smart cards with application programs stored thereon which use rewritable memory for storing transaction information such as the number of failures in identification attempts or an account balance are known. These values require periodic updating and have been used to advantage in past systems. However, none of these systems allow the changing of the application program itself once fixed in the smart card.

In a card having memory which is initially not loaded with any particular program, the memory may initially have a random pattern in it. This makes it difficult (if not impossible) to determine whether or not anything specific has been loaded into the memory such as a desired application program, or whether the random pattern from initialisation of memory by chance appears to be a portion of an application program loaded in it.

Some smart cards presently existing are undesirable in that they usually include multiple integrated circuit elements which must be separately handled and assembled and interconnected. Accordingly, the prior art smart cards are undesirable in having a fixed, unchangeable memory. Further, however, the mere provision of an alterable memory for storing an application program only changes the concerns. Accordingly, the smart cards of the prior art have limitations and disadvantages and do not address the needs of the society who might use, issue and operate with smart cards.

EP-A-0 217 281 discloses a smart card comprising a system controller, a number of ROM memories and an EEPROM alterable memory. The card can communicate with an external terminal device through an input/output terminal I/O. Application software is stored partly in said ROM memories and partly in the alterable memory. More precisely the alterable memory stores secret codes which are necessary for the operation of the card and status data showing whether the card has been completely manufactured, duly issued, or made usable by entering code PIN. A fixed unit address stores a specific address of the alterable memory which is not used. When reading at the specific address is attempted a comparator produces an output which erases the alterable memory thereby preventing illegal access to the data stored therein. This document EP-A-0 217 281 falls under the terms of Article 54(3) and (4) EPC.

The content of this document is not prejudicial to the novelty of the claimed subject-matter. It discloses a smart card with an alterable memory storing data which are part of an application program and which are erased in response to an illegal attempt to read into the alterable memory. The alterable memory furthermore stores status data indicating whether the data of the application program have been loaded therein.

It is the object of the present invention to overcome the limitations and disadvantages of the prior art smart card systems.

#### Summary of the Invention

This and other objects are solved basically by applying the features laid down in the independent claims. In advantageous manner the invention provides an improved smart card and method of making and operating it in which the card includes a variable or reloadable storage element for application programs. As manufactured, the card includes a bootstrap program which includes the necessary instructions for receiving and storing an application program. The application program, once loaded, may be reloaded into the reloadable storage element. In this manner, the application program may be loaded after manufacture, and may be reloaded or changed as desired.

In the preferred embodiment of the present invention, the loading of memory of the smart card with a program is accompanied by the loading of a flag indicating that the application program in fact has been loaded. Thereafter, one can merely test for the flag to determine if the smart card has had an application program loaded therein. This overcomes the limitation of the prior art memories in that the random data during initial manufacture makes it difficult to determine if an application program has been loaded in the card.

The smart card of the present invention includes a security feature to prevent unauthorized tampering with the program loaded therein. This feature prevents the reading of certain portions of memory to prevent hacking. This is accomplished by erasing a portion, for example the first two pages, of memory prior to executing a dump of the memory. In this way, the card remains free for reprogramming, but a hacker who wishes to determine what the initial program and any secret keys stored in the memory is thwarted by having the pages disappear (permanently) prior to reading in an attempt to read those pages. The card is thereafter worthless as a smart card until reloaded by a possessor of the total program. Otherwise, the accessing of that data might allow a person with dishonest intentions to modify the program slightly (to, for example, change his identity or to avoid

logging of his transactions) to evade accountability designed into the system.

The present smart card and method of making and operating it has the advantage that hardware fabrication (namely the manufacture of cards without application programs loaded thereon) can be occurring while the software is being developed. Thus, the rather long development process of a smart card with an application program loaded thereon can be accomplished in a shorter time by allowing parallel development of the software. Further, the fact that the application program is reloadable or changeable upon desire means that the smart card manufacturer will no longer be required to predict how many of a particular application program will be required. A large quantity of "blank" cards can be fabricated in advance, then loaded with the desired application program.

The fact that the application program is developed and loaded after manufacture has several other advantages. The issuer of a smart card (for example, a bank) no longer must divulge the details of his security plan, floor limits for credit or other sensitive details to the manufacturer of the smart cards. All of these features can be loaded by the bank itself into a blank smart card later. Further, the bank who has not included a feature in its cards, either through oversight or through changing market requirements, can simply modify the application program which it is loading and have a smart card with an improved application program.

While in one embodiment of the present invention, the smart card of the present invention may be manufactured using integrated circuits of conventional design, an alternate embodiment of the present invention envisions the use of a single custom integrated circuit to be used, avoiding interconnection between various integrated circuits as well as the separate mountings necessary to the base of the credit card itself. While the use of conventional design integrated circuit allows low volumes of smart cards to be manufactured quickly and inexpensively, the savings in assembly occur by the use of a single integrated circuit.

Other objects and advantages of the present invention will be apparent to those skilled in the art in view of the following description of the preferred embodiment, taken together with the appended claims and the accompanying drawings.

#### Brief Description of the Drawings

Figure 1 is a block diagram view of the smart card of the present invention.

Figure 2 is a block diagram view of the method of loading a smart card with an application program on the smart card.



### Best Mode of Carrying out the Invention

Figure 1 depicts a smart card 10 which includes an instruction processor 12, a read-only-store or memory 14 and changeable memory 16. Input/output (I/O) lines 18 are connected to the instruction processor 12 for communication between the card 10 and the external world (external communication). Communication lines 20 interconnect the instruction processor 12, the read-only-store 14 and the changeable memory 16 for internal communication between portions of the card 10. A portion of the changeable memory 16 has been identified as a flag 22.

The smart card 10 is, in its preferred embodiment, the size of a standard credit card and meets the recognized standards established by ISO for credit cards. Although it is not shown, it may include a magnetic stripe, again of a type meeting the appropriate commercial standard for storing information for use in magnetic stripe communication applications, all of which are well known. Other indicia may be added to the card as desired in the way of security markings, issuer, customers' name and account number as may be desired by the particular application, so long as the essential functioning of the smart card is not impaired.

The instruction processor 12 is a conventional microprocessor of a type which is well known and commercially available. For the present application, a Model 8051 from Intel is well suited, although other processors could also be used to advantage.

The read-only-storage 14 is a fixed read-only-memory which includes a bootstrap program fixed therein at the time of manufacture. This bootstrap program includes the basic instruction repertoire and instructions for loading an application program into the alterable memory 16. Although any one of numerous read-only-storage devices could be used to advantage in the present design, a 8051 microprocessor from Intel includes a read-only-memory in it, obviating the need for a separate read-only-memory.

The alterable memory 16 is used as a storage for the application program. In its preferred embodiment, this is an electrically erasable read-only-memory (EEPROM), although other non-volatile memories could be used to advantage. The present invention uses a Model 9864A EEPROM made by American Micro-Devices, although similar devices could be used in its place.

The alterable memory 16 contains the application program as well as other information which, although non-public, may be changeable, such as encryption keys or personal verification data. These application programs are those algorithms or other procedures which the smart card undertakes during its operation and which could vary from one ap-

plication for a smart card to the next application for a smart card. These application programs include techniques for communication between the smart card and the external world, for example, with an automatic teller machine for conducting a banking transaction. Other application programs might conduct necessary security and identification processes, conduct the actual transaction desired, and/or make a record on the smart card in the form of a log entry of the transaction.

In the nature of security or identification application programs, there is a necessity for the smart card and the terminal to mutually conduct device authentication. That is, each must make sure that the other is a legitimate device, and not merely a decoy whose mission is to obtain information leading to penetration of the overall system. In this regard, a system of challenges and passwords which avoids the disclosure of meaningful information to a decoy is disclosed in co-pending patent application EP-86114963.1 (EP-A-0 223 122). That patent is specifically incorporated by reference as disclosing one such application program which might be loaded into the alterable memory 16. In general, other application programs which had been fixed in smart cards having a fixed memory are also suitable for use in the smart cards of the present invention in which the application program is loadable after manufacture of the card and reloadable if it is desired to change the application program.

The application programs also could be used to conduct user identification. This differs from the device authentication discussed in the previous paragraph, and would generally be conducted following such authentication. The purpose of such user identification is to insure that the person who is conducting the transaction or doing the other business using the smart card is identified. In the context of an automatic teller transaction such as banks presently use, this user authentication may be by way of entry of a personal identification number (PIN) into the automatic teller machine keyboard. The card then compares the entered number with a stored or calculated value to determine if the user has entered a correct PIN number.

Other forms of user identification could also be employed in application programs such as potentially more accurate and less deceivable forms of positive personal verification, such as fingerprint analysis or signature dynamics. Such improved forms of positive personal verification are presently known and could be implemented by suitable application programs.

Of course, application programs for formatting data for communication with the outside world through the I/O lines 18 is also a necessary application program. The data must be presented in a

format which the recipient device (such as the automatic teller machine previously mentioned) can recognize the data and use it. Other application programs would include the details of conducting the transaction or other business for which the smart card has been designed -- the useful business which is the whole reason for being of the smart card. Such could be a cash withdrawal at the automatic teller machine, use in funds transfer, or an electronic funds transfer device in a point of sale environment, where money from the consumers account is transferred to a merchant's account as a result of a consumer purchase, carried out at a machine in the merchant's store and coupled electronically to a bank or clearing house. Finally, since the smart card includes memory which is alterable and writable, a written record of the transaction may be logged on the smart card itself via an application program -- so the user can't forget the transaction and claim that a mistake had been made.

The I/O lines 18 connect the instruction processor to the outside world. This outside world may be an automatic teller machine in which the card has been inserted, or other suitable device for communication. In the typical smart card system existing today, these I/O line 18 terminate in a plurality of electrical contacts arranged on the surface of the smart card in a circular pattern set forth in a recognized standard at predetermined locations and spacings. The terminal then has complementary contacts arranged to physically contact the I/O lines 18 to transmit data therebetween in accordance with a predetermined standard. Other forms of coupling (even non-contact coupling) could be used to advantage, so long as the card communicates. Typically, this communication is serial communication in which data is transmitted sequentially.

For the initial loading of programs, the I/O lines 18 are coupled to receive the application program from a mainframe processor wherein the instructions are downloaded sequentially and stored in series in the alterable memory 16 in the order in which they are received. Alternately, the instructions may be downloaded from the other processor by specifying the address in the alterable memory in which each instruction is to be loaded. Either technique can be used, and depending on the amount of data and storage pattern, and whether the memory is being fully overwritten and replaced or only selectively overwritten, one technique may be desirable over the other technique.

While the present embodiment has been described in terms of a command processor 12, a read-only-store 14 and an alterable memory 16 in one embodiment and using conventional, commercially available components, a design in which all

components are on a single chip is commercially feasible. While this is expected to be the preferred embodiment chosen by many designers, it would involve a custom designed chip. While that is clearly within the skill of today's circuit designers, the use of multiple commercially available components is believed desirable in many instances.

Figure 2 illustrates a method of downloading the application program for the present system of making a smart card with a reloadable or changeable application program. As shown in this figure, the card 10 is separate from the development of the application program which occurs in a mainframe processor 50. The application program is written, compiled (if necessary), debugged and tested in the mainframe processor 50. The application program 52 is created as a result. The application server program 54 then serves to load and verify that the application program 52 is loaded onto the smart card 10.

The card 10, which includes, as a part of its bootstrap program, the software necessary to accomplish the functions described in this Figure 2, responds to a load signal (which is, in essence a double reset as described below) on line 60. This signal on line 60 is handled first by a discriminator 62 which differentiates between load instructions and execute instructions. The execute instructions proceed to block 64 (where they are executed) and load instructions proceed to block 66. At the block 66, a load instruction is subject to secure storage supervision which guarantees that the secret pages have been previously erased and that the program remains in a load state. From block 66, control then proceeds to block 68 which is a status reporting function. When each step has been accomplished correctly and the card is ready for additional data, the status reporting function sends a signal to the application server program 54 on line 70. In response to that signal on line 70, the application server program 54 then sends an additional instruction or portion of the application program on line 72 to a command interpreter 74. All commands are passed with a length and "checksum" value to insure that data is not lost in transmission. The checksum calculation is a counting of the ones in the data being transmitted which, together with the length information, functions to insure that the information passed has not changed during the passing. The command interpreter 74 then proceeds to perform one of the functions illustrated by five boxes 74a, 74b, 74c, 74d, 74e, representing the functions of testing the page, initialize loading, loading data, verifying a page or end of loading, respectively, depending on the instruction from the application server program 54. The function of testing the page in the block 74a is a check of a particular page of data in the EEPROM memory 16

by writing and reading data to each byte of data on the page, in essence a memory check. The function of initialize loading in the block 74b sets the EEPROM type, the address for the first byte of data and the byte count before the next load initialization. The function of loading data in the block 74c is the transfer of one byte of data from the application server program 54 to the alterable memory 16 of the card. The function of verifying a page in the block 74d is an internal generation of a checksum for the indicated page, which checksum is then passed to the application server program 54 for verification that the entire page has been transferred correctly. The step of end of loading in the block 74e sets a lockswitch bit in the card to inhibit further load commands (such further load commands being a possible indicating of tampering or improper adjustment of the program or its data. The double reset sequence of a load command as described below must then be followed to load any further application program after the lockswitch has been set.

The "Load" function on the card is invoked by a timed double reset sequence on reset line 60. In a newly created card, that is, a card manufactured without an application program stored thereon, it is impossible to predict the state of any bit in the application program storage 16 or the flag 22. It is therefore desirable in some instances to know whether an application program has been loaded onto the card, or whether this is a new card having no application program and therefore requiring one. This time double reset sequence accomplishes this, and resolve any uncertainty or ambiguity of whether an application program has been loaded.

When the reset line 60 is activated, the instruction processor 12 proceeds to a section of instructions designed to prevent any ambiguity as to whether a program has been loaded. The first step in response to a load instruction is to test a predetermined portion of the application program storage 16 for a predetermined sequence. If that sequence is not found, the load instruction then writes that predetermined sequence in the predetermined portion of the application program storage. A time is also set then to erase the predetermined sequence from the predetermined portion after a fixed time interval. If a program load is to occur, a second activation on the reset line 60 must occur before the end of the fixed time interval after the writing of the predetermined sequence. Now the test for the predetermined sequence in the predetermined portion of the application program storage 16 is successful (because it had been just written there by the first reset and not yet erased). This presence of the sequence indicates that this is the second reset, or the signal that a program load is desired. As a result of the program

load, a first result is that the predetermined sequence in the predetermined portion of storage is erased. A second result is the overwriting of selected pages of memory, for example, pages 0 and 1 of the application program storage. This overwriting effectively erases all the sensitive information from a previous program, for example, encryption keys or personal identification information that could be useful in defeating system security.

Of course, the predetermined sequence which is written must be large enough to insure against accidentally having that sequence appear unless it has just been written as a result of a first reset. Otherwise, the double reset will not be effective as the indicator for program loading. That is, if the predetermined sequence may appear in the predetermined portion without having been written there by a first reset, then a program load will be improperly attempted in response to the first reset signal. Further, if that predetermined sequence appears other than through the reset function (which erases the sequence the fixed time interval later), then the predetermined sequence may not be erased. In short, the predetermined sequence must happen only through the first reset in order for this timed double reset to signify a program loading.

Of course, many alternatives to the preferred mode of carrying out the present invention are apparent to those skilled in the art of smart card design and manufacture, and furthermore, some features of the present invention may be used without the corresponding use of other features described in this description. For example, the use of flags to indicate the presence or absence of a loaded application program is a convenience for those handling such cards; its absence may require more effort to determine whether an application program has been loaded, but the entire contents of the card could be compared to the possible application programs to determine whether a match exists, indicating that a program was loaded.

While the description of the preferred embodiment indicates that the card includes an application program, more than one application program can be loaded into a card, limited only by the size of the programs relative relative to the memory available. Thus, a single card could concurrently include multiple application programs, selected by an external input. The described technique for loading an application program is desirable, although other techniques might be used to advantage. Further, those skilled in the relevant arts will know that certain features, such as the method of creating and downloading application programs, can be changed from that described in the foregoing description of the preferred embodiment.

## Claims

1. A method for fabricating and operating a portable card (10) having a changeable memory (16), a processor (12) and means (18) for communicating with an external terminal device, comprising:
  - mounting a changeable memory (16), a processor (12) and communication means (18) on a card, said memory (16) being without an application program at the time of mounting;
  - connecting the processor (12) to the memory (16) and the communication means (18) to fabricate a smart card without an application program;
  - after the smart card has been assembled and the processor (12), memory (16) and communication means (18) have been connected, loading an application program into the memory by coupling the card to an external processor (50) and downloading an application program from the external processor (50) to the memory (16) of the smart card, and erasing a portion of the memory (16) of the smart card in response to an attempt to read out that portion of the memory.
2. The method of Claim 1 wherein at least portions of the application program are sequentially loaded through the instruction processor (12) of said card.
3. The method of Claim 1 or 2 wherein the loading step includes responding to a reset signal by testing the memory (16) for preset information and loading the application program only if the preset information is present, writing preset information on the card for a fixed interval if the preset information is not present, then removing the preset information if a second reset signal has not been received before the end of the fixed interval, whereby an application program may be loaded into the changeable memory (16) only in response to two reset signals being received within the fixed interval.
4. The method of one of the Claims 1 - 3 wherein the method further includes the step of replacing an existing application program in a programmed smart card with a second application program.
5. A portable card (10) which selectively can be coupled to an external device (50) for receiving and transmitting information therobetween, said card comprising:
  - a base having approximately the dimension of a standard credit card and including contacts (18) for selectively coupling the card to the

- external device;
  - a command processor (12) mounted to the base and electrically coupled to the contacts, said command processor including means for coupling the command processor to an external terminal device;
  - a changeable memory (16);
  - a non-volatile memory (14) coupled to the command processor including data for loading an application program from the external terminal device into the changeable memory, whereby the portable card may be manufactured without an application program and the application program may be generated externally of the smart card and loaded into the changeable memory after the card is manufactured; and
  - including means for erasing a portion of the changeable memory (16) in response to an attempt to read a portion of the memory (16) externally, whereby an attempt to alter the application program may be prevented.
6. The card of Claim 5 card further including means (22) for indicating whether an application program has been loaded therein, said means including at least a first state when no application program has been loaded thereon and a second state when an application program is present.
  7. The card of Claim 5 or 6 wherein the command processor (12) and the non-volatile memory (14) are included in a single integrated circuit carried on the base of the portable card.
  8. The card of one of the Claims 5 - 7 wherein the changeable memory (16) includes a memory portion which receives and stores for a predetermined time period a predetermined sequence when a first reset signal is applied to the card and means for loading an application program in response to the application of a second reset signal to the card testing for the predetermined sequence.

#### Patentansprüche

1. Verfahren zur Herstellung und zum Betrieb einer tragbaren Karte (10) mit einem veränderbaren Speicher (16), einem Prozessor (12) und Mitteln (18) zur Datenübertragung an eine externe Station, folgendes umfassend:
  - Montage eines veränderbaren Speichers (16), eines Prozessors (12) und Datenübertragungsmitteln (18) auf einer Karte, wobei der Speicher zum Montagezeitpunkt kein Anwendungs-

- programm enthält;  
Anschluß des Prozessors (12) am Speicher (16) und der Datenübertragungsmittel (18) zur Herstellung einer intelligenten Karte ohne Anwendungsprogramm;  
nach Montage der intelligenten Karte und Anschluß des Prozessors (12), des Speichers (16) sowie der Datenübertragungsmittel (18) Laden des Anwendungsprogramms im Speicher durch Verbinden der Karte mit einem externen Prozessor (50) und Herunterladen eines Anwendungsprogramms aus dem externen Prozessor (50) in den Speicher (16) der intelligenten Karte sowie  
Löschen eines Teils des Speichers (16) der intelligenten Karte bei einem Ausleseversuch dieses Speicherteils.
2. Verfahren nach Anspruch 1, bei dem mindestens Teile des Anwendungsprogramms sequentiell durch den Anweisungsprozessor (12) der Karte geladen werden.
3. Verfahren nach Anspruch 1 oder 2, bei dem im Ladeschritt aufgrund eines Rücksetzsignals der Speicher (16) auf eingestellte Informationen getestet wird und das Anwendungsprogramm nur dann geladen wird, wenn die eingestellten Informationen vorhanden sind, eingestellte Informationen auf der Karte während einem festen Intervall eingeschrieben werden, wenn die eingestellten Informationen nicht vorhanden sind, und die eingestellten Informationen dann entfernt werden, wenn vor Ende des festen Intervalls kein zweites Rücksetzsignal empfangen wird, so daß ein Anwendungsprogramm in den veränderbaren Speicher (16) lediglich aufgrund des Empfangs zweier Rücksetzsignale innerhalb des festen Intervalls geladen werden kann.
4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem das Verfahren außerdem den Schritt umfaßt, daß ein vorhandenes Anwendungsprogramm in einer programmierten intelligenten Karte durch ein zweites Anwendungsprogramm ersetzt wird.
5. Tragbare Karte (10), die selektiv mit einer externen Station (50) zum Empfang und zur Übertragung von Informationen gekoppelt werden kann, folgendes umfassend:  
eine Basis mit ungefähr der Abmessung einer Standardkreditkarte und Kontakten (18) zum selektiven Koppeln der Karte mit der externen Station;  
einen auf der Basis angeordneten Befehlsprozessor (12), der elektrisch mit den Kontakten

- gekoppelt ist, wobei der Befehlsprozessor Mittel zum Koppeln des Befehlsprozessors an eine externe Station aufweist:  
einen veränderbaren Speicher (16);  
einen Festspeicher (14), der mit dem Befehlsprozessor gekoppelt ist und Daten enthält zum Laden eines Anwendungsprogramms aus der externen Station in den veränderbaren Speicher, wobei die tragbare Karte ohne Anwendungsprogramm hergestellt werden und das Anwendungsprogramm außerhalb der intelligenten Karte erzeugt und nach Fertigstellung der Karte in den veränderbaren Speicher geladen werden kann; sowie  
Mittel zum Löschen eines Teils des veränderbaren Speichers (16) aufgrund eines externen Leseversuchs eines Teils des Speichers (16), wodurch ein Änderungsversuch des Anwendungsprogramms verhinderbar ist.
6. Karte nach Anspruch 5, die außerdem Mittel (22) enthält, die anzeigen, ob auf derselben ein Anwendungsprogramm geladen ist, wobei besagte Mittel mindestens einen ersten Zustand aufweisen, in dem kein Anwendungsprogramm geladen ist und einen zweiten Zustand, in dem ein Anwendungsprogramm vorhanden ist.
7. Karte nach Anspruch 5 oder 6, bei der der Befehlsprozessor (12) und der Festspeicher (14) in einer einzigen integrierten Schaltkarte auf der Basis der tragbaren Karte enthalten sind.
8. Karte nach einem der Ansprüche 5 bis 7, bei der der veränderbare Speicher (16) ein Speicherteil umfaßt, welcher eine bestimmte Sequenz für eine bestimmte Zeitspanne empfängt und speichert, wenn die Karte mit einem ersten Rücksetzsignal beaufschlagt wird, sowie Mittel zum Laden eines Anwendungsprogramms bei Beaufschlagung der Karte mit einem zweiten Rücksetzsignal, um während der vorbestimmten Sequenz zu testen.

#### Revendications

1. Méthode de fabrication et d'exploitation d'une carte portable (10) ayant une mémoire modifiable (16), un processeur (12) et un moyen (18) pour communiquer avec un dispositif terminal externe, comprenant:  
le montage d'une mémoire modifiable (16), d'un processeur (12) et d'un moyen de communication (18) sur une carte, ladite mémoire (16) n'ayant pas de programme d'application au moment du montage;  
la connexion du processeur (12) à la mé-

- moire (16) et au moyen de communication (18) pour fabriquer une carte à circuit intégré sans programme d'application;
- une fois la carte à circuit intégré assemblée et le processeur (12), la mémoire (16) et le moyen de communication (18) connectés, le chargement d'un programme d'application dans la mémoire en couplant la carte à un processeur externe (50) et en téléchargeant un programme d'application depuis le processeur externe (50) jusque sur la mémoire (16) de la carte à circuit intégré, et
- l'effacement d'une portion de la mémoire (16) de la carte à circuit intégré en réponse à une tentative de lecture de cette portion dans la mémoire.
2. Méthode selon la revendication 1, dans laquelle au moins des portions du programme d'application sont successivement chargées par le processeur d'instructions (12) de ladite carte. 20
  3. Méthode selon les revendications 1 ou 2, dans laquelle l'étape de chargement comprend la réponse à un signal de restauration en testant la mémoire pour des informations pré-définies, et le chargement du programme d'application uniquement si les informations pré-définies sont présentes, l'écriture des informations pré-définies sur la carte pendant un intervalle fixe si les informations pré-définies ne sont pas présentes, puis suppression des informations pré-définies si un deuxième signal de restauration n'a pas été reçu avant la fin de l'intervalle fixe, ce qui fait qu'un programme d'application ne peut être chargé dans la mémoire modifiable (16) qu'en réponse à deux signaux de restauration alors reçus dans l'intervalle fixe. 30
  4. Méthode selon l'une quelconque des revendications 1 à 3, dans laquelle la méthode comprend en outre l'étape qui consiste à remplacer un programme d'application existant dans une carte à circuit intégré programmée par un deuxième programme d'application. 40
  5. Carte portable (10) qui peut être sélectivement couplée à un dispositif externe (50) pour la réception et la transmission d'informations entre eux, la dite carte comprenant: 50
    - une base ayant approximativement la dimension d'une carte de crédit standard et comportant des contacts (18) pour coupler sélectivement la carte au dispositif externe,
    - un processeur de commandes (12) monté sur la base et électriquement couplé aux contacts, ledit processeur de commandes comprenant des moyens pour coupler le pro-
- cesseur de commandes à un dispositif terminal externe,
- une mémoire modifiable (16),
  - une mémoire permanente (14) couplée au processeur de commandes comprenant des données pour charger un programme d'application depuis le dispositif terminal externe jusque dans la mémoire modifiable, ce qui fait que la carte portable peut être fabriquée sans programme d'application et que le programme d'application peut être engendré hors de la carte à circuit intégré et chargé dans la mémoire modifiable une fois la carte fabriquée, et
  - comprenant des moyens pour effacer une portion de la mémoire modifiable (16) en réponse à une tentative de lecture d'une portion de la mémoire (16) de façon externe, ce qui fait que toute tentative de changement du programme d'application peut être empêchée.
6. Carte selon la revendication 5, comprenant en outre des moyens (22) pour indiquer si un programme d'application y a été chargé, lesdits moyens ayant au moins un premier état lorsqu'il n'est chargé aucun programme d'application, et un deuxième état lorsqu'un programme d'application est présent.
  7. Carte selon les revendications 5 ou 6, dans laquelle le processeur de commandes (12) et la mémoire permanente (14) sont inclus dans un seul circuit intégré porté sur la base de la carte portable.
  8. Carte selon l'une quelconque des revendications 5-7, dans laquelle la mémoire modifiable (16) comprend une portion de mémoire qui reçoit et emmagasine pendant une période de temps prédéterminée une séquence prédéterminée lorsqu'un premier signal de restauration est appliqué à la carte, et des moyens pour charger un programme d'application en réponse à l'application sur la carte d'un deuxième signal de restauration pour le test de la séquence prédéterminée.

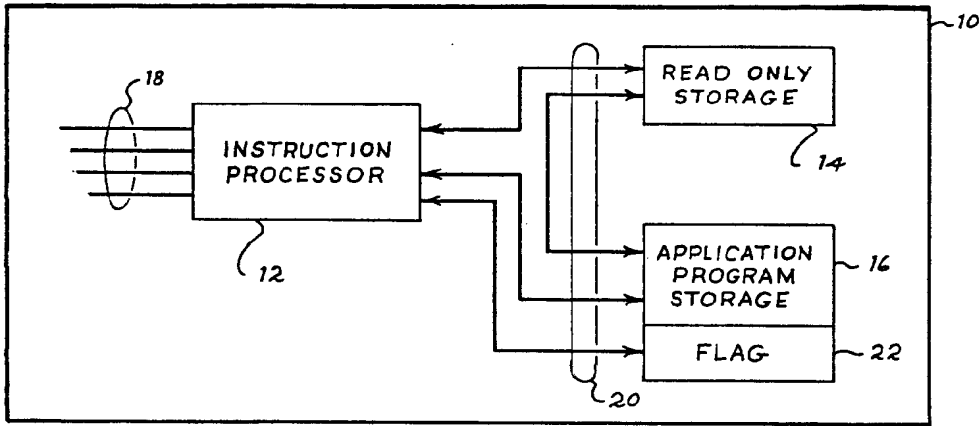


Fig. 1

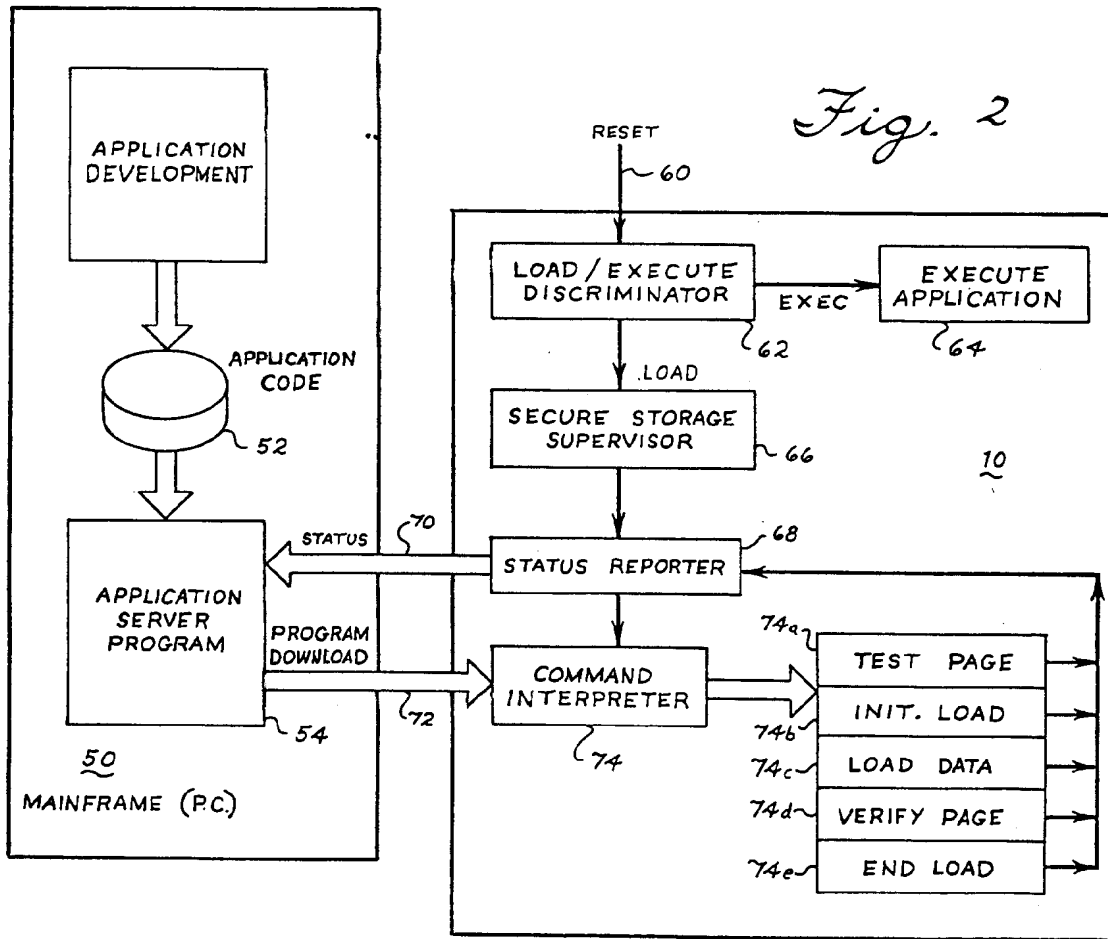
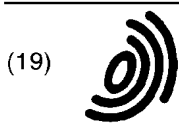


Fig. 2



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) **EP 0 328 289 B2**

(12) **NEW EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention  
of the opposition decision:  
**04.03.1998 Bulletin 1998/10**

(51) Int Cl.<sup>6</sup>: **G07F 7/10**

(45) Mention of the grant of the patent:  
**18.05.1994 Bulletin 1994/20**

(21) Application number: **89300933.2**

(22) Date of filing: **31.01.1989**

(54) **IC card and method of writing its operation program**

Chipkarte und Verfahren zum Einschreiben seines Arbeitsprogramms

Carte à circuit intégré et méthode d'inscription de son programme d'opération

(84) Designated Contracting States:  
**DE FR GB**

(74) Representative: **Senior, Alan Murray et al**  
**J.A. KEMP & CO.,**  
**14 South Square,**  
**Gray's Inn**  
**London WC1R 5LX (GB)**

(30) Priority: **03.02.1988 JP 21919/88**  
**11.01.1989 JP 2899/89**

(43) Date of publication of application:  
**16.08.1989 Bulletin 1989/33**

(56) References cited:  
**EP-A- 0 217 654** **WO-A-87/05420**  
**FR-A- 2 591 008**

(73) Proprietor: **Hitachi Maxell Ltd.**  
**Osaka-fu (JP)**

- **PATENT ABSTRACTS OF JAPAN** vol. 11, no. 42  
(P-545)(2489) 06 February 1987 ; & JP-A-61 211  
788
- **"Keine Angst für UNIX: Ein Lehrbuch für**  
**Einsteiger"**, Duesseldorf 1987, VDI-Verlag

(72) Inventor: **Shinagawa, Toru**  
**Toride-shi (JP)**

**EP 0 328 289 B2**



**Description****BACKGROUND OF THE INVENTION**

This invention relates to an IC card and a method of writing its operation program. More particularly, this invention relates to an IC card in which its operation program cannot be altered by any person or party except an authorized one and relates also to a method of writing the operation program in the IC card.

IC cards are now being put into practical use in various systems including credit systems for the sales and purchases of commodities, cash payment/deposit systems in banks, and debt payment systems in hospitals, company employees' restaurants, etc. In such systems, an illicit use of the IC card is a serious problem.

Commonly, the IC card has a microprocessor and a memory built in it. Also, the IC card includes a built-in interface for data transmission and reception between it and an external apparatus such as a host computer or an IC card reader/writer. The IC card is used in a state connected to the host computer or loaded on the IC card reader/writer. The operation sequence for transmission and reception of data between the IC card and the external apparatus includes the steps of decoding a command group, transmitted from the external apparatus, by an internal control program of the IC card, executing necessary memory access, for example, data writing, reading or erasing according to an operation program stored in the memory of the IC card, and transmitting the result of the memory access to the external apparatus as a response to the command group.

Programs stored in the IC card include a program pertinent to the control operation of the built-in microprocessor itself and a program for controlling the fundamental internal circuit of the IC card. Besides these programs, there are operation programs a suitable one of which is selected so that the microprocessor can execute a specific processing procedure corresponding to a specific function. Such operation programs include a test program and various application programs.

Generally, the former programs are mostly prepared together with the built-in microprocessor and stored in, for example, a mask ROM. Therefore, these programs are not easily rewritable or alterable. On the other hand, the latter programs or operation programs are down-loaded later to the memory from, for example, the host computer. Therefore, these operation programs are alterable.

An IC card in which its operation program is down-loaded later is disclosed in, for example, JP-A-61-211788. In the disclosed IC card, an electrically erasable non-volatile memory or the like is used as a program storage part storing an operation program so that the operation program is alterable. However, in such an IC card, the operation program stored in the IC card may be illicitly altered by rewriting, and there is the fear of illicit use of the altered IC card.

**Summary of the Invention**

With a view to obviating the defect of the prior art IC card, that its operation program is easily alterable, it is an object of the present invention to provide an IC card in which its operation program cannot be easily altered so as to prevent its illicit use and in which the secrecy of its operation program can be secured.

Another object of the present invention is to provide an IC card in which an operation program written by down-loading cannot be altered by any person or party except an authorised one.

Still another object of the present invention is to provide a method of writing an operation program in an IC card so as to attain the above objects.

FR-A-2,591,008 and US-A-4,887,234 disclose an IC card comprising memory means for storing data which is alterable, and processor means for executing a predetermined sequence of processing steps according to a control program, wherein said memory means stores alterability/non-alterability information indicating whether respective data files are alterable or non-alterable, and said IC card comprises means for executing alteration of said operation programs when said operation program alterability/non-alterability information indicates that a respective data file is alterable.

WO-A-87/05420 discloses an IC card comprising memory means for storing data which is alterable, and processor means for executing a predetermined sequence of processing steps according to a control program, wherein said memory means stores alterability/non-alterability information indicating whether respective data fields are alterable or non-alterable, and said IC card comprises means for executing alteration of said operation programs when said operation program alterability/non-alterability information indicates that a respective data field is alterable.

WO-A-87/07063 discloses an IC card comprising memory means for storing data which is alterable, and processor means for executing a predetermined sequence of processing steps according to an executive operating system, wherein said memory means stores alterability/non-alterability information indicating whether respective data files are alterable or non-alterable, said IC card comprises means for executing alteration of said operation programs when said operation program alterability/non-alterability information indicates that a respective data file is alterable, and the card uses an optional password which the user must enter before gaining access to and being able to alter a file.

The present invention, as defined in claim 1, provides means for permitting change-over of an operation program alterability/non-alterability information stored in the IC card memory between the alterable and non-alterable modes by detecting coincidence between collation information and externally applied input information.

A method of utilising the IC card to make use of the

invention is defined in claim 10.

The present invention is featured by the fact that, at the time of writing an operation program in an IC card, identification information and attribute information of the operation program are written in the IC card, while at the time of altering the operation program, the attribute information is referenced to permit alteration only when the operation program is alterable, thereby improving the security of secrecy during writing the operation program in the IC card. Further, at the time of alteration of the attribute information, the identification information is collated with externally applied input information so as to detect coincidence therebetween, and, when the coincidence is detected, and the attribute information is to be altered, any person or party except a specifically limited or authorized one is not permitted to execute the alteration of the attribute information.

The IC card of the present invention which attains the above objects comprises a memory for storing operation program alterability non-alterability information indicating whether or not an operation program can be altered and collation information referenced to permit change-over of the operation program alterability/non-alterability information between an alterable mode and a non-alterable mode, means for changing over the operation program alterability/non-alterability information to one of the alterable mode and the non-alterable mode by detecting coincidence between the collation information and externally applied input information, and means for executing alteration of the operation program when the operation program alterability/non-alterability information is in the alterable mode.

Thus, according to the IC card of the present invention, operation program alterability/non-alterability information and collation information are stored in the IC card. In the IC card, the operation program alterability/non-alterability information is referenced to decide whether an operation program is alterable or non-alterable, and, when the collation information coincides with externally applied input information, alteration of the operation program by an authorized person or party is permitted. Therefore, the security of secrecy of the operation program of the IC card or of the alteration of the operation program can be improved, and illicit alteration of the operation program can be prevented.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of an IC card which is not an embodiment of the present invention but is useful for understanding.

Fig. 2 is a flow chart showing a sequence of steps for writing an operation program in the IC card shown in Fig. 1.

Fig. 3 is a flow chart showing a sequence of steps for writing identification information and attribute information in the IC card shown in Fig. 1.

Figs. 4A and 4B show examples of combinations of

the identification information and the attribute information stored in the IC card shown in Fig. 1.

Fig. 5 is a block diagram of an embodiment of the IC card according to the present invention.

Fig. 6 is a flow chart showing a sequence of steps for writing a plurality of operation programs in the IC card shown in Fig. 5.

Fig 7 is a flow chart showing a sequence of steps for writing identification information and attribute information in the IC card shown in Fig. 5.

Figs. 8A to 8M show examples of combinations of the identification information, attribute information and various programs stored in the program storage part of the IC card shown in Fig. 5.

An IC card which is not an embodiment of the present invention but is useful for understanding will now be described in detail with reference to Figs. 1, 5 and 9 of the drawings. Referring to each of Figs. 1, 5 and 9, the IC card generally designated by the reference numeral 1 comprises a program storage part 4, an information memory part 5, a central processor unit (CPU) 6 and an information input/output part 7. The IC card 1 is mounted on or connected to an external apparatus 8 (which is, for example, an IC card reader/writer or a host computer) and starts to operate in response to a signal applied from the external apparatus 8. The operation of the IC card 1 is determined by an internally stored operation program or an operation program down-loaded and stored in the program storage part 4, and the CPU 6 activates such an operation program. The CPU 6 executes transmission and reception of information between the IC card 1 and the external apparatus 8 (for example, the IC card reader/writer or the host computer) through the information input/output part 7, writing information in the information memory part 5 and program storage part 4, and reading information out of the information memory part 5 and program storage part 4.

The program storage part 4 and the information memory part 5 of the IC card 1 are each in the form of an alterable non-volatile memory such as an EEPROM (an electrically erasable and programmable ROM). The program storage part 4 includes an attribute information storage region 2 storing attribute information of an operation program, an identification information storage region 3 storing identification information of the operation program and an operation program storage region 9.

The contents of the IC card shown in Fig. 1 will first be described.

In the attribute information storage region 2, attribute information relevant to alteration of the operation program is recorded. For example, attribute information "W (write)" meaning that the operation program is alterable, and attribute information "R (read-only)" meaning that the operation program is non-alterable, are recorded in the attribute information storage region 2. In the identification information storage region 3, identification information of the operation program or of the name of

the writer of the operation program is recorded. For example, the pass word and the name of the operation program are recorded in the identification information storage region 3. The operation program is recorded in the operation program storage region 9.

The attribute information is information which indicates whether or not the operation program stored in the operation program storage region 9 can be altered, and the identification information is collation information (alterable condition information) which is collated at the time of changing over the mode of the attribute information. Both the attribute information and the identification information may be written at the time of writing the operation program or may be written independently of the operation program writing operation.

Writing or alteration of an operation program is carried out in response to the application of a command from the external apparatus 8 to the CPU 6 which includes a microprocessor. When the CPU 6 decodes the command and detects that an operation program is to be written, a sequence of processing steps is executed according to an operation program writing control program 6a stored in the CPU 6. This operation program write control program 6a is as shown in Fig. 2.

In a step 101 in Fig. 2, decision is made as to whether or not attribute information is written already in the attribute information storage region 2. When the result of decision in the step 101 is "Yes", decision is then made in the next step 102 as to whether or not the attribute information indicates the alterability of an operation program. When the result of decision in the step 102 is "Yes", the CPU 6 carries out, in the next step 103, necessary processing to write an externally supplied operation program in the IC card 1.

In the manner of processing described above, an externally supplied operation program can be written in the operation program storage part 9 under the condition that attribute information is written already, and such an operation program cannot be written unless the attribute information is in its alterable mode. Therefore, writing of an operation program can be inhibited by rendering the attribute information in its non-alterable mode.

Writing of the attribute information itself, as well as writing of identification information and alteration of these information, is executed by activating a managing information writing control program 6b stored in the CPU 6. Fig. 3 is a flow chart of the control sequence, according to the managing information writing control program 6b.

In a step 111 in Fig. 3, decision is made as to whether or not identification information is stored already in the identification information storage region 3. When the result of decision in the step 111 is "No", the step 111 is followed by a step 112a. In the step 112a, the CPU 6 decodes information contained at a predetermined position in input information to decide whether or not writing of identification information is commanded. When

the result of decision in the step 112a is "Yes", the identification information is written in the next step 113a. On the other hand, when the result of decision in the step 112a is "No", the control sequence according to this program 6b is ended.

When, on the other hand, the result of decision in the step 111 is "Yes", the identification information stored already is read out from the identification information storage region 3 in the next step 112 and is collated with the new identification information applied to the IC card 1 as part of the input information. Then, in the next step 113, coincidence between the former and latter identification information is checked. Only when the result of checking in the step 113 is "Yes", the step 113 is followed by a step 114. In the step 114, the CPU 6 receives the new identification information or attribute information applied to the IC card 1, and, after deciding the information to be stored, stores the new identification information or attribute information in the identification information storage region 3 or attribute information storage region 2 to execute alteration of the information stored already in the storage region 3 or 2. On the other hand, when the result of collation in the step 112 followed by the result of checking in the step 113 proves non-coincidence between the identification information, the control sequence according to this program 6b comes to its end.

Usually, an IC card maker manufactures IC cards, and an IC card issuer purchased the IC cards writes predetermined data, an operation program, etc. in the IC cards so that the IC cards can be utilized in a desired form. The IC card issuer issues the IC cards to IC card utilizers, and the IC card utilizers (holders) received the IC cards use the IC cards or further issue the IC cards to IC card users.

In such a case, the operation program is generally written in the IC card 1 by both the IC card maker and the IC card issuer. The IC card maker who manufactures the IC card 1 from an IC chip is required to test the IC card 1 so as to confirm whether or not the IC card 1 can properly operate. For this purpose, it is necessary to write another operation program, that is, a test program in the IC card 1. In this case, the identification information "M-ID" of the IC card maker is first written in the identification information storage region 3 according to the managing information writing control program 6b as shown in Fig. 4A. and, using this identification information "M-ID", the attribute information "W --- (alterable)" is then written in the attribute information storage region 2. Then, the test-purpose operation program (the test program) is written in the operation program storage region 9, and the IC card 1 is tested according to the test program. When the IC card 1 is decided to properly operate, the IC card 1 is delivered from the IC card maker to an IC card issuer A as shown in Fig. 4B. At this time, the IC card issuer A receiving the IC card 1 is informed of the identification information "M-ID" written in the IC card 1 by the IC card maker.

The IC card issuer A writes a necessary operation program in the operation program storage region 9 of the IC card 1. (In this case, the test program written previously by the IC card maker is automatically altered.) Then, according to the operation program writing control program 6a, the identification information "M-ID" reported from the IC card maker is altered to, for example, "I-ID" representing the identification information of the IC card issuer A, and the attribute information "W" is also altered to "R --- (non-alterable)".

In the IC card 1 having such attribute information "R" stored in the storage region 2, alteration of its operation program according to the operation program writing control program 6a shown in Fig. 2 is now impossible, and an attempt to alter the operation program fails. Alteration of the operation program written in the IC card 1 is not possible unless the attribute information "R --- (non-alterable)" stored in the attribute information storage region 2 is altered to the attribute information "W --- (alterable)" according to the managing information writing control program 6b shown in Fig. 3. Thus, alteration of the operation program is impossible for persons or parties except the IC card issuer A who knows the identification information "I-ID".

Suppose, for example, that another IC card issuer B desires addition of another operation program. In such a case, the IC card issuer A alters the attribute information from "R --- (non-alterable)" to "W --- (alterable)" using the identification information "I-ID" and then delivers the IC card 1 to the IC card issuer B. After the IC card issuer B adds an operation program, the IC card issuer A alters the attribute information from "W --- (alterable)" to "R --- (non-alterable)" again. In this case, the IC card issuer A is authorized to alter the operation program. When the IC card issuer A abandons the right to alter the operation program, the IC card issuer B receiving the IC card 1 is namely informed of the identification information "I-ID".

An embodiment of the ID card according to the present invention will now be described in detail with reference to Figs. 5, 6 and 7.

Referring to Fig. 5, the IC card 1 can store a plurality of operation programs. For example, the program storage part 4 is designed to include two operation program storage regions, that is, a first and a second operation program storage regions 9a and 9b, so that two operation programs can be stored in the program storage part 4. Further, the program storage part 4 includes a first and a second attribute information storage regions 2a and 2b storing attribute information corresponding to the first and second operation programs stored in the first and second operation program storage regions 9a and 9b respectively, and a first and a second identification information storage regions 3a and 3b storing identification information corresponding to the first and second attribute storage regions 2a and 2b respectively.

As in the case of the IC card of Fig 1, the attribute information, for example, "W (write = alterable)" or "R (read-only = non-alterable)" relevant to alteration of the

first and second operation programs stored in the first and second operation program storage regions 9a and 9b respectively is recorded in each of the first and second attribute information storage regions 2a and 2b. Also, as in the case of the IC card of Fig 1, the identification information of the corresponding operation program or of the name of the writer of the corresponding operation program is recorded in each of the first and second identification information storage regions 3a and 3b. For example, the pass word and the name of the operation program are recorded in each of these storage regions 3a and 3b.

The operation of the IC card 1 shown in Fig. 5 will be described with reference to Fig. 6. In a step 121 in Fig. 6, the CPU 6 decodes information contained at a predetermined position in input information transmitted from the external apparatus 8, and, when the CPU 6 detects that a command for writing an operation program is applied, the CPU 6 decides whether or not such an operation program is to be written in the first operation program storage region 9a.

When the result of decision in the step 121 is "Yes" meaning that the operation program is to be written in the first operation program storage region 9a, decision is made in the next step 122a as to whether or not attribute information is written already in the first attribute information storage region 2a. When the result of decision in the step 122a is "Yes", decision is made in the next step 123a as to whether or not the attribute information is in the alterable mode. When the result of decision in the step 123a is "Yes", the CPU 6 permits alteration of the operation program in the next step 124a. Therefore, the first operation program can be written in the first operation program storage region 9a in the IC card 1, and, after executing writing of the operation program transmitted from the external apparatus 8, the processing according to the processing program comes to its end.

The manner of processing by the CPU 6 to permit alteration of the operation program is such that, in the program storage part 4 which is formed by, for example, an EEPROM, the address space of the first and second operation program storage regions 9a and 9b, in which writing is normally inhibited, is managed to permit writing of the operation program.

When the result of decision in the step 121 is "No" meaning that writing of the operation program in the first operation program storage region 9a is not commanded, decision is made in the next step 122b as to whether or not attribute information is written already in the second attribute information storage region 2b. When the result of decision in the step 122b is "Yes", decision is then made in the next step 123b as to whether or not that attribute information is in its alterable mode. When the result of decision in the step 123b is "Yes", the CPU 6 makes necessary processing in the next step 124b to permit alteration of the operation program. As a result, the operation program can be written in the second op-

eration program storage region 9b of the IC card 1, and, after writing the operation program transmitted from the external apparatus 8, the processing according to this processing program comes to its end.

When the result of decision in the step 122a or 122b is "No", or when the result of decision in the step 123a or 123b is "No", the processing according to this processing program comes to its end without writing the operation program.

Thus, by merely maintaining the attribute information in its non-alterable mode, writing of the operation program in the IC card 1 can be inhibited.

At the time of writing the attribute information itself, at the time of writing the identification information and at the time of altering these information in the manner described above, the external apparatus 8 sends out a command indicating writing of the managing information (the attribute information and the identification information). When the CPU 6 receives and decodes the command and detects that writing of the managing information is commanded, the CPU 6 activates the managing information writing control program 6b stored therein. As a result, a managing information writing sequence as shown in Fig. 7 is executed.

In a step 131 in Fig. 7, the CPU 6 decodes a command contained at a predetermined position of input information, and, when the CPU 6 detects that writing of managing information is commanded, decision is made as to whether or not writing of the managing information relevant to the first operation program is commanded. When the result of decision in the step 131 is "Yes", this means that writing of the managing information relevant to the first operation program is commanded. Then, in the next step 132a, decision is made as to whether or not identification information is written already in the first identification information storage region 3a. When the result of decision in the step 132a is "No", the step 132a is followed by a step 134a. When the CPU 6, which decodes the information contained at the predetermined position of the input information, detects in the step 134a that writing of identification information is commanded, the identification information is written in a step 136a in the first identification information storage region 3a, and, after writing, the processing according to this processing program comes to its end. On the other hand, when the result of decision in the step 134a is "No", the processing according to this processing program comes to its end, and another processing sequence takes place.

When, on the other hand, the result of decision in the step 132a is "Yes", the written identification information is read out from the first identification information storage region 3a in a step 133a, and this identification information is collated with the identification information relevant to the first operation program and contained in the input information transmitted from the external apparatus 8. A coincidence/noncoincidence flag reflecting the result of collation is stored in a predetermined memory region of the memory. In a step 135a, the co-

incidence/noncoincidence flag is referenced to decide whether or not coincidence between the identification information is detected. Only when the coincidence is detected, the step 135a is followed by a step 137a. In the step 137a, the CPU 6 receives the identification information or attribute information relevant to the applied new first operation program and decides that either the identification information or the attribute information is contained in the input information. According to the result of decision, the CPU 6 stores the identification information or the attribute information in the corresponding storage region which is the first attribute information storage region 2a or the first identification information storage region 3a. This executes alteration of the identification information or attribute information. After the alteration, the processing according to this processing program comes to its end. When the result of decision in the step 135a is "No" meaning that noncoincidence is detected, the processing according to this processing program comes to its end.

When the result of decision in the step 131 is "No" meaning that writing of the managing information relevant to the first operation program is not commanded, the step 131 is followed by a step 132b. In the step 132b, decision is made as to whether or not identification information is written already in the second identification information storage region 3b. When the result of decision in the step 132b is "No", the step 132b is followed by a step 134b. When the CPU 6, which decodes the information contained at the predetermined position of the input information, detects in the step 134b that writing of identification information is commanded, the identification information is written in a step 136b in the second identification information storage region 3b, and, after writing, the processing according to this processing program comes to its end. On the other hand, when the result of decision in the step 134b is "No", the processing according to this processing program comes to its end, and another processing sequence takes place.

On the other hand, when the result of decision in the step 132b is "Yes", the written identification information is read out from the second identification information storage region 3b in a step 133b, and this identification information is collated with the identification information relevant to the second operation program and contained in the input information. Decision is made in a step 135b as to coincidence or noncoincidence between these identification information. Only when the coincidence is detected, the step 135b is followed by a step 137b. In the step 137b, the CPU 6 receives the identification information or attribute information relevant to the applied new second operation program and decides that either the identification information or the attribute information is contained in the input information. According to the result of decision, the CPU 6 stores the identification information or the attribute information in the corresponding storage region which is the second attribute information storage region 2b or the

second identification information storage region 3b. After storing, the processing according to this processing program comes to its end. When the result of decision in the step 135b is "No" meaning that noncoincidence is detected as the result of collation between the identification information, the processing according to this processing program comes to its end, and another processing sequence takes place.

The procedure for issuing the IC card operating as described above will now be described with reference to Figs. 8A to 8M.

Fig. 8A shows the IC card 1 in a state in which nothing is written in its program storage part 4. The IC card maker loads the IC card 1 on the external apparatus 8, and a command for writing the identification information "M-ID" relevant to the first operation program is sent out from the external apparatus 8 to the IC card 1. The CPU 6 in the IC card 1 decodes the command sent out from the external apparatus 8 and detects that writing of the managing information is commanded. According to the result of decoding the command, the managing information writing control program 6b is activated. Then, the CPU 6 decodes information contained at the predetermined position of the input information and detects that writing of the managing information relevant to the first operation program is commanded. The CPU 6 checks whether or not the identification information is written already in the first identification information storage region 3a. When the CPU 6 decides that the identification information is not written in the identification information storage region 3a, the CPU 6 decodes information contained at another predetermined position of the input information and detects that writing of the identification information is commanded. After the identification information "M-ID" is written in the first identification information storage region 3a, the CPU 6 acts to end the processing according to the processing program and, at the same time, sends out a response to the external apparatus 8 to inform the termination of the processing according to the managing information writing control program 6b. The external apparatus 8 having received the response informs the IC card maker of the fact that the managing information writing process has been terminated. A display or the like is provided for this purpose.

In the processing program described above, the CPU 6 decodes the information contained at the predetermined position of the input information to detect that writing of the managing information or writing of the identification information is commanded. For this purpose, the external apparatus 8 may send out an electrical message containing a managing information writing command together with information at a predetermined position of the message, and the CPU 6 may decode such information. Alternatively, the external apparatus 8 may send out an electrical message each time some processing is executed in the IC card 1, and the CPU 6 may decode information contained at a command position of each electrical message. The same applies to the

later description and also to the embodiment shown in Fig. 1.

By the processing described above, the IC card 1 is changed from the state shown in Fig. 8A to the state shown in Fig. 8B.

The IC maker then actuates the external apparatus 8 to send out a command for writing the managing information relevant to the first operation program in the IC card 1 whose state is shown in Fig. 8B. The CPU 6 in the IC card 1 decodes the command sent out from the external apparatus 8 and detects that writing of the managing information is commanded. The CPU 6 activates the managing information writing control program 6b. The CPU 6 decodes the information contained at the predetermined position of the input information and detects that writing of the managing information relevant to the first operation program is commanded. Then, the CPU 6 checks whether or not the identification information is written already in the first identification information storage region 3a. When the CPU 6 decides that the identification information is written already, the CPU 6 reads out the identification information "M-ID" from the first identification storage region 3a, and, at the same time, sends out a response to the external apparatus 8 to inform that the IC card 1 is ready to receive identification information.

The external apparatus 8 received this response sends out a message which informs the IC card maker of the fact that the IC card 1 is ready to receive identification information and which requests application of the identification information.

The IC card maker received the above message applies to the external apparatus 8 an input representing the identification information "M-ID" relevant to the first operation program together with a command commanding writing of attribute information relevant to the first operation program. The external apparatus 8 received such an input sends out to the IC card 1 an electrical message containing the identification information and the attribute information writing command.

In the IC card 1 received the above electrical message, the identification information read out from the first identification information storage region 3a is collated by the CPU 6 with the identification information of the first operation program sent out from the external apparatus 8. After confirmation of coincidence between these identification information, the CPU 6 decodes the information contained at another predetermined position of the input information and detects that writing of the attribute information "W" relevant to the first operation program is commanded, and this attribute information "W" is written in the first attribute information storage region 2a. Then, the CPU 6 acts to terminate the processing according to this processing program and sends out a response to the external apparatus 8 to inform that the managing information writing control program 6b has ended. As a result, the IC card maker is informed from the external apparatus 8 of the fact that the managing

information writing sequence has ended. As a result of the above manner of processing, the state of the IC card 1 shown in Fig. 8B is changed into the state shown in Fig. 8C.

Then, the IC card maker actuates the external apparatus 8 to send out a command for writing a test program in the first operation program storage region 9a of the IC card 1. This test program is one of operation programs and is used to test the operation of the IC card 1.

When the command is received, the CPU 6 of the IC card 1 decodes the command and detects that writing of the operation program (the test program) is commanded. The CPU 6 activates the operation program writing control program 6a. Then, the CPU 6 decodes information contained at a predetermined position of the input information and detects that writing of the operation program in the first operation program storage region 9a is commanded. Then, the CPU 6 checks whether or not attribute information is written already in the first attribute information storage region 2a. Since the attribute information "W" is written already in the first attribute information storage region 2a, the CPU 6 decides that the attribute information "W" is written already in the first attribute information storage region 2a. The CPU 6 sends out a response to the external apparatus 8 to inform that the operation program can be written. Now, the IC card 1 is ready to receive program data to be then sent out from the external apparatus 8. When the program to be sent out is specified already, the external apparatus 8 sends out the specified program. When, however, the program to be sent out is not specified yet, the external apparatus 8 delivers a message to the IC card maker to request the maker to send out the program. Finally, the test program is sent out from the external apparatus 8.

When the CPU 6 receives the data of the program sent out from the external apparatus 8, the CPU 6 executes the processing program for writing the operation program (which is the test program now) in the first operation program storage region 9a. After writing, the CPU 6 terminates the processing according to the processing program and, at the same time, sends out a response to the external apparatus 8 to inform the termination of program writing according to the operation program writing control program 6a. The IC card maker is informed, through the external apparatus 8, of the fact that the writing of the operation program has ended. As a result of the above manner of processing, the IC card 1 is changed from the state shown in Fig. 8C to the state shown in Fig. 8D.

Then, using the test program stored in the first operation program storage region 9a, the IC card maker tests the operation of the IC card 1. After the IC card maker confirms (decides) that the IC card properly operates, the IC card maker delivers the IC card having the state shown in Fig. 8D to an IC card issuer A, and the identification information "M-ID" relevant to the test program is also reported from the IC card maker to the

IC card issuer A.

The IC card issuer A then applies a signal representing the identification information "M-ID" as an input to the external apparatus 8 so as to collate it with the identification information "M-ID" stored in the IC card 1 having the state shown in Fig. 8D. After collation, the IC card issuer A alters the identification information "M-ID" to personally selected identification information, for example, "I-ID". The IC card 1 in this state is shown in Fig. 8E. Then, the IC card issuer A writes, for example, an operation program P in the first operation program storage region 9a by carrying out processing similar to that described above.

As a result, as shown in Fig. 8F, the test program stored already in the first operation program storage region 9a is altered to the operation program P. Therefore, the test program does not remain in the IC card 1.

The IC card 1 is issued in the manner described above. When the IC card issuer A desires to inhibit alteration of the operation program P by another person or party, the CPU 6 is activated to execute the managing information writing control program 6b to collate the identification information stored in the first identification information storage region 3a and to write the attribute information "R" in the first attribute information storage region 2a. By carrying out the program 6b, the attribute information stored in the first attribute information storage region 2a can be altered from "W" to "R". Therefore, unless the identification information "I-ID" is used for later alteration of the attribute information of the operation program P from "R" to "W", the operation program P cannot be altered. The IC card 1 in this state is shown in Fig. 8G, and, by the above manner of inhibition of alteration, the security of the IC card 1 can be greatly improved.

A person who directly uses the IC card may be present besides the IC card issuer A. Also, an IC card utilizer B who utilizes the IC card and offers the IC card to the IC card user. In this case, the IC card issuer A can permit free writing of an operation program Q prepared by the IC card utilizer B himself and can also inhibit alteration of the operation program Q.

This is attained by a process in which the IC card issuer A permits writing of the operation program Q, prepared by the IC card utilizer B, in the second operation program storage region 9b of the IC card 1. That is, the CPU 6 of the IC card 1 executes the managing information writing control program 6b to write the identification information "I-ID" in the second identification information storage region 3b. The IC card 1 in this state is shown in Fig. 8H. Then, the attribute information "W" is written in the second attribute information storage region 2b. The IC card 1 in this state is shown in Fig. 8I. The IC card issuer A delivers the IC card 1 shown in Fig. 8I to the IC card utilizer B.

The IC card utilizer B writes the operation program Q in the second operation program storage region 9b of the IC card 1 having the state shown in Fig. 8I, thereby

changing the IC card 1 to the state shown in Fig. 8J. In the IC card 1 having the state shown in Fig. 8J, the attribute information of the operation program Q cannot be altered from "W" to "R". Therefore, alteration of the operation program Q cannot be inhibited.

When the IC card utilizer B desires inhibition of alteration of the operation program Q, he brings the IC card 1 having the state shown in Fig. 8J to the IC card issuer A. The IC card issuer A writes provisional identification information "C-ID" relevant to the operation program Q specified by the IC card utilizer B in the second identification information storage region 3b to obtain the IC card 1 having the state shown in Fig. 8K. Thus, inhibition of alteration of the operation program Q can be simply done.

Thereafter, using the provisional identification information "C-ID" relevant to the operation program Q, the IC card utilizer B alters the identification information "C-ID" stored in the second identification information storage region 3b to identification information "B-ID" relevant to the operation program Q according to the managing information writing control program 6b. Then, the attribute information stored in the second attribute information storage region 2b is altered from "W" to "R" thereby obtaining the IC card 1 having the state shown in Fig. 8L.

On the other hand, when the IC card issuer A does not permit writing, by another person or party, of an operation program in the second operation program storage region 9b of the IC card 1, the identification information "I-ID" is written in the second identification information storage region 3b of the IC card 1 having the state shown in Fig. 8G, thereby obtaining the IC card 1 having the state shown in Fig. 8H. Then, the attribute information "R" is written in the second attribute information storage region 2b, thereby obtaining the IC card 1 having the state shown in Fig. 8M.

Suppose further a case where the IC card issuer A originally permits writing, by the IC card utilizer B, of the operation program Q in the second operation program storage region 9b of the IC card 1 and also permits inhibition of alteration of the operation program Q. In such a case, the IC card 1 where nothing is written in each of the second identification information storage region 3b and the second attribute information storage region 2b of the IC card 1, that is, the IC card 1 having the state shown in Fig. 8G, is delivered from the IC card issuer A to the IC card utilizer B.

In the embodiment shown in Fig. 5, two operation programs are stored in the program storage part 4 of the IC card 1 by way of example. However, it is apparent that three or more operation program may be stored in the program storage part 4 of the IC card 1. Further, to deal with the increase in the number of operation programs, the number of identification information storage regions or attribute information storage regions may be increased correspondingly, so that the IC card 1 meeting more conditions can be issued.

In the aforementioned embodiments, the attribute information storage region 2 and the identification information storage region 3 are provided in the program storage part 4. However, these regions 2 and 3 may be provided in the information memory part 5. That is, these regions 2 and 3 may be provided anywhere in the alterable memory region. Further, the attribute information storage region 2 and the identification information storage region 3 may be allocated in combination to form part of a single information storage. In this case, these information read out from the single storage are utilized as the attribute information and the identification information respectively. Further, the attribute information and the identification information may be disposed at predetermined positions of the operation program.

The operation program writing control program 6a and the managing information writing control program 6b are preferably stored in a ROM, a mask ROM or the like built in the CPU 6. However, these programs 6a and 6b need not necessarily be stored in the CPU 6 and may be stored in the program storage part 4. Further, this program storage part 4 may be a RAM instead of the EEPROM.

In each of the aforementioned embodiments, it is apparent that the information input/output part 7 may be integrally combined with the central processor unit (CPU) 6, and the CPU 6 executes the various programs described above in response to commands sent through the information input/output part 7.

It will be understood from the foregoing detailed description of the present invention that a region for storing information indicating alterability or non-alterability of an operation program is provided in an IC card together with a region for storing collation information. The operation program alterability/non-alterability information is referenced to control the alteration or non-alteration of the operation program, and, when coincidence between the internal collation information and external collation information is detected, alteration of the operation program is permitted. Therefore, the security of secrecy of the operation program of the IC card or alteration of the operation program can be greatly improved to prevent illicit alteration of the operation program of the IC card.

## Claims

### 1. An IC card comprising

memory means (4) for storing a plurality of operation programs (9) which are alterable, and processor means (6) for executing a predetermined sequence of processing steps according to each operation program, said memory means storing operation program alterability/non-alterability information indicating whether each respective operation program is alterable or non-alterable, and



- said IC card comprising means (6a) for executing alteration of each operation program when said operation program alterability/non-alterability information indicates that the respective operation program is alterable, wherein said memory means stores collation information referenced with respect to respective operation programs for permitting change-over of said operation program alterability/non-alterability information between an alterable mode and a non-alterable mode, and said IC card also comprises means (6b) for changing over said operation program alterability/non-alterability information of one of said operation programs from one to the other of said alterable mode and said non-alterable mode on detection of coincidence between said collation information of said one operation program and externally applied input information.
2. An IC card according to claim 1, wherein said IC card stores a program for changing over the mode of said operation program alterability/non-alterability information when coincidence between said input information and said collation information is detected and a program for executing alteration of said operation program when said operation program alterability/non-alterability information is in said alterable mode, and wherein said collation information is identification information referenced to identify a card handler.
  3. An IC card according to claim 1 or 2, wherein said memory means (4) storing said operation program is an alterable non-volatile memory.
  4. An IC card according to claim 1, 2 or 3, wherein said collation information is identification information referenced to identify said operation program.
  5. An IC card according to any preceding claim, wherein said collation information includes identification information referenced to identify a card handler and identification information referenced to identify said operation program.
  6. An IC card according to any preceding claim, wherein said operation program alterability/non-alterability information and said collation information are stored in memory regions where said operation programs are not stored.
  7. An IC card according to any preceding claim, wherein said plural operation programs (9a,9b) are stored in different memory regions respectively.
  8. An IC card according to any preceding claim, wherein said plural operation programs include a

system program.

9. A method of writing an operation program in an IC card comprising the steps of storing operation program alterability/non-alterability information in an alterable mode in an attribute information storage region by alterability/non-alterability information writing means,

said IC card comprising memory means including an operation program storage region (9a, 9b) for storing a plurality of operation programs, an attribute information storage region (2a, 2b) for storing operation program alterability/non-alterability information indicating whether or not each respective operation program can be written in said operation program storage region, operation program writing means (6a) for storing an externally supplied operation program in said operation program storage region when said operation program alterability/non-alterability information is in said alterable mode, and execution processor means (6) for executing a predetermined sequence of processing steps according to an operation program, wherein said memory means of said IC card further includes an identification information storage region (3a, 3b) for storing collation information referenced with respect to respective operation programs for permitting change-over of said operation program alterability/non-alterability information stored in said attribute information storage region between the alterable mode and a non-alterable mode, said IC card further includes alterability/non-alterability information writing means (6b) for storing said operation program alterability/non-alterability information of one of said operation programs in said attribute information storage region when externally applied input information coincides with said collation information of said one operation program stored in said identification information storage region, and the method further includes the steps of storing an externally supplied operation program in said operation program storage region by said operation program writing means, and then storing said operation program alterability/non-alterability information of said non-alterable mode in said attribute information storage region by said alterability/non-alterability information writing means.

#### Patentansprüche

1. Eine Chipkarte, mit

einer Speichereinrichtung (4) zum Speichern mehrerer veränderbarer Betriebsprogramme (9), und

einer Prozesseinrichtung (6) zum Ausführen einer vorgegebenen Folge von Verarbeitungsschritten gemäß jedem Betriebsprogramm, wobei die Speichereinrichtung Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit der Betriebsprogramme speichert, die angibt, ob jedes entsprechende Betriebsprogramm veränderbar oder nicht veränderbar ist, und

die Chipkarte eine Einrichtung (6a) enthält, die eine Veränderung jedes Betriebsprogramms ausführt, wenn die Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit der Betriebsprogramme angibt, daß das jeweilige Betriebsprogramm veränderbar ist, wobei die Speichereinrichtung Vergleichsinformation speichert, auf die für die entsprechenden Betriebsprogramme Bezug genommen wird, um ein Umschalten der Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit der Betriebsprogramme zwischen einem veränderbaren Modus und einem nicht veränderbaren Modus zu ermöglichen, und die Chipkarte außerdem versehen ist mit einer Einrichtung (6b) zum Umschalten der Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit der Betriebsprogramme eines der Betriebsprogramme vom veränderbaren Modus in den nicht veränderbaren Modus oder umgekehrt, wenn eine Übereinstimmung zwischen der Vergleichsinformation des einen Betriebsprogramms und von außen eingegebener Eingangsinformation erfaßt wird.

2. Eine Chipkarte gemäß Anspruch 1, bei der die Chipkarte ein Programm zum Umschalten der Form der Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit des Betriebsprogramms bei Erfassung der Übereinstimmung zwischen der Eingabeinformation und der Vergleichsinformation sowie ein Programm für die Ausführung der Veränderung des Betriebsprogramms speichert, wenn die Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit des Betriebsprogramms in der Form der Veränderbarkeit ist, und bei der die Vergleichsinformation eine Identifizierungsinformation ist, auf die Bezug genommen wird, um einen Kartenbenutzer zu identifizieren. 40
3. Eine Chipkarte gemäß Anspruch 1 oder 2, bei der die das Betriebsprogramm speichernde Speichereinrichtung (4) ein veränderbarer nichtflüchtiger Speicher ist. 45
4. Eine Chipkarte gemäß Anspruch 1, 2 oder 3, bei der

die Vergleichsinformation eine Identifizierungsinformation ist, auf die Bezug genommen wird, um das Betriebsprogramm zu identifizieren.

5. Eine Chipkarte gemäß einem vorangehenden Anspruch, bei der die Vergleichsinformation eine Identifizierungsinformation, auf die Bezug genommen wird, um einen Kartenbenutzer zu identifizieren, sowie eine Identifizierungsinformation, auf die Bezug genommen wird, um das Betriebsprogramm zu identifizieren, enthält. 50
6. Eine Chipkarte gemäß irgendeinem vorangehenden Anspruch, bei der die Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit der Betriebsprogramme und die Vergleichsinformation in Speicherbereichen gespeichert sind, in denen keine Betriebsprogramme gespeichert sind. 15
7. Eine Chipkarte gemäß irgendeinem vorangehenden Anspruch, bei der die mehreren Betriebsprogramme (9a, 9b) in jeweils unterschiedlichen Speicherbereichen gespeichert sind. 20
8. Eine Chipkarte gemäß irgendeinem vorangehenden Anspruch, bei der die mehreren Betriebsprogramme ein Systemprogramm enthalten. 25
9. Ein Verfahren zum Schreiben eines Betriebsprogramms in eine Chipkarte, das die Schritte des Speicherns von Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit von Betriebsprogrammen in einem veränderbaren Modus in einem Attributinformation-Speicherbereich mittels einer Einrichtung zum Schreiben von Veränderbarkeits-/Nichtveränderbarkeits-Information enthält, 30

wobei die Chipkarte enthält:

eine Speichereinrichtung mit einem Betriebsprogramm-Speicherbereich (9a, 9b) zum Speichern mehrerer Betriebsprogramme, einem Attributinformation-Speicherbereich (2a, 2b) zum Speichern von Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit der Betriebsprogramme, die angibt, ob jedes entsprechende Betriebsprogramm in den Betriebsprogramm-Speicherbereich geschrieben werden kann, 45

eine Betriebsprogramm-Schreibeinrichtung (6a) zum Speichern eines von außen gelieferten Betriebsprogramms in den Betriebsprogramm-Speicherbereich, wenn die Information bezüglich der Veränderbarkeit/Nichtveränderbarkeit der Betriebsprogramme im veränderbaren Modus ist, und

eine Ausführungsprozesseinrichtung (6) zum Ausführen einer vorgegebenen Folge von Verarbeitungsschritten gemäß einem Betriebspro-

gramm,  
 wobei die Speichereinrichtung der Chipkarte  
 ferner einen Identifizierungsinformation-Spei-  
 cherbereich (3a, 3b) zum Speichern von Ver-  
 gleichsinformation enthält, auf die für entspre-  
 chende Betriebsprogramme Bezug genommen  
 wird, um ein Umschalten der im Attributinforma-  
 tion-Speicherbereich gespeicherten Informa-  
 tion bezüglich der Veränderbarkeit/Nicht-  
 veränderbarkeit der Betriebsprogramme zwi-  
 schen dem veränderbaren Modus und dem  
 nicht veränderbaren Modus zu ermöglichen,  
 wobei die Chipkarte ferner eine Einrichtung  
 (6b) zum Schreiben der Veränderbarkeits-/  
 Nichtveränderbarkeits-Information enthält, die  
 die Information bezüglich der Veränderbarkeit/  
 Nichtveränderbarkeit der Betriebsprogramme  
 eines der Betriebsprogramme im Attributinforma-  
 tion-Speicherbereich speichert, wenn von  
 außen eingegebene Eingangsinformation mit  
 der Vergleichsinformation des einen Betriebs-  
 programmiertes, die in dem Identifizierungsinfor-  
 mation-Speicherbereich gespeichert ist, übere-  
 einstimmt, und  
 wobei das Verfahren ferner die Schritte des  
 Speicherns eines von außen eingegebenen  
 Betriebsprogramms in den Betriebsprogramm-  
 Speicherbereich durch die Betriebsprogramm-  
 Schreibeinrichtung und anschließend des  
 Speicherns der Information bezüglich der Ver-  
 änderbarkeit/Nichtveränderbarkeit des Be-  
 tribsprogramms des nicht veränderbaren Mo-  
 dus im Attributinformation-Speicherbereich  
 mittels der Einrichtung zum Schreiben der Ver-  
 änderbarkeits-/Nichtveränderbarkeits-Info-  
 mation enthält.

## Revendications

### 1. Carte CI de circuit intégré comprenant :

- un moyen formant mémoire (4) pour stocker une pluralité de programmes d'opérations (9) qui sont modifiables, et
- un moyen formant processeur (6) pour exécuter une séquence prédéterminée d'étapes de traitement conformément à chaque programme d'opérations,

ledit moyen formant mémoire stockant une informa-  
 tion d'altérabilité/non-altérabilité du programme  
 d'opérations qui indique si chaque programme  
 d'opérations respectif est modifiable ou non modi-  
 fiable, et ladite carte de circuit intégré comprenant  
 un moyen (6a) pour exécuter une modification de  
 chaque programme d'opérations quand ladite informa-  
 tion d'altérabilité/non-altérabilité du programme

d'opérations indique que le programme d'opéra-  
 tions respectif est modifiable,  
 dans laquelle :

- 5 ledit moyen formant mémoire stocke une informa-  
 tion d'interclassement référencée pour les  
 programmes d'opérations respectifs afin de  
 permettre une commutation de ladite informa-  
 tion d'altérabilité/non-altérabilité du program-  
 me d'opérations entre un mode modifiable et  
 un mode non-modifiable; et  
 ladite carte de circuit intégré comprend égale-  
 ment un moyen (6b) pour commuter ladite in-  
 formation d'altérabilité/non altérabilité de l'un  
 desdits programme d'opérations de l'un desdits  
 modes modifiable et non-modifiable vers l'autre  
 lors de la détection d'une coïncidence entre la-  
 dite information d'interclassement dudit pro-  
 gramme d'opérations et une information d'en-  
 trée appliquée de l'extérieur.
2. Carte de circuit intégré selon la revendication 1,  
 dans laquelle ladite carte de circuit intégré mémo-  
 rise un programme pour commuter le mode de la-  
 dite information d'altérabilité/non-altérabilité du  
 programme d'opérations quand une coïncidence  
 entre ladite information d'entrée et ladite informa-  
 tion d'interclassement est détectée, et un program-  
 me pour exécuter une modification dudit program-  
 me d'opérations quand ladite information d'altéra-  
 bilité/non-altérabilité du programme d'opérations  
 est dans ledit mode modifiable, et dans laquelle la-  
 dite information d'interclassement est une informa-  
 tion d'identification consultée pour identifier l'utilisa-  
 teur de la carte.
3. Carte de circuit intégré selon la revendication 1 ou  
 2, dans laquelle ledit moyen formant mémoire (4)  
 qui stocke ledit programme d'opérations est une  
 mémoire rémanente modifiable.
4. Carte de circuit intégré selon la revendication 1, 2  
 ou 3, dans laquelle ladite information d'interclasse-  
 ment est une information d'identification consultée  
 pour identifier ledit programmc d'opérations.
5. Carte de circuit intégré selon l'une quelconque des  
 précédentes revendications, dans laquelle ladite in-  
 formation d'interclassement contient une informa-  
 tion d'identification consultée pour identifier l'utilisa-  
 teur de la carte ainsi qu'une information d'identifi-  
 cation consultée pour identifier ledit programme  
 d'opérations.
6. Carte de circuit intégré selon l'une quelconque des  
 revendications précédentes, dans laquelle ladite in-  
 formation d'altérabilité/ non-altérabilité du program-  
 me d'opérations et ladite information d'interclasse-

ment sont stockées dans des régions de mémoire où lesdits programmes d'opérations ne sont pas stockés.

7. Carte de circuit intégré selon l'une quelconque des revendications précédentes, dans laquelle lesdits plusieurs programmes d'opérations (9a, 9b) sont respectivement stockés dans des régions de mémoire différentes. 5
8. Carte de circuit intégré selon l'une quelconque des revendications précédentes, dans laquelle lesdits plusieurs programmes d'opérations incluent un programme de système. 10
9. Procédé pour écrire un programme d'opérations dans une carte de circuit intégré qui comprend les étapes consistant à mémoriser une information d'altérabilité/non-altérabilité du programme d'opérations dans un mode modifiable dans une région de stockage d'information de caractéristique grâce à un moyen d'écriture d'information d'altérabilité/non-altérabilité, 20  
ladite carte de circuit intégré comprenant : 25
- un moyen formant mémoire qui contient une région (9a, 9b) de stockage de programmes d'opérations pour stocker une pluralité de programmes d'opérations, une région (2a, 2b) de stockage d'information de caractéristique pour stocker une information d'altérabilité/ non-altérabilité du programme d'opérations indiquant si chacun desdits programmes d'opérations peut être écrit ou non dans ladite région de stockage de programmes d'opérations, 30
  - un moyen (6a) d'écriture de programmes d'opérations servant à enregistrer un programme d'opérations appliqué de l'extérieur dans ladite région de stockage de programmes d'opérations quand ladite information d'altérabilité/ non-altérabilité du programme d'opérations est dans ledit mode modifiable, et 35
  - un moyen (6) formant processeur d'exécution, servant à exécuter une séquence prédéterminée d'étapes de traitement en accord avec un programme d'opérations, 45

dans lequel ledit moyen formant mémoire de ladite carte CI contient en outre une région (3a, 3b) de stockage d'information d'identification pour stocker une information d'interclassement associée aux programmes d'opérations respectifs pour permettre une commutation de ladite information d'altérabilité/non-altérabilité du programme d'opérations mémorisée dans ladite région de stockage d'information de caractéristique entre le mode modifiable et le mode non-modifiable, 50  
55

ladite carte CI contient en outre un moyen (6b) d'écriture d'information d'altérabilité/non-altérabilité pour enregistrer ladite information d'altérabilité/non-altérabilité de l'un desdits programmes d'opérations dans ladite région de stockage d'information de caractéristique quand une information d'entrée appliquée de l'extérieur coïncide avec ladite information d'interclassement dudit programme d'opérations mémorisée dans ladite région de stockage d'information d'identification, et le procédé comprend en outre les étapes consistant à mémoriser un programme d'opérations appliqué de l'extérieur dans ladite région de stockage de programmes d'opérations à l'aide dudit moyen d'écriture de programmes d'opérations, puis à stocker ladite information d'altérabilité/non-altérabilité du programme d'opérations dudit mode non-modifiable dans ladite région de stockage d'information de caractéristique à l'aide dudit moyen d'écriture d'information d'altérabilité/ non-altérabilité.

FIG. 1

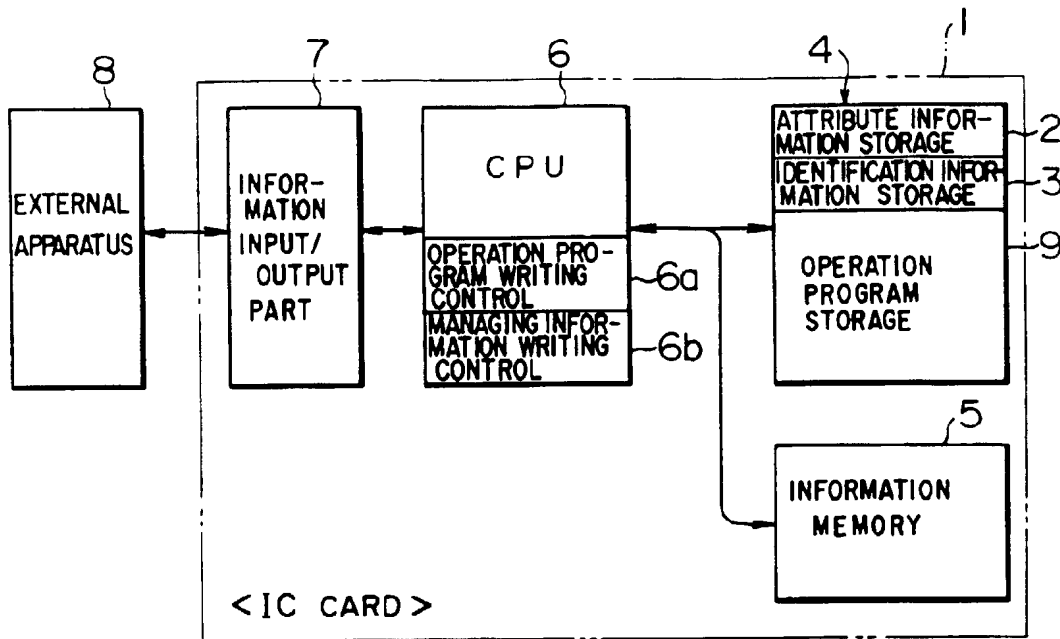


FIG. 2

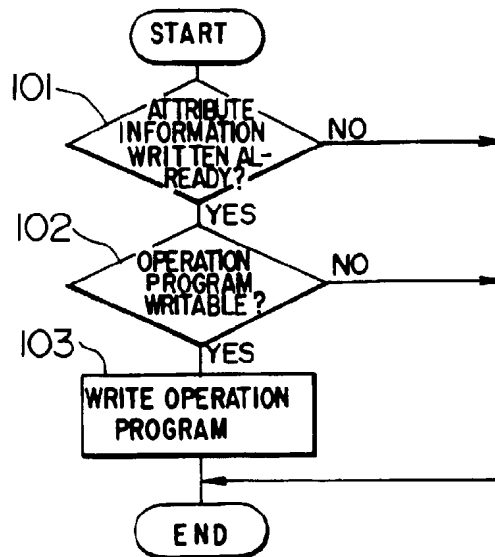


FIG. 3

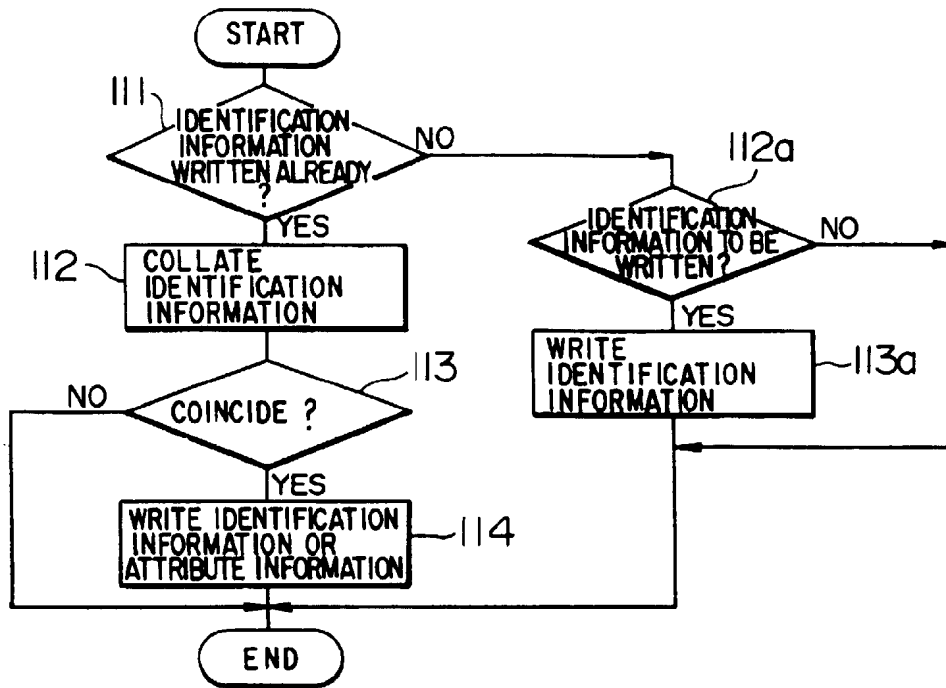


FIG. 4A

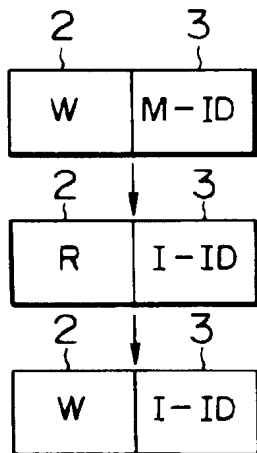


FIG. 4B

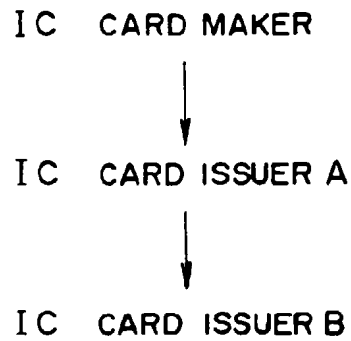


FIG. 5

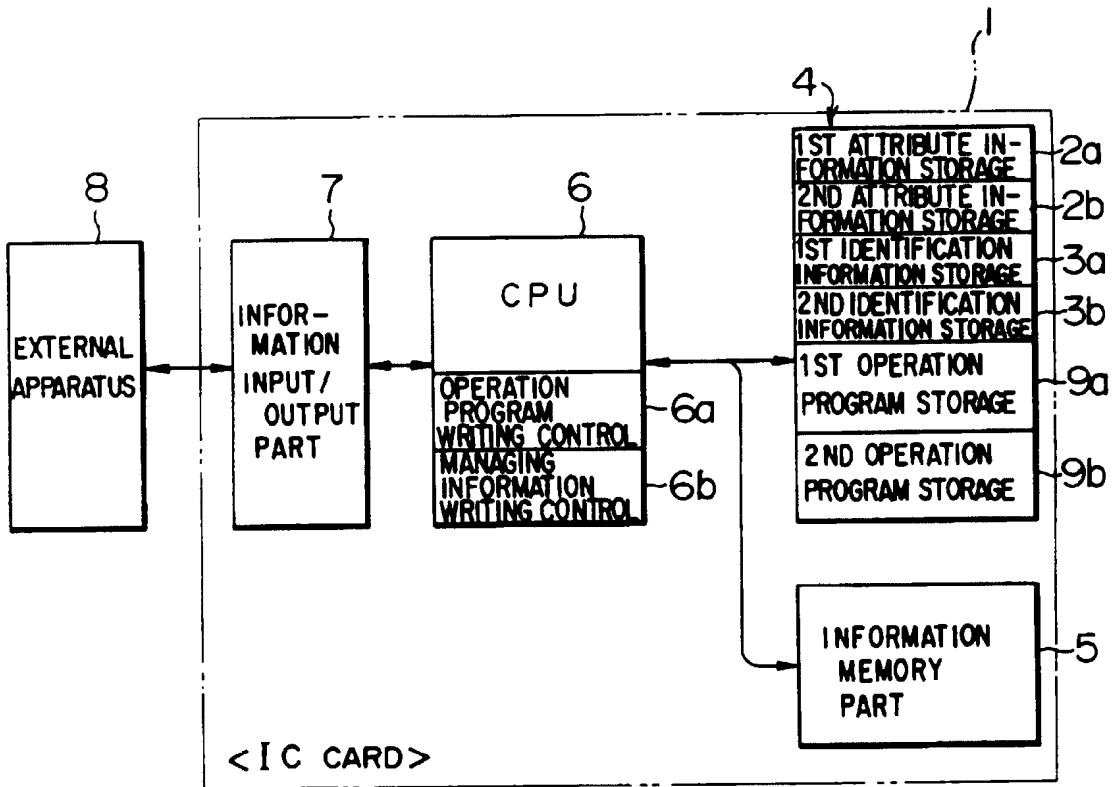


FIG. 6

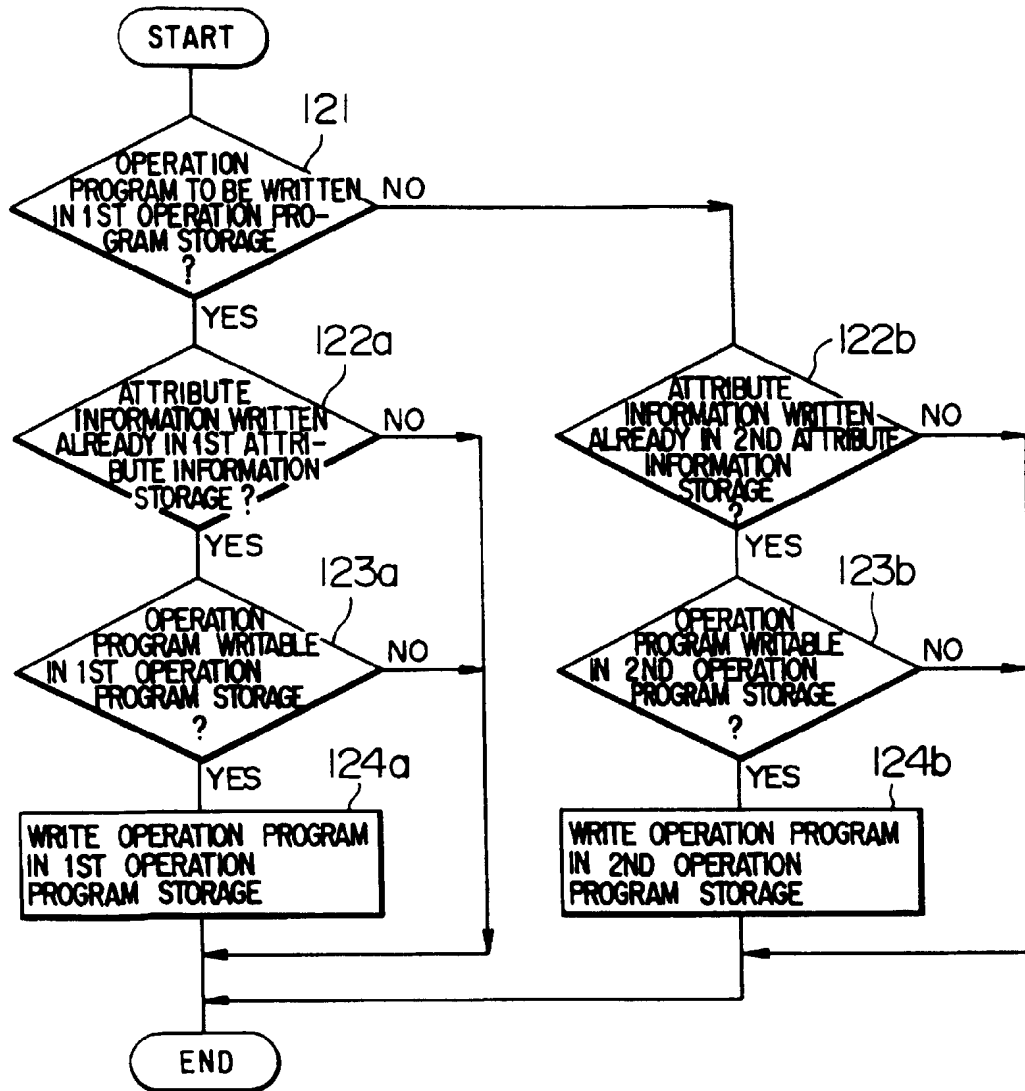
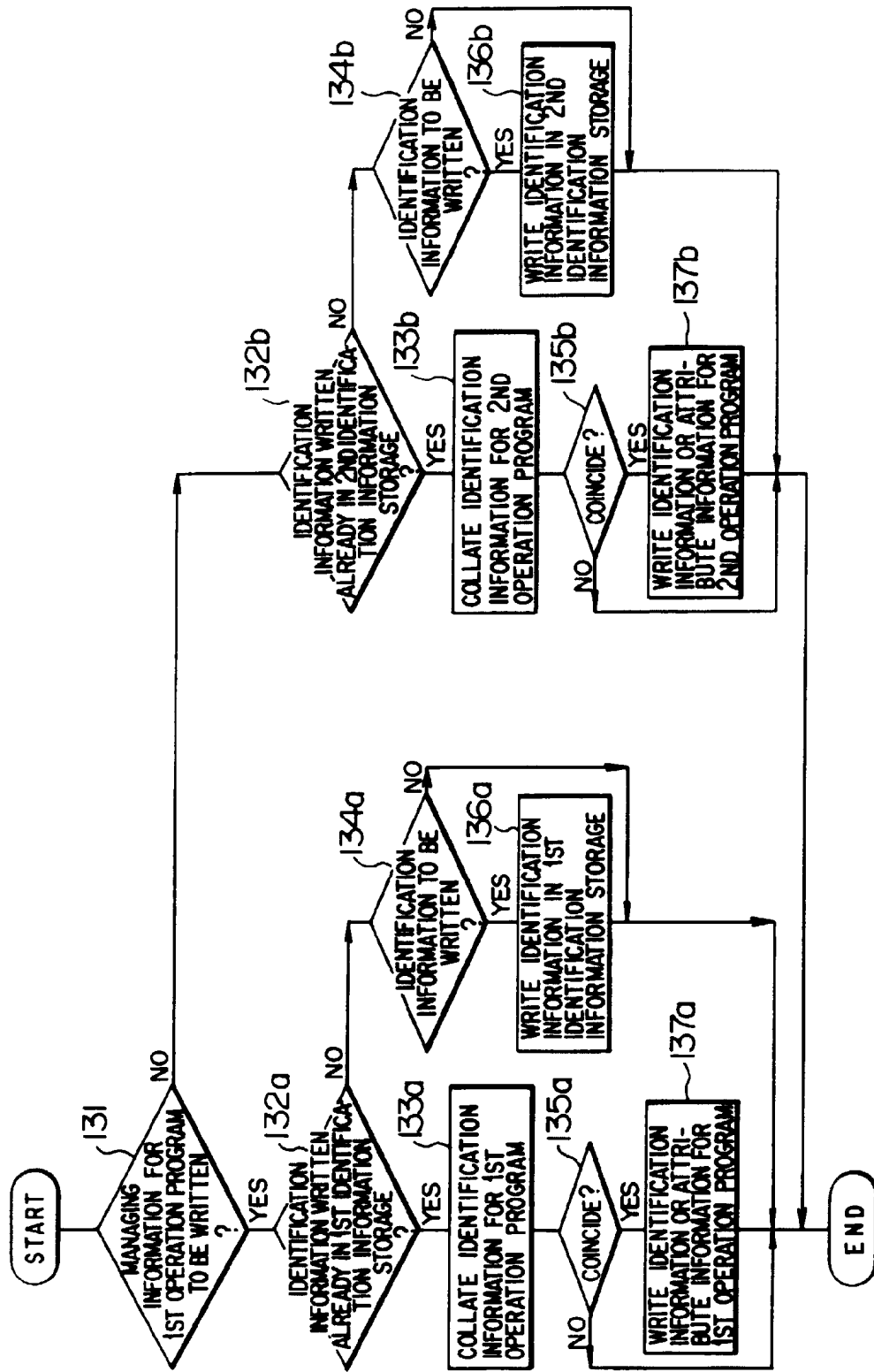
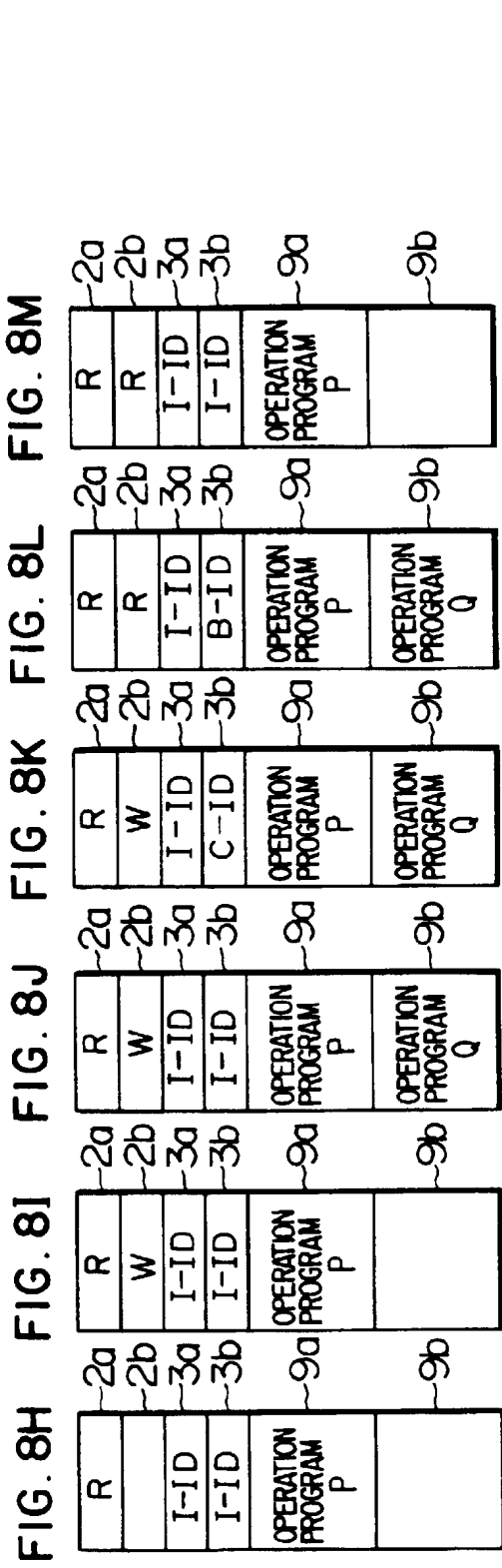
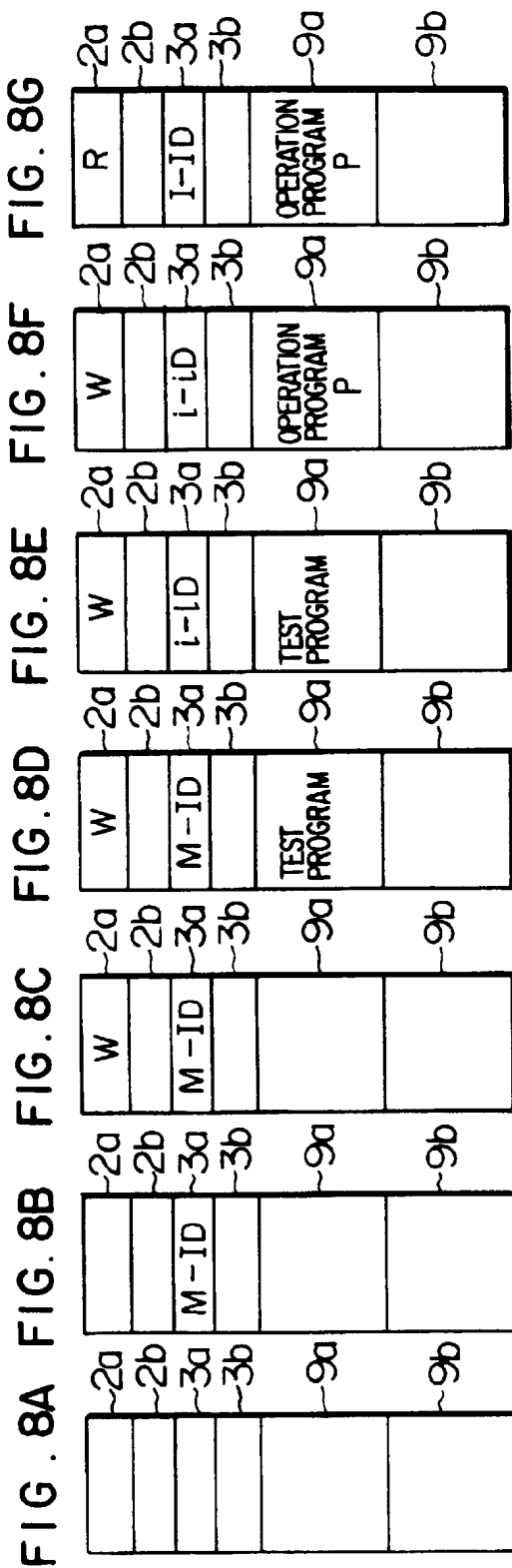




FIG. 7







(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent: **23.10.1996 Bulletin 1996/43** (51) Int Cl.<sup>6</sup>: **G07F 7/10, G06K 19/073**

(21) Application number: **89308141.4**

(22) Date of filing: **10.08.1989**

(54) **IC card and method for rewriting its program**  
Chipkarte und Verfahren zum Wiedereinschreiben ihres Programmes  
Carte à circuit intégré et méthode pour réécrire son programme

<p>(84) Designated Contracting States: <b>DE FR GB</b></p>	<p>(72) Inventor: <b>Shinagawa, Toru</b> <b>Toride-shi (JP)</b></p>
<p>(30) Priority: <b>12.08.1988 JP 201218/88</b> <b>12.08.1988 JP 201219/88</b></p>	<p>(74) Representative: <b>Senior, Alan Murray et al</b> <b>J.A. KEMP &amp; CO.,</b> <b>14 South Square,</b> <b>Gray's Inn</b> <b>London WC1R 5LX (GB)</b></p>
<p>(43) Date of publication of application: <b>14.02.1990 Bulletin 1990/07</b></p>	<p>(56) References cited: <b>FR-A- 2 600 446</b> <b>US-A- 4 829 169</b></p>
<p>(73) Proprietor: <b>HITACHI MAXELL, LTD.</b> <b>Ibaraki-shi Osaka (JP)</b></p>	

**EP 0 354 793 B1**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

## Description

### BACKGROUND OF THE INVENTION

The present invention relates to an IC card and a method for rewriting its program, and more particularly to a down-loadable IC card which is capable of rewriting its program quickly and a method for rewriting its processing program.

'IC cards' are now being used in a wide variety of applications. The IC cards issued in accordance with several kinds of transactions contain their individual data contents to be processed by different processing procedures. Therefore, the processing programs for the IC cards are peculiar to the terminals or host computers (hereinafter represented by terminals) in which they are employed.

For this reason, there has been proposed 'download processing' IC cards in which from the terminals corresponding to several transactions including bank transaction, their corresponding processing programs are afterwards written into the IC cards.

These IC cards include a rewritable non-volatile memory at their information memory part in which a processing program is stored; and thus if the operation of an IC card is desired to be changed, its program can be rewritten.

However, such a system has the following problem. In performing the write or rewrite of a program for the IC card belonging to the above class, used are instructions dedicated to high speed transfer in which programs of about 1 to 8 K bytes are transferred each byte in place of block transfer in which blocks of about 10 to 80 bytes are transferred for each byte and provides a long overhead time. And also even if the program is to be partially rewritten, the IC card is adapted so that the program has to be wholly rewritten, which takes a long time for the rewrite of program.

The program may include an application program and some parameters necessary for execution thereof. The parameters are constants, identification codes of the card and a user. Moreover, since a large amount of data must be transferred at a high speed in order to rewrite the program, the transfer error detection system becomes also complicated.

JP-A-62-231,393 discloses an IC card containing a memory for storing data which is indexed, and is not concerned with the execution of program.

FR-2,600,446 also discloses an IC card for storing indexed data.

An aim of the present invention is to provide an IC card and a method for rewriting its program in which the rewrite can be done in a very short time only by transferring to the IC card a divided program including a part to be rewritten.

Another aim of the present invention is to provide an IC card and a method for rewriting its program in which after a program is recorded in a plurality of divided

programs in a memory area, if the size of the divided programs which are objects to be newly rewritten is made larger than that before the rewriting, they can be rewritten in accordance with their corresponding memory areas.

Thus, according to the present invention there is provided a method for storing, rewriting and executing a program in an IC card having an input/output port for inputting a program to be down-loaded and outputting its processing result, a main storage area for storing data and programs, and a processor for sending the program input from the input/output port to said main storage area of the IC card, and a terminal for communicating commands to said IC card through said processor, the steps of the method comprising:

storing the program comprised of a plurality of program parts in a plurality of corresponding sub-areas of a first portion of said main storage area of the IC card,

storing a plurality of management information to identify each of the program parts stored in said sub-areas, each of said plurality of management information including a sub-area number for one of said program parts and a base address in a second portion of said main storage area of the IC card,

selecting a sub-area to be rewritten by referring to the management information based on said sub-area number,

sending the program part to be rewritten,

rewriting the contents of the selected sub-area with the sent program part, and

executing sequentially said plurality of program parts in an order based on said management information.

According to the present invention there is provided a system for storing, rewriting and executing a program in an IC card as set out in claim 6.

The circuits arranged in the IC card include rewritable non-volatile memory means for storing the processing program to be executed by an ALU and management information for managing the areas where the processing program is stored in sub-areas of divisional programs; and means for writing, referring to the management information in accordance with the information specifying one or plural of the sub-areas input to the ALU, input programs in the sub-area(s).

In order to manage a processing program stored in the rewritable non-volatile memory in the manner of being divided into plural programs constituting it, a region for storing attribute information, including the leading address and area length of each of the sub-areas where the program parts are stored, as management information indicative of the reality of the areas. It is possible to

set attribute information optionally. The processing program with any size composed of the program parts can be stored. Moreover, the above sub-areas can be optionally selected afterwards. In rewriting the processing program, it is not rewritten by transferring a whole program to an IC card but is partially rewritten only as to the sub-area storing the contents to be changed in the rewritable non-volatile memory, referring to the management information including the top address and area length of that sub-area previously stored in the IC card (the management information may be rewritten before writing the program parts if necessary).

In this way, in rewriting the processing program, only the program(s) which are desired to be rewritten in the processing program may be transferred to the IC card from the external device such as an IC card reader and writer, and therefore on the side of the IC card the entire program is not required to be rewritten so that the processing of rewriting the program can be efficiently carried out.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of the IC card according to one embodiment of the present invention;

Fig. 2a is a table showing the relation between the entire processing program of the IC card and its divided program/data parts;

Fig. 2b is a view showing the relation between areas for storing the divided program parts and their corresponding attribute information;

Figs. 3a to 3c are memory maps showing several relations between the processing program and the divided program/data parts;

Figs. 4a to 4c are views showing the relation between the attribute information about the program memory areas where a plurality of programs are stored, and their corresponding discrimination information; and

Fig. 5 is a view for explaining one example of the communication sequence between an IC card and a terminal device.

#### DESCRIPTION OF THE PREFERRED EMBODIMENT

As seen from Fig. 1, an IC card 1 is composed of an I/O part 2, an ALU or microprocessor unit (MPU) 3 and an information memory part 5 which may be rewritable non-volatile memory such as EEPROM. The I/O part 2 includes electrical contacts (not shown) on the surface of the IC card for inputting/outputting programs and for power supply. In place of the electrical contacts, electromagnetic induction may be adopted for downloading the program in the IC card. The information memory part 5 is composed of an application program memory section 7, an attribute information section 6 for storing management information for the areas of the program parts into which the application program to be

stored in the application program memory 7 is divided, and data memory section 8 for storing several kinds of data.

MPU 3 includes a system program memory 4 (e.g. mask ROM) in which a system program 4a for performing the hardware control of the IC card 1 is stored. By executing the system program 4a, MPU 3 performs the write/read of the program for the application program memory section 7 and the control of communication with terminal devices (e.g. IC card reader/writer incorporated therein). Moreover, MPU 3, by executing the system program 4a, performs the write of the attribute information transferred from an external device (the above terminal device) in the attribute information memory section 6 in accordance with an instruction transferred from the external device. As will be described later, the application program memory section 7 is managed in the manner of dividing it into a plurality of memory areas, corresponding to a plurality of program parts of the application program to be stored therein, in accordance with the attribute information stored in the attribute information memory section 6.

If the application program is to be down-loaded, it is executed for each of dividable program parts. Now it is assumed that the processing program is equally divided into program parts each with e.g. 32 bytes. However, the unit of division is not limited to 32 bytes but may be optionally selected.

First, the attribute information (Fig. 2a) about each of the areas storing each program part (32 bytes) received at the I/O part 2 is written in the attribute information memory section 6. The write of the attribute information is executed by activating the system program stored in the system program memory 4.

After the write of the attribute information, the write of the application program is performed in accordance with the sequence as shown in Fig. 5. First, a write instruction specifying the program part area to be subjected to the write using discrimination information provided in accordance with the divided program parts, i.e. the area numbers, is transferred to the IC card 1 from the terminal device (not shown). In response to the receipt of the write instruction, MPU 3 of the IC card 1 acquires, in accordance with the above discrimination information, the top address, size, etc. of the pertinent program part memory area in the application program memory section 7 from the attribute information stored in the attribute information memory section 6 and prepares the write thereof.

After the completion of this preparation of write, MPU 3 of the IC card 1 informs the terminal device of this fact through a data/control line 12 in accordance with the system program 4a.

Thus, data to be written (one of the divided program parts constituting a part of the processing program, i.e. 32 bytes) is transferred from terminal device. When received this write data, MPU 3 executes the write of the transferred program part (write data), in accordance

with the system program 4a, in the program part memory area (32 bytes) specified by the top or leading address and the size in the application program memory section 7 of the information memory part 5 of the IC card 1. Incidentally, if the memory area is fixed to 32 bytes, the above acquisition of the size of the memory area may be omitted.

After the completion of write of one data (32 bytes), discrimination information about the subsequent program part (32 bytes) is transferred from the terminal device in the same way. In accordance with the response on the side of the IC card 1, the program part (32 bytes) corresponding to the discrimination information is transferred from the terminal device. Then, this program part is stored in the program part memory area specified in accordance with the attribute information decided by the precedently transferred discrimination information. In this way, the program parts of one processing program are sequentially stored by 32 bytes. As a result, the entire processing program will be stored as a collection of the program data parts in the application program memory section 7.

Fig. 2a shows the relation between the entire processing program thus stored (a in Fig. 3a) and its program parts (b to g in Fig. 3a), and Fig. 2b shows the relation between the memory areas for storing the program parts (Fig. 2b) and their attribute information (Fig. 2a). In this embodiment, as seen from Fig. 2b, the application program memory section 7 is divided into n (n: integer of 2 or more) program memory areas 7a to 7n. Stored in plural memory areas (e.g. 7a to 7h) of the respective divided memory areas 7a to 7n are the program parts through the above write processing. In this case, the program part memory areas 7i to 7n are vacant areas reserved for rewrite. The order of writing the program parts may be optional since the write is performed in accordance with the numbers of the sub-areas, i.e. items of discrimination information.

As seen from Fig. 2a, the attribute information is stored in a table form in the attribute information memory section 6. Program area numbers are stored at the heads of the respective rows as information for discriminating the program areas for storing the program parts and further spaces for storing the base address and size for each row are provided.

The program area numbers, a, b, c, ... n in Fig. 2a correspond to the program part memory areas 7a, 7b, 7c, ... 7n with the same subscripts in Fig. 2b. Also, in Fig. 2a, aaaa, AA; bbbb, BB; cccc, CC; ... nnnn, NN in the respective spaces corresponding to the program area numbers a, b, c, ... n represent the base address and size thereof, respectively. The reason why both base address and size are provided is that although this is not required in the case the application program is managed in the equally divided program parts of 32 bytes, it is intended to manage the program in the program parts of any integer times of 32 bytes.

The application program in the case where it is man-

aged in the program divided parts is executed in the sequence of the above program area numbers, namely in the sequence of a, b, c, ... n this embodiment. Therefore, initially, as shown in Fig. 2b, the sequence of the program area numbers a, b, c, ... n accord with the sequence of arranging the program parts. And even if the sequence is changed by rewriting any program part, any problem does not occur since the previous program area numbers are retained.

Moreover, in the case where the processing program is not to be executed in the sequence of the numbers of program areas, information for specifying the sequence of connecting the program parts in the respective memory areas is previously stored in the information memory section 5, or the program area number to be subsequently executed is previously stored at the end of the program part to be stored in each program area, thereby executing the application program composed of program parts the memory areas of which are discontinuously arranged. The sequence of executing the program parts may be stored in the attribute information memory section 6.

Now it is assumed that a shaded portion 70 of the program part 7b is desired to be rewritten. In this case the rewrite of the program part 7b has only to be instructed from the terminal device, where the program parts relative to the program areas 7a and 7c to 7n are not required to be transferred. More specifically, if the rewrite portion is specified from the terminal device in terms of the discrimination information referring to the attribute information corresponding to the program memory area 7b, MPU 3, as in the case of write of the application program mentioned above, searches, acquires and accesses the attribute information relative to the program part 7b, referring to the discrimination information stored in the attribute memory section 6, in response to comparison between the description information and the attribute information, and writes the program part sent from the terminal device in the specified memory area.

Additionally, if the program part to be rewritten is smaller in size than the previous program part, the attribute information is not required to be changed since NOP is embedded in the remaining portion of the sub-area. On the other hand, if the program data to be rewritten is in size larger than the previous program part, the overflowing portion is written in a vacant area 7b'. And in executing the application program, added is an instruction of jumping to the top address (bbbb' in Fig. 2b) of the area 7b' to execute the program part therein and jumping to the top address of the memory area subsequent to the area subjected to the rewrite. It is of course that the memory area of the program part to be stored in the vacant area is previously set by newly writing the attribute information thereof in the attribute information memory section 6. Otherwise, if the program part to be rewritten is larger in size than the previous program part, attribute information may be previously sent from

the terminal device to register renewed base address and size for the same program area number in the attribute information memory section 6, thereby setting the area for storing in another vacant area of the information memory part 5. Then, the information in the memory area where the program part before the rewrite has been stored is cleared.

Several manners of setting program part memory areas will be explained with reference to Figs. 3a and 3b. In these cases, the program part memory areas can be optionally provided by setting (writing) their attribute information in the table of the attribute information section 6. Incidentally, Figs. 3a to 3c are all directed to the initial writing.

In an embodiment of Fig. 3a, the corresponding items of attribute information are set so that the entire application program can be stored in the way of dividing it into plural program parts each having a previously set information length. In initially writing the application program, the entire application program is first written in the program part memory area a. In this case, the program memory area is set to have a fixed length, regardless of the contents of the application program. In this way, the entire application program is previously stored in the program part memory area a which is a memory area of the entire application program. Thereafter, attribute information is written so that the program part a can be managed doubly as program parts b to g by writing the corresponding program parts as indicated by arrows for the partial change of the program.

In the case where the application program can be divided by sub-routines as function units, the program is stored by the sub-routine in the program part memory areas. In this case, the size of the program part memory area may be set at the size necessary to store the maximum one of the sub-routines.

In an embodiment of Fig. 3b, attribute information is previously written so that the program memory area a can be set doubly as only the program part areas b and c which are areas (e.g. area for table information) the rewrite of which is expected. The application program commonly has the constants employed internally or externally, the table for deciding the operation, etc. These are indicated internally in the program and hence the specification of the program can be changed to a certain degree by rewriting them. If the table information and the constants have only to be changed in rewriting the program, the program part memory areas may be rewritten.

Fig. 3c is directed to the case of setting an area for e.g. table information, like Fig. 3b. In this case, the entire table information area is set as a program part memory area b. Information relative to specific controls of the table information is stored collectively in a program part memory area c. In this way, the sub-memory area can be further doubly set so that part of the table information can be further rewritten.

In all of the above cases, if the program part to be

rewritten in the program memory area a is comparatively large, a program instructing the jump to another program part memory area, which is a rewrite destination, is written. Thus, the execution sequence is shifted to the other program part stored in a vacant memory area of the application program memory section 7, thereby executing the entire application program.

Moreover, a single application program need not be stored in the application program memory section 7 but plural different may be stored therein. Figs. 4a to 4c show one such an example. In this example, four application programs A, B, C and D (Fig. 4a) are stored in application program memory areas 71, 72, 73 and 74 of the application program memory section 7 (Fig. 4c). In this example, a program discrimination information section 9 is provided in the information memory part in order to discriminate the program memory areas for storing the program parts included in each application program.

If, prior to executing the write, discrimination information for discriminating the application program and program part memory areas is inserted in a write instruction, it is possible to rewrite the program parts in each application program, in the same procedure and sequence as mentioned above, referring to the program discrimination information section 9 and attribute information memory section 61 (Fig. 4b). Additionally, specifying the application program in this example may be made by preparing a dedicated instruction without inserting the discrimination information in the write instruction. Moreover, if there are plural application programs, attribute information about the program may be provided for each program.

Fig. 5 shows the procedure for rewriting program parts. A terminal device specifies, using a program area number, the program part memory area corresponding to the program part to be written and issues a write instruction thereof. An IC card, after having received the write instruction, searches the specified program part memory area from the attribute information. Then, it acquires the base address and size of the pertinent program memory area for the preparation of write. After the completion of the preparation, the IC card informs the fact of the terminal device. In response to this, the terminal device prepares the transfer of the program to be written and transfers it to the IC card. The IC card performs the write of the program part after the receipt thereof or concurrently with the receipt. After the completion of the write, the IC card informs the terminal device of this fact, thereby completing the write. As understood from the above description, the terminal device has only to specify the program number corresponding to the pertinent program part whereby the IC card internally tests the finding of the area to be subjected to the write and the possibility of the write. The write is performed only if the IC card judges that the write can be made.

In the arrangement of the IC card shown in Fig. 1, the system program memory 4 may be provided in the

information memory part 5. Moreover, the attribute information about the program part memory areas may include the end address of each program memory area in place of the base address to specify the area by adding 1 to the end address of the previous area, or subtracting by 1 from the end address of the specified area. It may also include the end address and others in addition to the base address. Further, the attribute information should not be limited to such items but may be and management indicative of the reality of the program parts in the information memory part 5.

The information memory part 5 may be composed of either a single memory element or plural elements as long as the application program memory section 7 is rewritable. Moreover, although the application program was made partially rewritable in the above embodiment, it may be any program as long as it can be executed by MPU 3. Additionally, address updating in the card reader/writer for producing the program part for rewrite is ceased at the address corresponding to the end address for the program part memory area for rewrite.

#### Claims

1. A method for storing, rewriting and executing a program in an IC card having an input/output port (2) for inputting a program to be down-loaded and outputting its processing result, a main storage area (5) for storing data and programs, and a processor (3) for sending the program input from the input/output port to said main storage area of the IC card, and a terminal for communicating commands to said IC card through said processor, the steps of the method comprising:

storing the program comprised of a plurality of program parts in a plurality of corresponding sub-areas of a first portion (7) of said main storage area of the IC card,

storing a plurality of management information to identify each of the program parts stored in said sub-areas, each of said plurality of management information including a sub-area number for one of said program parts and a base address in a second portion (6) of said main storage area (5) of the IC card,

sending a sub-area number corresponding to a program part to be rewritten from the terminal to the IC card,

selecting a sub-area to be rewritten by referring to the management information based on said sub-area number,

sending the program part to be rewritten,

rewriting the contents of the selected sub-area with the sent program part, and

executing sequentially said plurality of program parts in an order based on said management

information.

2. A method according to claim 1, further comprising the steps of, if a selected program part to be rewritten exceeds the capacity of the sub-area previously occupied by an original program part, rewriting a base address of the management information corresponding to said original program part with an address of another vacant sub-area and automatically storing said selected program part into said other vacant sub-area of said plurality of sub-areas in said main storage of the IC card.
3. A method according to claim 1 or 2, wherein each said management information also includes the size of the sub-area in correspondence to said sub-area number and said base address included in said management information.
4. A method according to claim 1, 2 or 3, further comprising the step of:
  - when the program part for rewrite exceeds the capacity of the sub-area where an original program part has been stored, providing an instruction of jumping to the address of a vacant sub-area in the program part and thereafter jumping to the vacant sub-area.
5. A method according to claim 1, 2, 3 or 4 wherein the memory capacity of the sub-areas is fixed at 32 bytes.
6. A system for storing, rewriting and executing a program in an IC card (1) having an input/output port (2) for inputting a program to be down-loaded and outputting its processing result, a main storage area (7) for storing data and programs, and a processor (3) for sending the program input from the input/output port to said main storage area of the IC card, and a terminal for communicating commands to said IC card through said processor, the system comprising:

means (3) for storing the program comprised of a plurality of program parts in a plurality of corresponding sub-areas of a first portion (7) of said main storage area of the IC card,

means (3) for storing a plurality of management information to identify each of the program parts stored in said plurality of sub-areas, each of said plurality of management information including a sub-area number for one of said sub-areas and a base address in a second portion (6) of said main storage area of the IC card,

means (3) for sending a sub-area number corresponding to a program part to be rewritten from the terminal to the IC card,

means for selecting a sub-area to be rewritten



by referring to the management information based on said sub-area number, means (3) for sending the program part to be rewritten,  
 means for rewriting contents of the selected sub-area with the sent program part, and means for executing sequentially said plurality of program parts in an order based on said management information.

### Patentansprüche

1. Verfahren zum Speichern, Einschreiben und Ausführen eines Programms in einer IC-Karte mit einem Eingangs/Ausgangsanschluß (2) zur Eingabe eines zu ladenden Programms und zur Ausgabe seines Verarbeitungsergebnisses, einem Hauptspeicherbereich (5) zum Speichern von Daten und Programmen und einem Prozessor (3) zum Senden der Programmeingabe von dem Eingangs-/Ausgangsanschluß zum Hauptspeicherbereich der IC-Karte und einem Anschluß zum Übermitteln von Anweisungen über den Prozessor an die IC-Karte, wobei das Verfahren die folgenden Schritte umfaßt:
  - Speichern des aus mehreren Programmteilen bestehenden Programms in mehreren entsprechenden Unterbereichen eines ersten Abschnitts (7) des Hauptspeicherbereichs der IC-Karte,
  - Speichern mehrerer Verwaltungsinformationen zur Identifikation jedes der in den Unterbereichen gespeicherten Programmteile, wobei jede der Verwaltungsinformationen die Nummer eines Unterbereichs für eines der Programmteile und eine Basisadresse in einem zweiten Abschnitt (6) des Hauptspeicherbereichs (5) der IC-Karte enthält,
  - Senden der Nummer des einem einzuschreibenden Programmteil entsprechenden Unterbereichs vom Anschluß zur IC-Karte,
  - Auswählen eines einzuschreibenden Unterbereichs durch Bezugnahme auf die Verwaltungsinformationen auf der Grundlage der Nummer des Unterbereichs,
  - Senden des einzuschreibenden Programmteils,
  - Einschreiben des gesendeten Programmteils auf die Inhalte des gewählten Unterbereichs und
  - sequentielles Ausführen der mehreren Programmteile in einer auf den Verwaltungsinformationen basierenden Reihenfolge.
2. Verfahren nach Anspruch 1, das ferner die folgenden Schritte umfaßt, wenn ein ausgewählter einzuschreibender Programmteil die Kapazität des vor-

her durch einen ursprünglichen Programmteil belegten Unterbereichs übersteigt:

- Einschreiben einer Adresse eines anderen leeren Unterbereichs auf eine Basisadresse der dem ursprünglichen Programmteil entsprechenden Verwaltungsinformation und
  - automatisches Speichern des ausgewählten Programmteils in den anderen leeren Unterbereich der mehreren Unterbereiche im Hauptspeicherbereich der IC-Karte.
3. Verfahren nach Anspruch 1 oder 2, bei dem jede der Verwaltungsinformationen auch die Größe des Unterbereichs einschließt, der der Unterbereichsnummer und der Basisadresse entspricht, die in den Verwaltungsinformationen enthalten sind.
  4. Verfahren nach Anspruch 1, 2 oder 3, das ferner den folgenden Schritt umfaßt, wenn der einzuschreibende Programmteil die Kapazität des Unterbereichs übersteigt, in dem ein ursprüngliches Programmteil gespeichert war:
    - Erzeugen einer Anweisung zum Springen zu der Adresse eines leeren Unterbereichs in dem Programmteil und anschließendes Springen zu dem leeren Unterbereich.
  5. Verfahren nach Anspruch 1, 2, 3 oder 4, bei dem die Speicherkapazität der Unterbereiche auf 32 Byte festgelegt ist.
  6. System zum Speichern, Einschreiben und Ausführen eines Programms in einer IC-Karte (1) mit einem Eingangs/Ausgangsanschluß (2) zur Eingabe eines zu ladenden Programms und zur Ausgabe seines Verarbeitungsergebnisses, einem Hauptspeicherbereich (7) zum Speichern von Daten und Programmen und einem Prozessor (3) zum Senden des Programmeingangs von dem Eingangs-/Ausgangsanschluß an den Hauptspeicherbereich der IC-Karte sowie einem Anschluß zum Übermitteln von Anweisungen über den Prozessor an die IC-Karte, wobei das System aufweist:
    - eine Einrichtung (3) zum Speichern des aus mehreren Programmteilen bestehenden Programms in mehreren entsprechenden Unterbereichen eines ersten Abschnitts (7) des Hauptspeicherbereichs der IC-Karte,
    - eine Einrichtung (3) zum Speichern mehrerer Verwaltungsinformationen zur Identifikation jedes der in den mehreren Unterbereichen gespeicherten Programmteile, wobei jede der mehreren Verwaltungsinformationen eine Unterbereichsnummer für einen der Unterbereiche und eine Basisadresse in einem zweiten

- Abschnitt (6) des Hauptspeicherbereichs der IC-Karte enthält,
- eine Einrichtung (3) zum Senden der einem einzuschreibenden Programmteil entsprechenden Unterbereichsnummer vom Anschluß zur IC-Karte,
  - eine Einrichtung zum Auswählen eines einzuschreibenden Unterbereichs anhand der Unterbereichsnummer unter Bezugnahme auf die Verwaltungsinformationen,
  - eine Einrichtung (3) zum Senden des einzuschreibenden Programmteils,
  - eine Einrichtung zum Einschreiben des gesendeten Programmteils auf die Inhalte des ausgewählten Unterbereichs und
  - eine Einrichtung zum sequentiellen Ausführen der mehreren Programmteile in einer auf den Verwaltungsinformationen basierenden Reihenfolge.

### Revendications

1. Procédé pour mémoriser, ré-écrire et exécuter un programme dans une carte de circuit intégré comprenant une borne (2) d'entrée/sortie servant à entrer un programme devant être téléchargé et à délivrer son résultat de traitement, une région (5) de mémorisation principale servant à stocker des données et des programmes, un processeur (3) servant à envoyer le programme entré par la borne d'entrée/sortie à ladite région de mémorisation principale de la carte de circuit intégré, et un terminal servant à communiquer des instructions à ladite carte de circuit intégré par l'intermédiaire dudit processeur, les étapes dudit procédé comprenant :
  - la mémorisation du programme composé d'une pluralité de parties de programme dans une pluralité de sous-régions correspondantes d'une première partie (7) de ladite région de mémorisation principale de la carte de circuit intégré,
  - la mémorisation d'une pluralité d'informations de gestion servant à identifier chacune des parties de programme mémorisées dans lesdites sous-régions, chacune desdites informations de gestion comprenant un numéro de sous-région pour l'une desdites parties de programme et une adresse de base dans une seconde partie (6) de ladite région (5) de mémorisation principale de la carte de circuit intégré,
  - l'envoi, du terminal à la carte de circuit intégré, d'un numéro de sous-région qui correspond à une partie de programme devant être ré-écrite,
  - le choix d'une sous-région devant être ré-écrite par référence à l'information de gestion basée sur ledit numéro de sous-région,

- l'envoi de la partie de programme devant être ré-écrite,
- la ré-écriture par la partie de programme envoyée du contenu de la sous-région choisie, et
- l'exécution séquentielle de ladite pluralité de parties de programme selon un ordre basé sur ladite information de gestion.

2. Procédé selon la revendication 1, comprenant en outre les étapes consistant, si une partie de programme choisie pour être ré-écrite dépasse la capacité de la sous-région précédemment occupée par une partie de programme de départ, à ré-écrire une adresse de base de l'information de gestion qui correspond à ladite partie de programme de départ avec l'adresse d'une autre sous-région vacante et à mémoriser automatiquement ladite partie de programme choisie dans ladite autre sous-région vacante de ladite pluralité de sous-régions de ladite région de mémorisation principale de la carte de circuit intégré.

3. Procédé selon la revendication 1 ou 2, dans lequel chaque information de gestion contient également la taille de la sous-région en correspondance avec ledit numéro de sous-région et ladite adresse de base contenus dans ladite information de gestion.

4. Procédé selon la revendication 1, 2 ou 3, comprenant en outre l'étape consistant, lorsque la partie de programme à ré-écrire dépasse la capacité de la sous-région dans laquelle a été mémorisée la partie de programme de départ, à envoyer une instruction de saut à l'adresse d'une sous-région vacante dans la partie de programme, puis à sauter à la sous-région vacante.

5. Procédé selon la revendication 1, 2, 3 ou 4, dans lequel la capacité de mémorisation des sous-régions est fixée à 32 octets.

6. Dispositif pour mémoriser, ré-écrire et exécuter un programme dans une carte de circuit intégré (1) comprenant une borne (2) d'entrée/sortie servant à entrer un programme devant être téléchargé et à délivrer son résultat de traitement, une région (5) de mémorisation principale servant à stocker des données et des programmes, un processeur (3) servant à envoyer le programme entré par la borne d'entrée/sortie à ladite région de mémorisation principale de la carte de circuit intégré, et un terminal servant à communiquer des instructions à ladite carte de circuit intégré par l'intermédiaire dudit processeur, ledit dispositif comprenant :
  - des moyens (3) pour mémoriser le programme composé d'une pluralité de parties de programme dans une pluralité de sous-régions corres-

- pondantes d'une première partie (7) de ladite région de mémorisation principale de la carte de circuit intégré,
- des moyens (3) pour mémoriser une pluralité d'informations de gestion servant à identifier chacune des parties de programme mémorisées dans lesdites sous-régions, chacune desdites informations de gestion comprenant un numéro de sous-région pour l'une desdites parties de programme et une adresse de base dans une seconde partie (6) de ladite région de mémorisation principale de la carte de circuit intégré, 5 10
  - des moyens (3) pour envoyer, du terminal à la carte de circuit intégré, un numéro de sous-région qui correspond à une partie de programme devant être ré-écrite, 15
  - des moyens pour choisir une sous-région devant être ré-écrite par référence à l'information de gestion basée sur ledit numéro de sous-région, 20
  - des moyens (3) pour envoyer la partie de programme à ré-écrire, 25
  - des moyens pour ré-écrire avec la partie de programme envoyée le contenu de la sous-région choisie, et
  - des moyens pour exécuter séquentiellement ladite pluralité de parties de programme selon un ordre basé sur ladite information de gestion. 30

35

40

45

50

55

FIG. 1

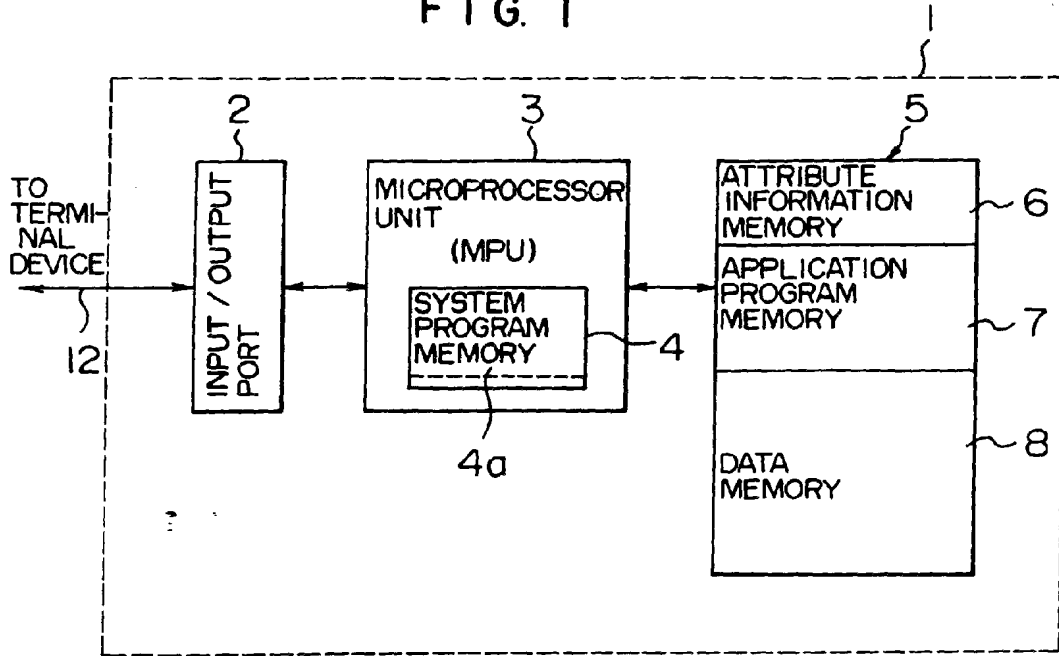


FIG. 2a  
ATTRIBUTE INFORMATION TABLE

PROGRAM AREA NO.	TOP ADDRESS	SIZE
a	aaaa	AA
b	bbbb	BB
c	cccc	CC
⋮	⋮	⋮
n	nnnn	NN

FIG. 2b

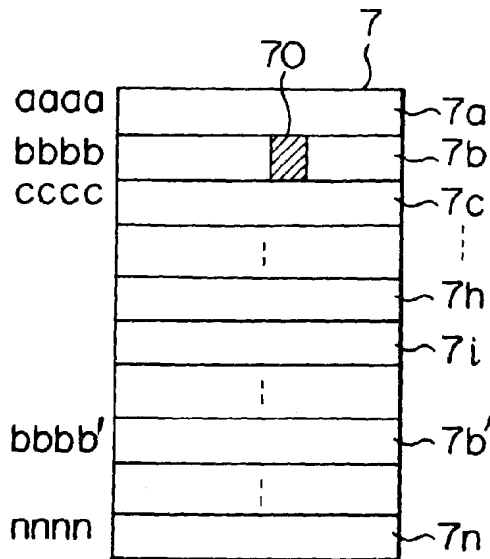


FIG. 3a

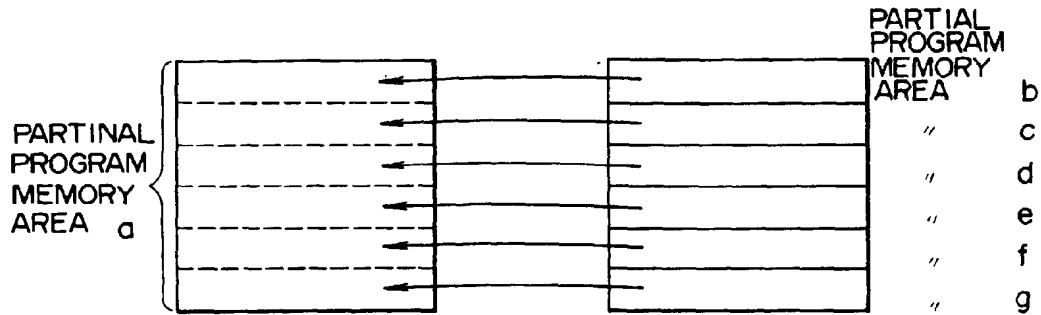


FIG. 3b

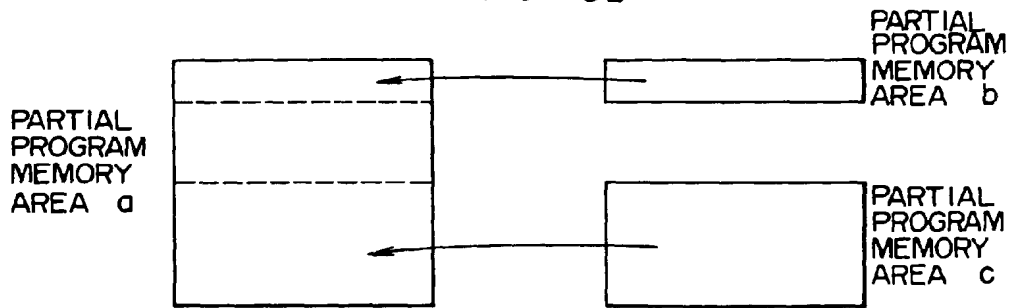


FIG. 3c

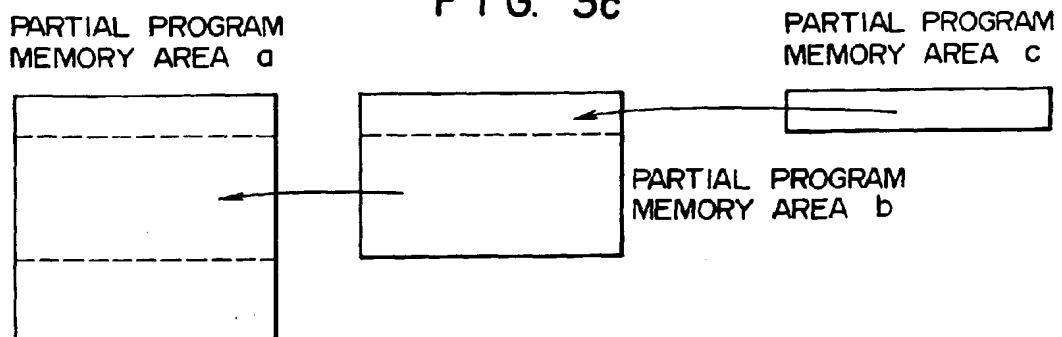


FIG. 4a 9

PROGRAM NO.	AREA NO.
A	1, 2, 3, ----, 10
B	21, ----
C	31, ----
D	41, ----

FIG. 4c 7

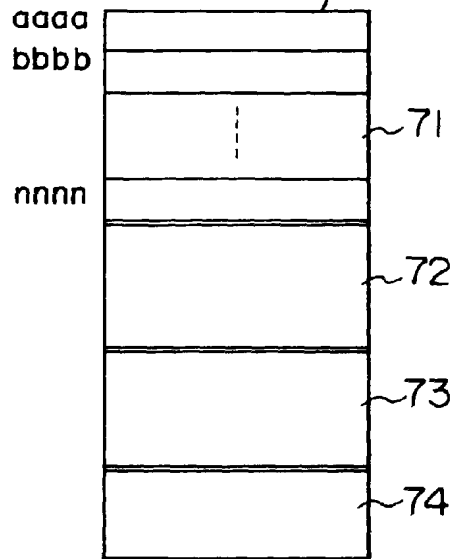
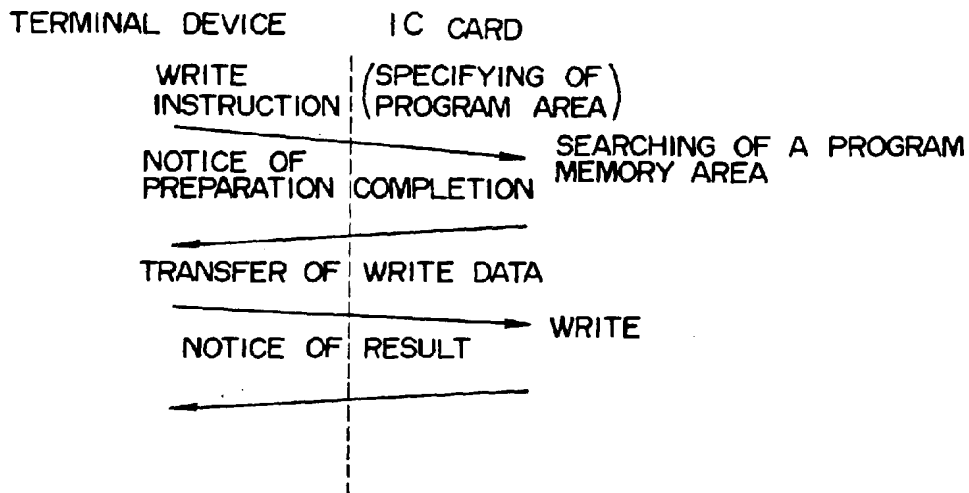
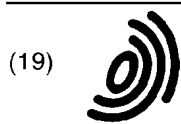


FIG. 4b

PARTIAL PROGRAM MEMORY AREA NUMBER (SUBAREA)	TOP ADDRESS	SIZE
a	aaaa	AA
b	bbbb	BB
⋮	⋮	⋮
n	nnnn	NN

FIG. 5 PROGRAM WRITE SEQUENCE





Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) **EP 0 536 792 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention  
of the grant of the patent:  
**18.03.1998 Bulletin 1998/12**

(51) Int Cl.<sup>6</sup>: **G06K 19/07, G11C 8/00**

(21) Application number: **92117330.8**

(22) Date of filing: **09.10.1992**

(54) **Audio sound recording/reproducing apparatus using semiconductor memory**

Gerät zur Aufzeichnung/Wiedergabe von Audiotönen mit einem Halbleiterspeicher

Appareil d'enregistrement/reproduction de sons audio utilisant une mémoire à semi-conducteur

(84) Designated Contracting States:  
**DE GB**

(30) Priority: **11.10.1991 JP 263654/91**

(43) Date of publication of application:  
**14.04.1993 Bulletin 1993/15**

(73) Proprietor: **SHARP KABUSHIKI KAISHA**  
**Osaka-shi Osaka-fu (JP)**

(72) Inventors:  
• **Hayashi, Kousou**  
**Higashihiroshima-shi, Hiroshima-ken (JP)**  
• **Koike, Tadashi**  
**Higashihiroshima-shi, Hiroshima-ken (JP)**

(74) Representative: **Müller, Frithjof E., Dipl.-Ing.**  
**Patentanwälte**  
**MÜLLER & HOFFMANN,**  
**Innere Wiener Strasse 17**  
**81667 München (DE)**

(56) References cited:  
**EP-A- 0 065 148**                      **EP-A- 0 294 201**  
**EP-A- 0 406 744**                      **WO-A-91/08572**  
**GB-A- 2 170 037**

- **PATENT ABSTRACTS OF JAPAN vol. 13, no. 179**  
**26 April 1989 & JP-A-01 008 949 (NIPPON DENKI**  
**SANEI KK)**
- **PATENT ABSTRACTS OF JAPAN vol. 13, no. 324**  
**21 July 1989 & JP-A-01 091 292 (HITACHI)**
- **PATENT ABSTRACTS OF JAPAN vol. 14, no. 35**  
**23 January 1990 & JP-A-01 270 192 (ASAHI**  
**GLASS CO LDT)**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

**EP 0 536 792 B1**

## Description

### BACKGROUND OF THE INVENTION

#### Field of the Invention

The invention relates generally to audio sound recording/reproducing apparatuses, and more specifically to an audio sound recording/reproducing apparatus for converting an analog signal obtained from a microphone or the like into a digital signal for recording in a semiconductor memory, converting a digital signal recorded in the semiconductor memory into an analog signal at the time of reproduction, and outputting the converted signal as an audio sound through a speaker or the like.

#### Description of the Related Art

Among audio sound recording/reproducing apparatuses, cassette tape recorders are generally known which utilize magnetic tapes such as cassette tapes. A cassette tape recorder has advantages that a magnetic tape which is a recording medium is not expensive, recording/reproducing for a long period of time is possible, etc. It is difficult however to reduce the size and volume of such a cassette tape recorder, because the apparatus needs a running mechanism for running a magnetic tape, the noise and trouble frequency of such a running mechanism are large, and a long period of time is necessary for accessing (fast forwarding, rewinding) at the time of program search (the head portion of a program is searched and brought to the position for reproduction).

The machine for noting oral statement (what is called a dictating machine) can record voice sound for a plurality of segments, and if necessary, can record information corresponding to a certain segment together with a mark for retrieval so as to aid a person to reproduce and note the information. For instance, when recording a certain document using the machine, if one desires his/her secretary to type the document later, he/she records a mark for retrieval (I mark 54) as shown in Fig. 10 (a). Subsequently he/she dictates "type this document" (the recorded portion will be referred to as an instruction portion 55). Then, the continuation of document 53 is recorded, and finally a document mark (D mark) 56 for retrieval is recorded.

Such recorded permits his/her secretary to retrieve the I mark 54 recorded on a magnetic tape 51 and listen to the instruction of the dictator subsequently recorded. Based on the instruction, the secretary retrieves the document mark 52 and types out the document 53 reproducing it from the beginning. At that time, the instruction portion 55 is skipped.

If the dictator wants to duplicate the content of the magnetic tape 51 on another magnetic tape and hand it to the secretary, for example, in the case of using the dictating machine formed of a master machine 58 and

a slave machine 57, a process will be necessary which includes in order (1) taking out the recorded magnetic tape 51 from the slave machine 57, (2) setting it in the master machine 58, (3) duplicating the content of magnetic tape 51 on a magnetic tape 59, and (4) returning the magnetic tape 51 to the slave machine 57.

As described above, in the case of the dictating machine, it takes time for retrieval and the duplicating process is cumbersome.

Accordingly, in recent years, audio sound recording/reproducing apparatuses having a semiconductor memory in place of a magnetic tape have been developed in order to solve the above-stated problem. More specifically, in an audio sound recording/reproducing apparatus utilizing a semiconductor memory, since the accessing speed is reduced to the order of  $\mu$ s, search of a program, for example, is instantaneously completed. Since a running mechanism is not required, it will be easier to reduce the size and volume of the apparatus. The apparatus will also be free from noise created by the running mechanism.

Although time for operation is reduced in a conventional audio sound recording/reproducing apparatus utilizing a semiconductor memory as described above, operation for retrieval of documents and instruction information from the audio sound recording area is still necessary.

Such an dictation recording and transcribing system with a variable playback sequence is known from the EP-A-0 065 184. In this system the dictation is recorded in the form of digitized samples in a disc memory. Like in the case of a magnetic tape recording there exists the possibility of inserting "jump codes" into the recorded dictation with the help of controls which also write jump addresses which indicate where the playback should be continued into a map memory. If one of the jump codes is reached during playback the map memory indicates the respective address where the playback has to be continued. Only the respective address of the jump code and the address where the reproduction is to be continued is written into the memory. This process ensures a continuous reproduction since several jump codes can be set with one control command. Because the disc memory, which includes a preceding RAM, has a faster access speed in comparison with the magnetic tape, all final dictation heard by the transcriber is continuous and in an order determined by the operation of the controls. It is to be noted that the reproduction is in the order of the recorded dictation and different jump positions allow to give another order of reproduction or to leave out certain parts of the dictation.

From the EP-A-0 294 201 a digital sound data storing device is known which stores digitized audio data in a semiconductor memory in the form of a detachable memory card. Additionally to the digitized audio data an address information is stored in the index region of the memory card so that the respective parts of the digitized audio data can be selected.



## SUMMARY OF THE INVENTION

It is therefore an object of the invention to retrieve/reproduce documents and instruction information instantaneously and in a simple manner in an audio sound recording/reproducing apparatus utilizing a semiconductor memory.

Another object of the invention is to eliminate the necessity for a user to retrieve instruction information prior to reproduction of a document when he/she reproduces a tape, in an audio recording/reproducing apparatus utilizing a semiconductor memory.

A further object of the invention is to eliminate the necessity for a user to retrieve instruction information in an audio sound recording/reproducing apparatus of master-slave type utilizing a semiconductor memory, in which the content of the semiconductor memory of a slave machine is stored in the memory of a master machine.

The above-stated objects of the invention are achieved by an audio sound recording/reproducing apparatus comprising a semiconductor memory, wherein said semiconductor memory includes a first recording region for recording a document and information including an instruction related to the document, both as audio information, and a second recording region for recording position data indicating the position of said document and instruction audio information in said first recording region and identification data for the information, means for storing in the first recording region the document and instruction audio information, and means for storing, during such recording, in the second recording region addresses indicating respectively the start and end of each instruction information segment and the end of a document in the first recording region as said position data characterized by : means for storing together with said addresses in said second recording region respective marks as identification data indicating whether the stored address is related to the start or end of instruction audio information or to the end of document audio information, respectively, reference means for referring to the data in said second recording region and for retrieving therefrom the start and end addresses of instruction audio information segments and end addresses of documents to be reproduced from the first recording region, based on the respective marks in the second recording region.

In the audio sound recording/reproducing apparatus, since the identification information of documents and instruction information is recorded in the second recording region, and an audio sound recording device refers to the data of the second recording region, at the time of retrieval/reproduction of the documents it is not necessary to retrieve/reproduce the audio sound data of the first recording region in which the documents and instructions related to the documents are recorded.

Consequently, it will be possible to retrieve/reproduce documents and instruction information instantane-

ously and in a simple manner in an audio sound recording/reproducing apparatus utilizing a semiconductor memory.

In another aspect of the invention, an audio sound recording system comprises the apparatus as stated above and includes a master machine and a slave machine, and a memory card is detachably attached to the master machine and the slave machine. The memory card includes said first recording region and said second recording region. The master machine includes storage means for storing the content of the memory card, and a controller for controlling the memory to record the instruction information recorded in the first recording region at the time of recording and then to store information on the document.

When the content of the memory card is stored in the memory of the master machine, document information is stored after the instruction information is stored. If the information stored in the memory is reproduced, reproduction of the instruction information is conducted prior to reproduction of the document, and therefore the user does not have to retrieve the instruction information.

The foregoing and other objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a representation showing a construction of a recording region and an index region in a memory card for use in an audio sound recording/reproducing apparatus in accordance with the invention;  
 Fig. 2 is a block diagram showing a construction of an audio sound recording/reproducing apparatus in accordance with the invention;  
 Fig. 3 is a block diagram showing the construction of the memory card shown in Fig. 2;  
 Fig. 4 is a flow chart showing an operation when a recording is conducted into a memory card by an audio sound recording/reproducing apparatus in accordance with the invention;  
 Fig. 5 is a flow chart showing an operation when a reproduction from a memory card is conducted by an audio sound recording/reproducing apparatus in accordance with the invention;  
 Fig. 6 is a representation showing a procedure when the content of a memory card is duplicated into a built-in memory in an audio sound recording/reproducing apparatus;  
 Fig. 7 is a flow chart showing an operation when the content of a memory card is duplicated in a built-in memory in an audio sound recording/reproducing apparatus;  
 Fig. 8 is a representation schematically showing a construction a built-in memory;

Fig. 9 is a flow chart showing an operation when an audio sound data duplicated in a built-memory in an audio sound recording/reproducing apparatus is reproduced;

Fig. 10 is a representation showing a construction of a magnetic tape in an audio sound recording/reproducing apparatus utilizing a conventional magnetic tape and an operation at the time of reproduction; and

Fig. 11 is a representation showing a procedure when the content of a magnetic tape is duplicated in another magnetic tape in a conventional audio sound recording/reproducing apparatus.

#### DESCRIPTION OF THE PREFERRED EMBODIMENTS

One embodiment of the invention will be described in conjunction with Figs. 1 to 8.

An audio sound recording/reproducing apparatus in accordance with the invention includes a master machine and a slave machine. The master machine, for example, as shown in Fig. 2, includes a recording/reproducing device body 1 and a memory card 6 detachable to the recording/reproducing device body 1.

The recording/reproducing device body 1 includes a system microcomputer 7 for controlling the audio sound recording/reproducing apparatus. The system microcomputer 7 is connected to an audio signal recording system, an audio signal reproducing system, a built-in memory 14, an input unit 12, a display unit 13, and the memory card 6.

The audio signal recording system includes a microphone 2 for converting an audio sound into an analog audio sound signal which is an electrical signal, an amplifier 3 for amplifying the analog audio sound signal, an AD converter 4 for digitizing the analog audio sound signal to output as a digital audio sound signal, and an audio sound compression circuit 5 for compressing the digital audio sound signal to a level in the range from a fraction to one/several tenths.

The audio sound signal reproducing system includes an audio sound expansion circuit 8 for returning audio sound data input from the memory card 6 into the digital audio sound signal before the compression, a D/A converter 9 for converting the digital audio sound signal into an analog audio sound signal for output, an amplifier 10 for amplifying the analog audio sound signal, and a speaker 11 for outputting the analog audio sound signal as audio sound.

The built-in memory 14 connected to the system microcomputer 7 has a capacity for storing all the content of the memory card 6. The capacity of the built-in memory 14 in the slave machine is about in a level allowing accommodation of indexes or data for working which will be described later, and the other construction is substantially identical to the master machine.

The input unit 12 connected to the system micro-

computer 7 includes a key portion formed of a reproduction key, a fast forwarding key, a rewinding key, an I mark key, and a D mark key. The display unit 13 is capable of displaying operation states such as reproduction and fast forwarding and elapsed time calculated from audio data by numerals and characters.

The above-stated audio sound compression circuit 5 and the audio sound expansion circuit 8 are connected to the system microcomputer 7 and the memory card 6. The audio sound compression circuit 5 inputs the audio data which is a compressed digital audio signal into the system microcomputer 7 through a data bus 20, and has the data output to the memory card 6 through the system microcomputer 7. More specifically, the system microcomputer 7 reads the compressed audio sound data and writes in the memory card 6 designating an address. The system microcomputer 7 takes in audio sound data from the audio sound compression circuit 5 one after another by incrementing the address, and repeats a writing operation into the memory card 6. At the time of reproduction, the system microcomputer 7 designates an address from the memory card 6 for reading out audio data and transmits the read out data to the audio sound expansion circuit 8.

The memory card 6 detachable to the recording/reproducing device body 1 is connected to the audio sound compression circuit 5 and the audio sound expansion circuit 8 through the data bus 20, and also connected to the system microcomputer 7 through the data bus 20, an address bus 21 and a control bus 22. The memory card 6 as shown in Fig. 3 includes an address decoder 15 and a plurality of semiconductor memories, batch erase type programmable read only memories (flash type EEPROM, hereinafter referred to as F-EEPROMs) 16, 17, 18, and 19. The higher order addresses of the address bus 21 and the card enable (CE) signal line 22a are connected to the address decoder 15.

The above-stated address 15 is connected to the F-EEPROMs 16, 17, 18 and 19 through chip select (CS) signal lines 23 and outputs a CS1 signal, a CS2 signal, a CS3 signal and a CS4 signal for selecting the F-EEPROMs 16, 17, 18 and 19, respectively. Furthermore, address bus 21, data bus 20, and an WE signal line 22b and an ERASE signal line 22c of control bus 22 are connected to the F-EEPROMs 16, 17, 18 and 19 other than the above-stated CS signal lines 23. A write enable (WE) signal for data writing is output by this WE signal line 22b, while an erase signal for batch erase of data is output by the ERASE signal line 22c.

The signals CS1-CS4 are produced by decoding higher order addresses on the address bus 21 by the address decoder 15. Since the signals CS-CS4 are exclusive, writing and reading of data can be conducted to only the F-EEPROM on which a corresponding signal is true (electrically turned on). The CE (Card Enable) signal is for detaching all the F-EEPROMs 16, 17, 18, and 19 in the memory card 6 from the data bus 20, and all the CS signals are decoded to be false when the CE

signal is true in the address decoder 15.

In the memory card 6, in addition to the recording region for recording audio data such as documents and instruction information, an index region for recording sub information (hereinafter referred to index) for addresses and identification information for identifying the documents and the instruction information is provided.

As shown in Fig. 1 (a), suppose that a document is recorded in a recording region 26 as a document portion 24. More specifically, the document portion 24 is recorded from the position indicated by address A, and instruction information is recorded from the position of the in-between address B as an instruction portion 25. The instruction portion 25 ends at the position of address C, and subsequently the document portion 24 is once again recorded to the position of address D. At that time, as shown in Fig. 1 at (b), in an index region 27, the address A is recorded, and then the flag 28 of I mark which is identification information for showing the start of the instruction portion 25 followed by recording of the address B. The flag 29 of I mark showing the end of the instruction portion 25 and the address C are recorded, followed by the flag 30 of D mark which is instruction information showing the end of the document portion 24 and its address D. Each flag and address in the index region 27 occupies a region of 4 bytes.

In the above-stated construction, a procedure when recording/reproduction is conducted to the memory card 6 utilizing an audio sound recording/reproducing apparatus in accordance with the invention will be described in conjunction with Figs. 4 and 5 and also referring to Figs. 1 and 2.

At the time of recording, a recording key which is not shown in the input unit 12 is pressed, and recording of an audio sound input from the microphone 2 into the memory card 6 is initiated by the system microcomputer 7. At that time, if the memory card 6 is partially recorded with information, recording is conducted from the D mark position which is at the end of the recorded document. More specifically, if the document is recorded to as far as the address A of the recording region 26, the flag 31 of the final D mark in the index region 27 and the address A are taken out, and recording of the document portion 24 is initiated from the position of the address A in the recording region 26 (S1). When the document is recorded through the microphone 2, recording of the document portion 24 is conducted (S2). When an I mark key (not shown) is pressed in the middle of recording (S3), the address B at that time is recorded as a priority segment into the index region 27 together with the flag 28 of I mark (S4). Then, after recording of an instruction in the instruction portion 25 (S5), when the I mark key is pressed once again (S6), the address C at that time is recorded into the index region 27 as an I mark end address together with the flag 29 of I mark (S7). Then, recording of the document is resumed (S8). When the recording is completed a D mark key (not shown) is pressed (S9), and the address D at that time is recorded

into the index region 27 together-with the flag 30 of D mark (S10).

As described above, when information recorded in the memory card 6 is reproduced, the address B at the starting end of I mark which is a priority segment, the address C at the termination end, the address A at the starting end of the document and the address B at the termination end are read out and stored in the built-in memory 14.

When reproduction is conducted a play key in the input unit 12 which is not shown is pressed and audio sound data is read out from the memory card 6 for reproduction from a speaker 11. A skip over and a skip back on a document by document basis can be made by pressing the FF and REW keys, respectively. The audio sound recording/reproducing apparatus utilizing a semiconductor memory in accordance with the present embodiment allows instantaneous skip over and skip back by referring to the data in the above-stated index region 27.

When reproduction is initiated, the reproduction is conducted from the priority segment. More specifically, as shown in Fig. 5, reproduction of the above read out address B, in other words reproduction of an audio sound from the instruction portion 25 is conducted (S11). When the reproduction of the instruction portion 25 is completed, the address A in other words the document portion 24 is reproduced from the beginning (S12), the instruction portion 25 which is the priority segment in the middle of the document portion 24 is skipped over (S13) and reproduction the document as far as the address B representing the position of D mark is conducted.

In the present embodiment, the case has been described in which only the instruction portion 25 in the single document portion 24 is reproduced as the priority segment before reproduction of the document portion 24, but the invention is not limited thereto, and the apparatus may have a function of reproducing only the instruction portions in the entire memory card 6. In that case, the most important document among a plurality of documents in the memory card 6 can be reproduced first, judging from the contents of the plurality of instruction portions. More specifically, a special code is designated for flag 28 and 29 to show the priority of the instruction and the same is referred to at the time of reproduction.

It is also possible to duplicate information from the memory card and temporarily store the information in the built-in memory in the apparatus and reproduce the information data when such information is necessary. This is because a memory card is generally expensive, and therefore, if information stored in the memory card is duplicated, the memory card can be used for another purpose.

A procedure when the above-stated operation is conducted in a slave machine and a master machine in the audio sound recording/reproducing apparatus in ac-

cordance with the present embodiment will be described in conjunction with Fig. 6. (1) The memory card 6 recorded in the slave machine 32 is taken out. (2) The memory card 6 is set in the master machine 33. (3) The content of memory card 6 is duplicated and stored in the built-in memory 14 of the master machine 33. (4) The memory card 6 is returned to the slave machine 32.

An operation when a duplication is conducted from the memory card 6 into the built-in memory 14 in the master machine 33 at that time will be described in conjunction with Figs. 7 and 8.

Fig. 8 is a representation schematically showing the construction of the built-in memory 14.

For example, when the document portion 24 in the memory card 6 is stored, the A address of D mark to be an address representing the head of the document portion 24 is read out from the index region 27 of the memory card 6, and stored in the storage region D1 in the built-in memory 14 (S14). Similarly, the address B, the address C, and the address D are stored in the storage regions I1, I2, and B2, respectively in the built-in memory 14. (S15-S17).

Then, the flag 31 of D mark in the index region 27 is stored in the index region of the built-in memory 14 (region for storing source side address hereinafter referred to as C1 index region) (S18), and similarly the flag 28 of I mark is stored in the C index region (S19).

Subsequently, the instruction portion 25 in the recording region 26 is searched (S20), and the content of the instruction portion 25 is stored in the data storage region E of the built-in memory 14 (S21). After storing of the instruction portion 25 is completed, the flag 29 of I mark is stored in the C2 index region (region for storing address where data is copied) (S22), and the start of the document portion 24 in the recording region 26 is searched (S23).

Subsequently, the document portion 24 in the recording region 26 is stored from the beginning in the data storage region E of the built-in memory 14 (S24). At that time, the instruction portion 25 is skipped over and not duplicated (S25).

When the document of the memory card 6 stored in the built-in memory 14 is reproduced, as shown in Fig. 9, until the document to be reproduced is selected documents stored before that are skipped over (S26). More specifically, the selection is effected by skipping the address and the mark stored in S19.

When the desired document is selected, the instruction portion is reproduced first (S27), and then the document portion is reproduced from the beginning (S28). At that time, in the recording region 26 of the memory card 6, since the instruction portion recorded in the middle of the document portion has been taken out and stored preceding the document portion when stored in the built-in memory 14, the document portion can be reproduced until the end without interruption by reproduction of the instruction portion.

Thus, skipping reproduction on a document by doc-

ument basis allows an instruction related to a document to be reproduced prior to reproduction of the document when the desired document is reproduced.

By the above-stated construction, since sub information related to identification information for documents to be stored and instruction (in other words I mark or D mark) is recorded in the index region 27, skipping over or skipping back of reproduction can instantaneously be conducted referring to the sub information in the index region 27. Also at the time of reproduction, since the instruction portion can be reproduced as a priority segment prior to reproduction of a document referring to the sub information in the index region 27, a user can listen to the instruction before the document without any special operation such as retrieval of the instruction portion. Furthermore, when the content of the memory card 6 is stored in the built-in memory 14 of the apparatus, the instruction portion is stored before the document portion on a document by document basis, and a document is stored skipping over the instruction portion in the middle. Therefore, when a reproduction from the built-in memory 14 is conducted, the instruction is reproduced prior to the document, and the user can instantaneously determine the content of the document, thus preventing careless mistakes and misjudgments.

Although the present invention has been described and illustrated in detail, it is clearly understood that the same is by way of illustration and example only and is not to be taken by way of limitation, the scope of the present invention being limited only by the terms of the appended claims.

## Claims

1. An audio sound recording/reproducing apparatus (1) comprising a semiconductor memory (6, 14), wherein said semiconductor memory (6, 14) includes a first recording region (26) for recording a document and information including an instruction related to the document, both as audio information, and a second recording region (27) for recording position data indicating the position of said document and instruction audio information in said first recording region and identification data for the information,

means for storing in the first recording region (26) the document and instruction audio information, and means for storing, during such recording, in the second recording region (27) addresses indicating respectively the start and end of each instruction information segment and the end of a document in the first recording region (26) as said position data,

characterized by:

means for storing together with said addresses in said second recording region (27) respective

marks as identification data, indicating whether the stored address is related to the start or end of instruction audio information or to the end of document audio information, respectively, reference means (7) for referring to the data in said second recording region and for retrieving therefrom the start and end addresses of instruction audio information segments and end addresses of documents to be reproduced from the first recording region (26), based on the respective marks in the second recording region (27).

2. An audio sound recording/reproducing apparatus (1) as recited in claim 1, further comprising, reproduction means (7, 8, 9, 10, 11) for reproducing the data of said first recording region (26) by referring to the data of said second region (27) using said reference means (7) when said document data is reproduced.
3. An audio sound recording/reproducing apparatus (1) as recited in claim 2, wherein said semiconductor memory (6, 14) includes a memory card (6) detachably mounted to said audio sound recording/reproducing apparatus.
4. An audio sound recording/reproducing apparatus (1) as recited in claim 3, wherein said memory card (6) includes a batch erase type programmable ROM (16, 17, 18, 19).
5. An audio sound recording/reproducing apparatus (1) as recited in claim 3, wherein audio sound-compressed data is written on said memory card (6).
6. An audio sound recording/reproducing apparatus as recited in claim 2, wherein said reproduction means (7, 8, 9, 10, 11) reproduces only said document audio information among the information recorded in said first recording region (26) excluding said instruction audio information at said time of reproduction.
7. An audio sound recording/reproducing apparatus (1) as recited in claim 2, wherein

a plurality of sets of document audio information and information relating thereto are stored in said first recording region (26) and second recording region (27), respectively, the apparatus (1), further comprising, specifying means (7) for specifying desired information among said plurality of sets of document audio information and information relating thereto, and reproduction means (7, 8, 9, 10, 11) for repro-

ducing only said specified document audio information when said specified information is selected.

8. An audio sound recording/reproducing system comprising the apparatus (1) of claim 3 including a master machine (33) and a slave machine (32), wherein said memory card (6) is detachably mounted to said master machine (33) and slave machine (32), and includes said first recording region (26) and said second recording region (27) and wherein said master machine (33) includes storage means (14) for storing the content of said memory card (6), and control means (7) for controlling said storage means such that the instruction information recorded in said first recording region (26) is stored and then the document information is stored when said storing operation is conducted.
9. An audio sound recording/reproducing system as recited in claim 8, wherein said storage means (14) has first and second storage regions (26, 27) for storing information recorded in said first and second recording regions (26, 27), and said control means (7) controls said storage means (14) such that the information of said second recording region (27) is stored in said second storage region (27) and said instruction information and document information are stored by referring to said second storage region (27).

#### 40 Patentansprüche

1. Gerät (1) zur Aufzeichnung/Wiedergabe von Audio-tönen mit einem Halbleiterspeicher (6, 14), bei dem der Halbleiterspeicher (6, 14) einen ersten Aufzeichnungsbereich (26) zur Aufzeichnung eines Dokuments und einer Information, die eine sich auf das Dokument beziehende Anweisung enthält, jeweils als Audioinformation, und einen zweiten Aufzeichnungsbereich (27) enthält, um die Position der Audioinformation des Dokuments und der Anweisung in dem ersten Aufzeichnungsbereich anzeigende Positionsdaten und Identifikationsdaten für die Information aufzuzeichnen, einem Mittel zur Speicherung der Dokumentaudioinformation und der Anweisungsaudioinformation in dem ersten Aufzeichnungsbereich (26), und einem Mittel zur Speicherung von Adressen als die Positionsdaten in dem zweiten Aufzeichnungsbereich

bereich (27) während einer solchen Aufzeichnung, die jeweils den Anfang und das Ende von jedem Segment für Anweisungsinformation und das Ende eines Dokuments in dem ersten Aufzeichnungsbereich (26) anzeigen,

**gekennzeichnet durch:**

ein Mittel zur Speicherung von jeweiligen Markierungen als Identifikationsdaten zusammen mit den Adressen in dem zweiten Aufzeichnungsbereich (27), die anzeigen, ob sich die gespeicherte Adresse jeweils auf den Anfang oder das Ende von Anweisungsaudioinformation oder auf das Ende von Dokumentaudioinformation bezieht,

ein Bezugnahmemittel (7) zur Bezugnahme auf die Daten in dem zweiten Aufzeichnungsbereich und zum Wiederauffinden der Anfangs- und der Endadressen von Segmenten von Anweisungsaudioinformation und der Endadressen von Dokumenten daraus, die aus dem ersten Aufzeichnungsbereich (26) wiedergegeben werden sollen, auf Grundlage der jeweiligen Markierungen in dem zweiten Aufzeichnungsbereich (27).

2. Gerät (1) zur Aufzeichnung/Wiedergabe von Audiotönen nach Anspruch 1, weiter mit einem Wiedergabemittel (7, 8, 9, 10, 11) zur Wiedergabe der Daten des ersten Aufzeichnungsbereichs (26) durch Bezugnahme auf die Daten des zweiten Aufzeichnungsbereichs (27) unter Verwendung des Bezugnahmemittels (7), wenn die Daten eines Dokuments wiedergegeben werden.
3. Gerät (1) zur Aufzeichnung/Wiedergabe von Audiotönen nach Anspruch 2, bei dem der Halbleiterspeicher (6, 14) eine Speicherkarte (6) umfaßt, die abnehmbar an dem Gerät zur Aufzeichnung/Wiedergabe von Audiotönen angebracht ist.
4. Gerät (1) zur Aufzeichnung/Wiedergabe von Audiotönen nach Anspruch 3, bei dem die Speicherkarte (6) ein stapellösbares programmierbares ROM (16, 17, 18, 19) enthält.
5. Gerät (1) zur Aufzeichnung/Wiedergabe von Audiotönen nach Anspruch 3, bei dem in die Speicherkarte (6) tonkomprimierte Audiodaten eingeschrieben werden.
6. Gerät zur Aufzeichnung/Wiedergabe von Audiotönen nach Anspruch 2, bei dem das Wiedergabemittel (7, 8, 9, 10, 11) bei der Wiedergabe nur die Dokumentaudioinformation von der in dem ersten Aufzeichnungsbereich (26) aufgezeichneten Information wiedergibt, und die

Anweisungsaudioinformation ausschließt.

7. Gerät (1) zur Aufzeichnung/Wiedergabe von Audiotönen nach Anspruch 2, bei dem

eine Mehrzahl von Gruppen von Dokumentaudioinformation und sich darauf beziehende Information jeweils in dem ersten Aufzeichnungsbereich (26) und dem zweiten Aufzeichnungsbereich (27) gespeichert sind, das Gerät (1) weiter enthält, ein Spezifizierungsmittel (7) zur Spezifizierung gewünschter Information aus der Mehrzahl von Gruppen von Dokumentaudioinformation und sich darauf beziehender Information, und ein Wiedergabemittel (7, 8, 9, 10, 11) zur Wiedergabe nur der spezifizierten Dokumentaudioinformation, wenn die spezifizierte Information ausgewählt wurde.

8. System zur Aufzeichnung/Wiedergabe von Audiotönen mit dem Gerät (1) nach Anspruch 3, das eine Hauptmaschine (33) und eine Nebenmaschine (32) enthält, wobei

die Speicherkarte (6) abnehmbar an der Hauptmaschine (33) und der Nebenmaschine (32) angebracht ist, und den ersten Aufzeichnungsbereich (26) und den zweiten Aufzeichnungsbereich (27) enthält, und bei dem die Hauptmaschine (33) ein Speichermittel (14) zur Speicherung des Inhalts der Speicherkarte (6) und eine Steuereinrichtung (7) enthält, die das Speichermittel so steuert, daß bei der Speicherung die in dem ersten Aufzeichnungsbereich (26) aufgezeichnete Anweisungsinformation gespeichert wird und danach die Dokumentinformation gespeichert wird.

9. System zur Aufzeichnung/Wiedergabe von Audiotönen nach Anspruch 8, wobei

das Speichermittel (14) einen ersten und einen zweiten Speicherbereich (26, 27) zur Speicherung von in dem ersten und dem zweiten Aufzeichnungsbereich (26, 27) aufgezeichneter Information aufweist, und die Steuereinrichtung (7) das Speichermittel (14) so steuert, daß die Information des zweiten Aufzeichnungsbereichs (27) in dem zweiten Speicherbereich (27) gespeichert wird und die Anweisungsinformation und die Dokumentinformation unter Bezugnahme auf den zweiten Speicherbereich (27) gespeichert werden.

## Revendications

1. Appareil (1) d'enregistrement/reproduction de sons audio comportant une mémoire (6, 14) à semi-conducteurs, dans lequel ladite mémoire (6, 14) à semi-conducteur comprend une première région d'enregistrement (26) servant à enregistrer un document et des informations contenant une instruction relative au document, dans les deux cas sous la forme d'informations audio, et une deuxième région d'enregistrement (27) servant à enregistrer des données de position indiquant la position dudit document et des informations audio d'instruction dans ladite première région d'enregistrement et des données d'identification pour les informations,

un moyen servant à stocker dans la première région d'enregistrement (26) le document et les informations audio d'instruction, et un moyen pour stocker dans la deuxième région d'enregistrement (27), pendant cet enregistrement, des adresses indiquant respectivement le début et la fin de chaque segment d'informations d'instruction et, dans la première région d'enregistrement (26), la fin d'un document en tant que données de position, caractérisé par:

un moyen servant à stocker conjointement avec lesdites adresses, dans ladite deuxième région d'enregistrement (27), des repères respectifs en tant que données d'identification indiquant si l'adresse stockée est relative respectivement au début ou à la fin d'informations audio d'instruction ou à la fin d'informations audio de document,

un moyen de consultation (7) servant à consulter les données dans ladite deuxième région et à extraire de celle-ci les adresses de début et de fin de segments d'informations audio d'instruction et les adresses de fin de document à reproduire à partir de la première région d'enregistrement (26), sur la base des repères respectifs de la deuxième région d'enregistrement (27).

2. Appareil (1) d'enregistrement/reproduction de sons audio selon la revendication 1, comportant en outre un moyen de reproduction (7, 8, 9, 10, 11) servant à reproduire les données de ladite première région d'enregistrement (26) en consultant les données de ladite deuxième région (27) à l'aide dudit moyen de consultation (7) lors de la reproduction desdites données de document.
3. Appareil (1) d'enregistrement/reproduction de sons audio selon la revendication 2, dans lequel ladite mémoire (6, 14) à semi-conducteurs comporte une carte (6) de mémoire montée de manière amovible sur ledit appareil d'enregistrement/

reproduction de sons audio

4. Appareil (1) d'enregistrement/reproduction de sons audio selon la revendication 3, dans lequel ladite carte (6) de mémoire comprend une mémoire morte programmable (16, 17, 18, 19) du type à effacement par paquets.

5. Appareil (1) d'enregistrement/reproduction de sons audio selon la revendication 3, dans lequel des données de compression de sons audio sont inscrites sur ladite carte (6) de mémoire.

6. Appareil d'enregistrement/reproduction de sons audio selon la revendication 2, dans lequel ledit moyen de reproduction (7, 8, 9, 10, 11) ne reproduit, audit moment de la reproduction, que lesdites informations audio de document parmi les informations enregistrées dans ladite première région d'enregistrement (26), à l'exclusion desdites informations audio d'instruction.

7. Appareil (1) d'enregistrement/reproduction de sons audio selon la revendication 2, dans lequel

une pluralité d'ensembles d'informations audio de document et les informations relatives à celles-ci sont stockées respectivement dans lesdites première région d'enregistrement (26) et deuxième région d'enregistrement (27), l'appareil (1) comportant en outre un moyen de désignation (7) servant à désigner des informations voulues parmi ladite pluralité d'ensembles d'informations audio de document et les informations relatives à celles-ci, et un moyen de reproduction (7, 8, 9, 10, 11) servant à reproduire seulement lesdites informations audio de document désignées lors de la sélection desdites informations désignées.

8. Système d'enregistrement/reproduction de sons audio comportant l'appareil (1) selon la revendication 3, comprenant une machine principale (33) et une machine secondaire (32), dans lequel

ladite carte (6) de mémoire est montée de manière amovible sur lesdites machine principale (33) et machine secondaire (32), et comporte ladite première région d'enregistrement (26), et dans lequel

ladite machine principale (33) comprend un moyen de stockage (14) servant à stocker le contenu de ladite carte (6) de mémoire, et un moyen de commande (7) servant à commander ledit moyen de stockage de façon que les informations d'instruction enregistrées dans ladite première région d'enregistrement (26) soient stockées et, donc, que les informations de do-

cument soient stockées lors de l'exécution de ladite opération de stockage.

9. Système d'enregistrement/reproduction de sons audio selon la revendication 8, dans lequel 5

ledit moyen de stockage (14) a une première et une deuxième régions de stockage (26, 27) servant à stocker des informations enregistrées dans lesdites première et deuxième régions d'enregistrement (26, 27), et 10

ledit moyen de commande (7) commande ledit moyen de stockage de façon que les informations de ladite deuxième région d'enregistrement (27) soient stockées dans ladite deuxième région d'enregistrement (27) et que les lesdites informations d'instruction et informations de document soient stockées par consultation de ladite deuxième région de stockage (27). 15  
20

25

30

35

40

45

50

55

10



FIG. 1

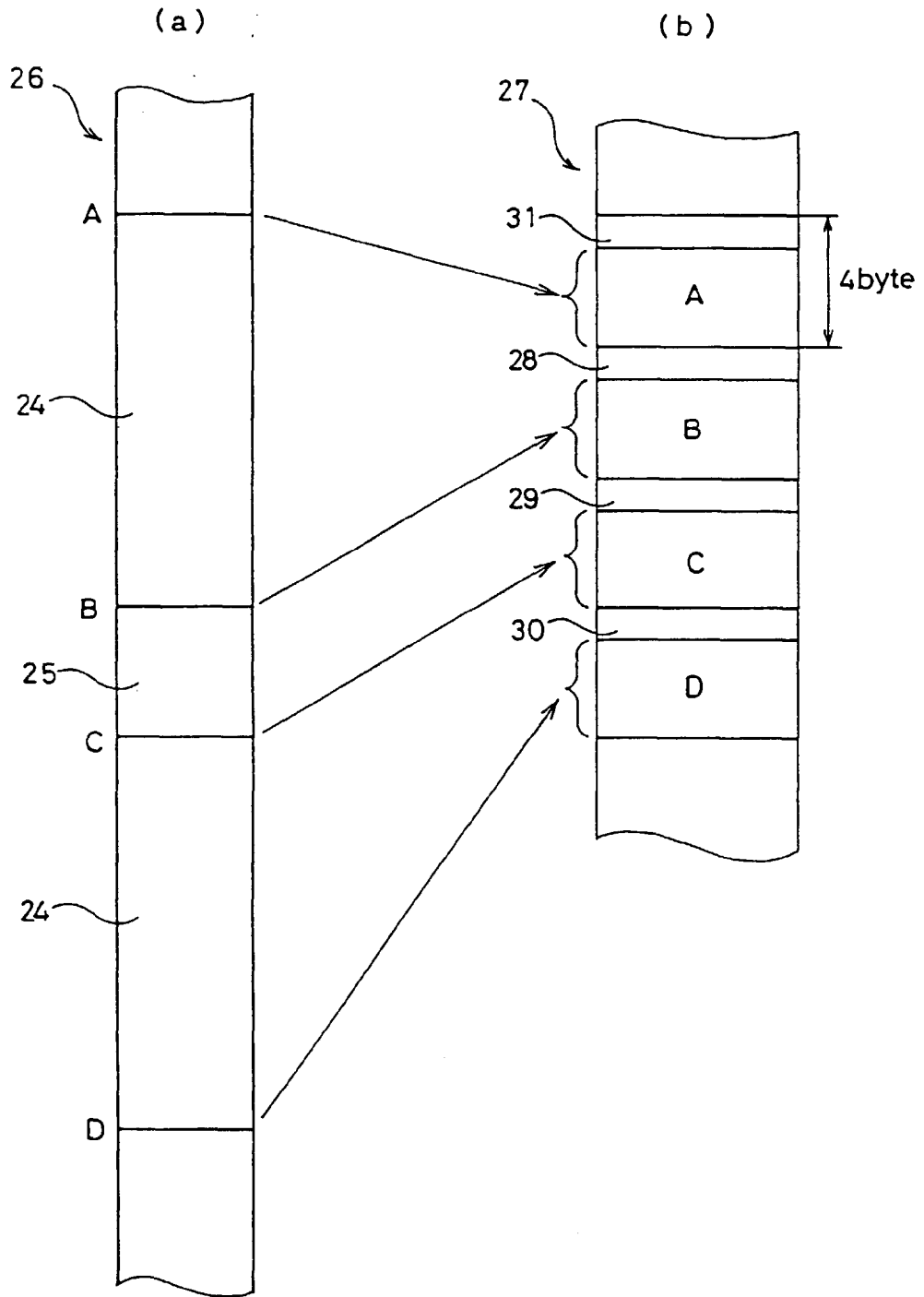


FIG. 2

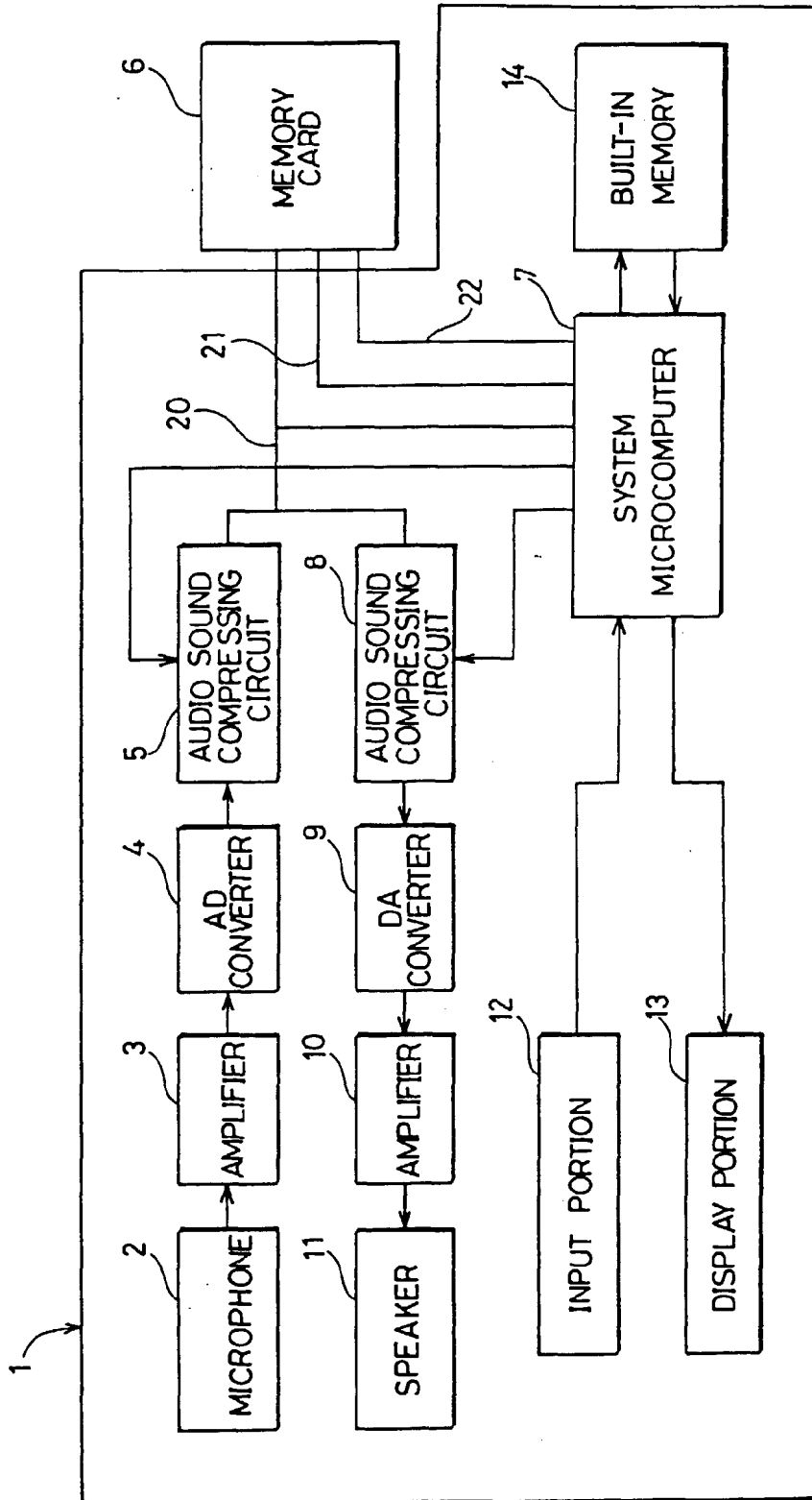


FIG. 3

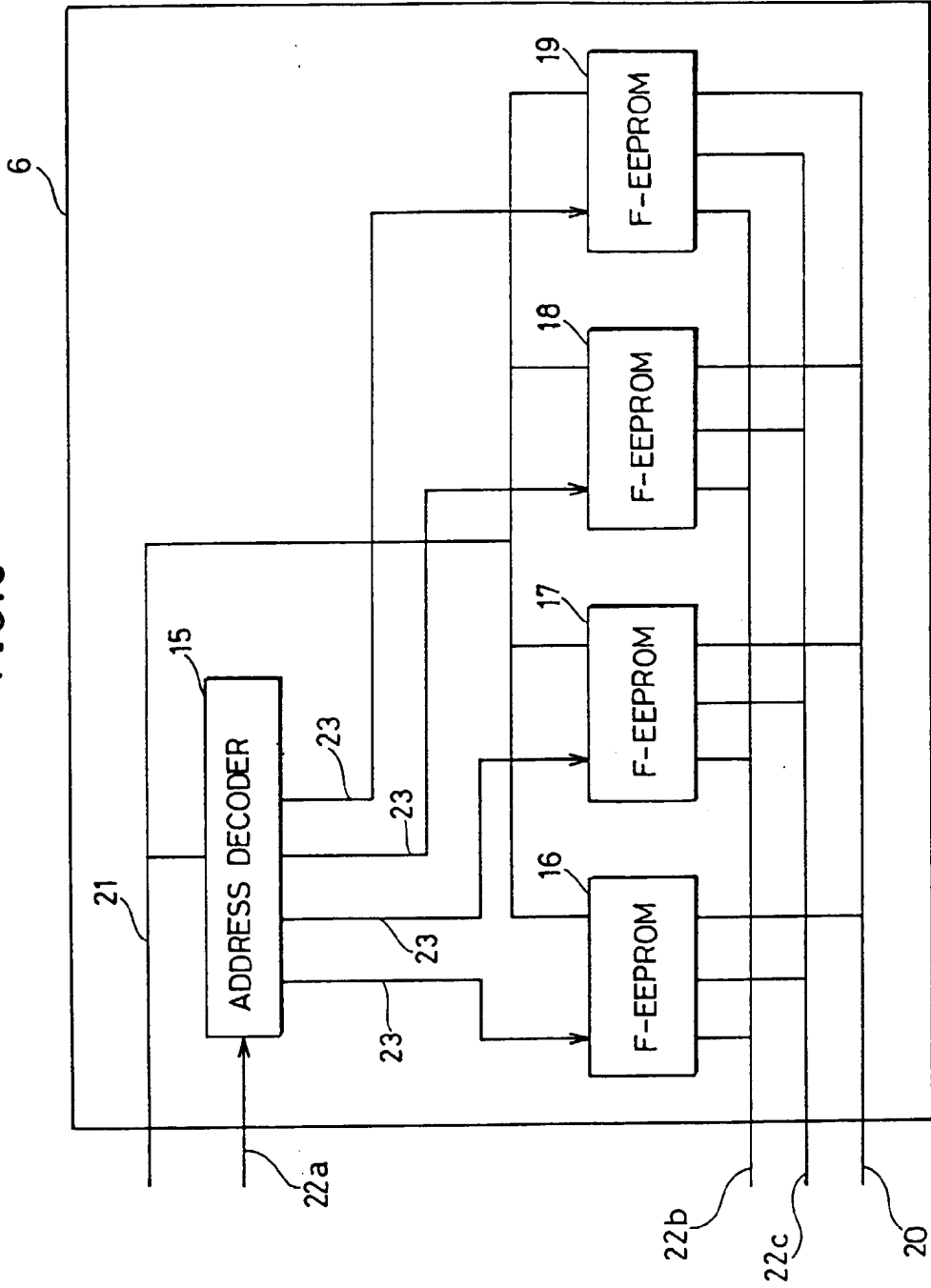


FIG.4

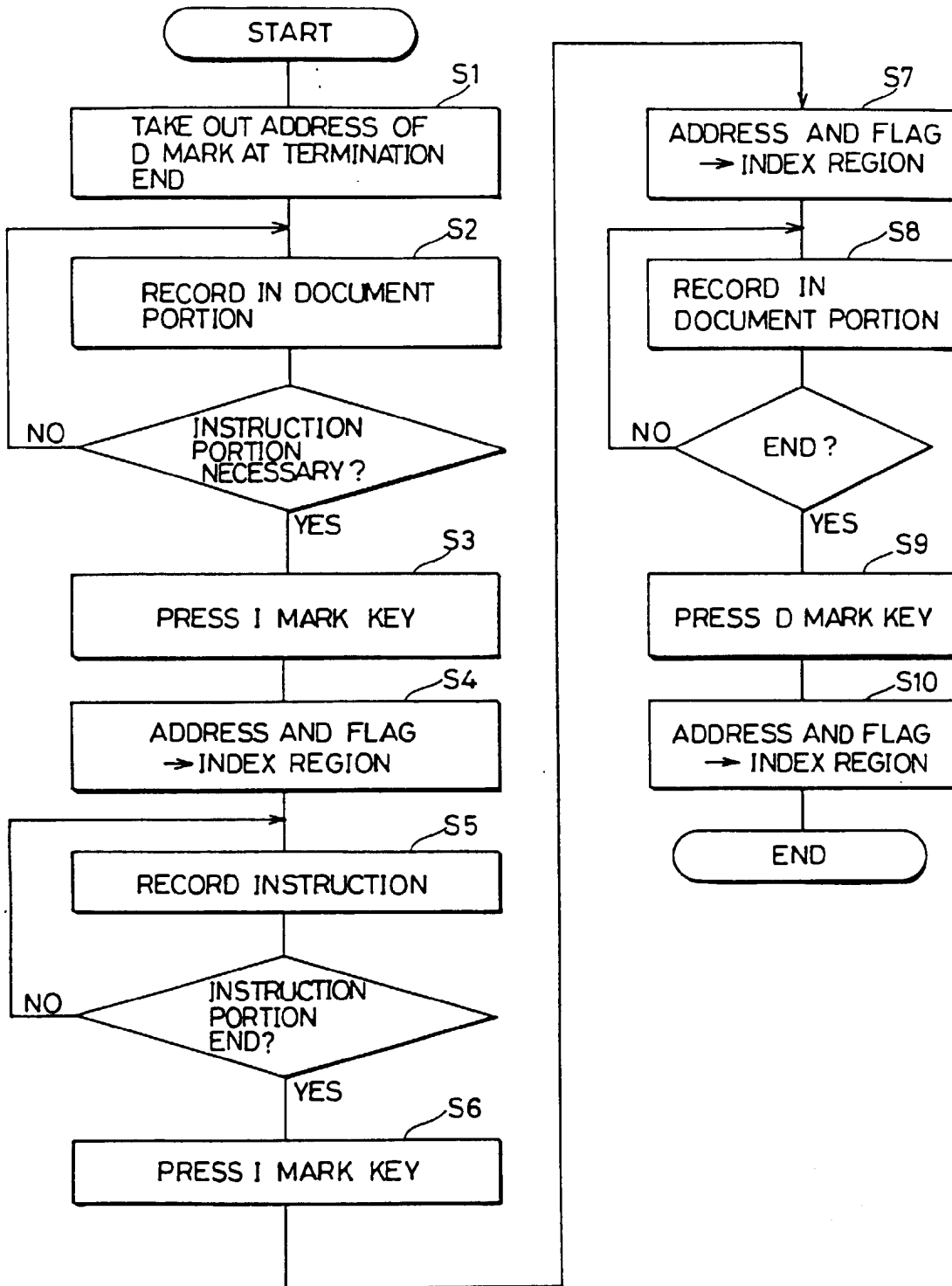
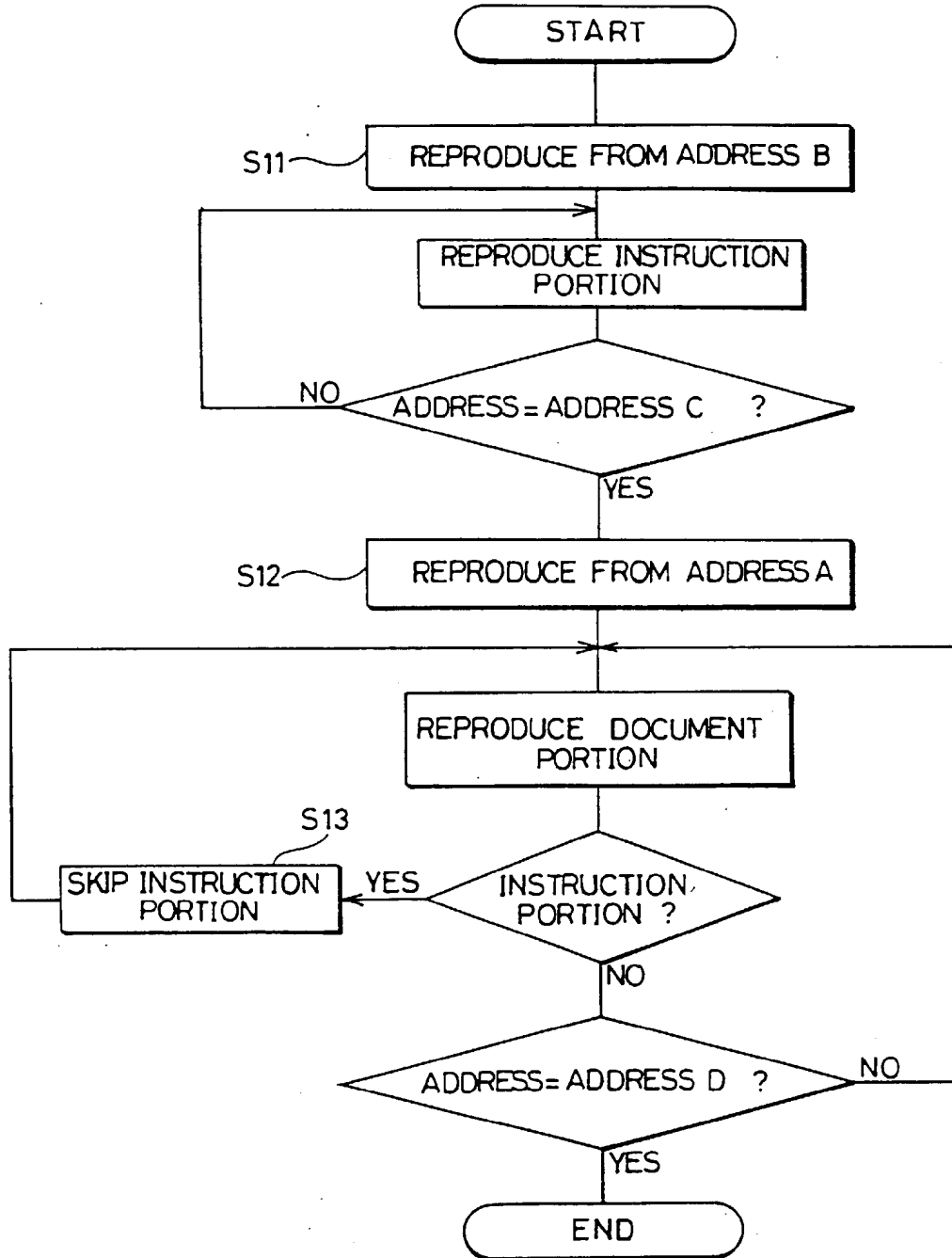


FIG. 5



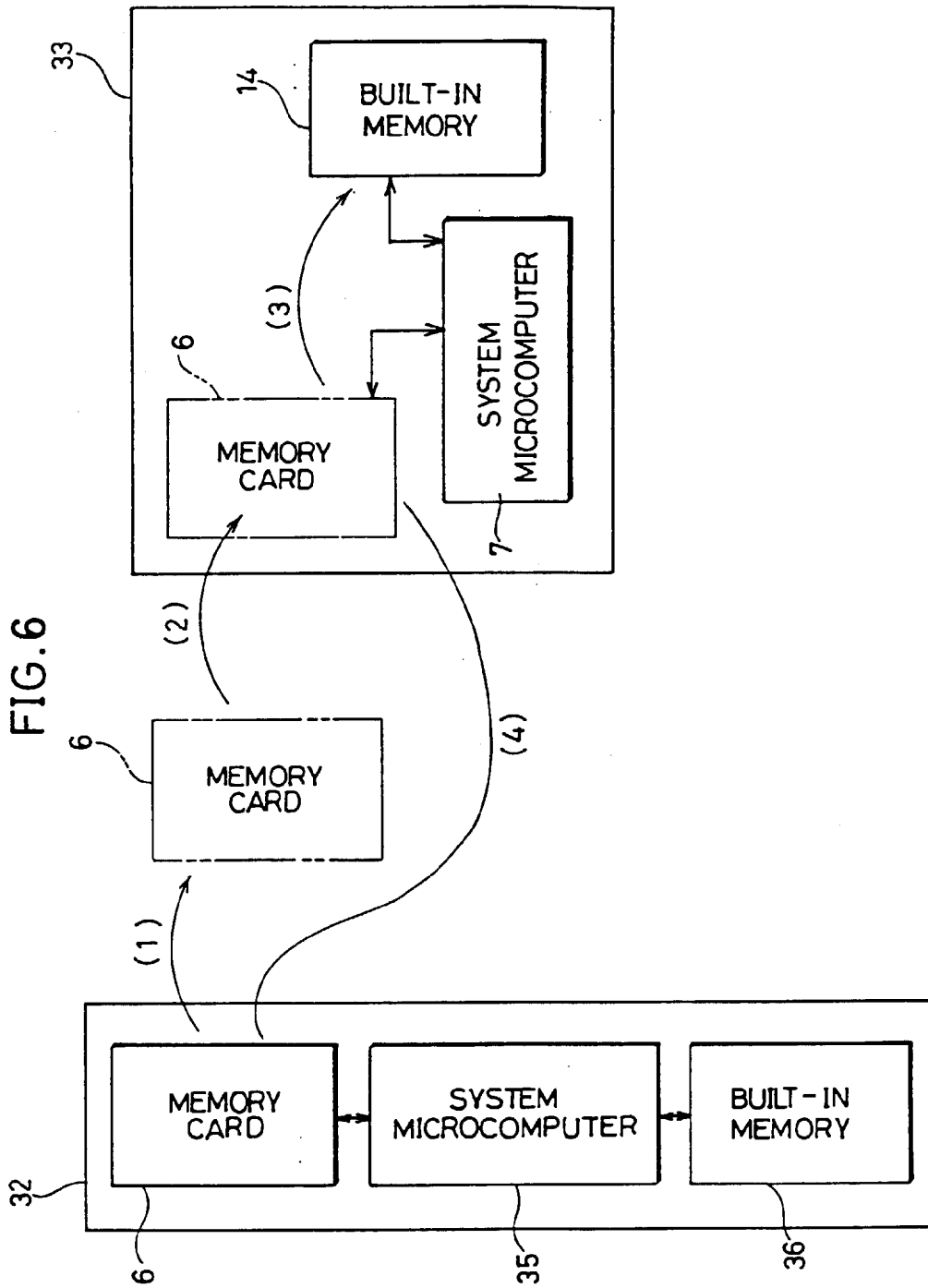


FIG. 7

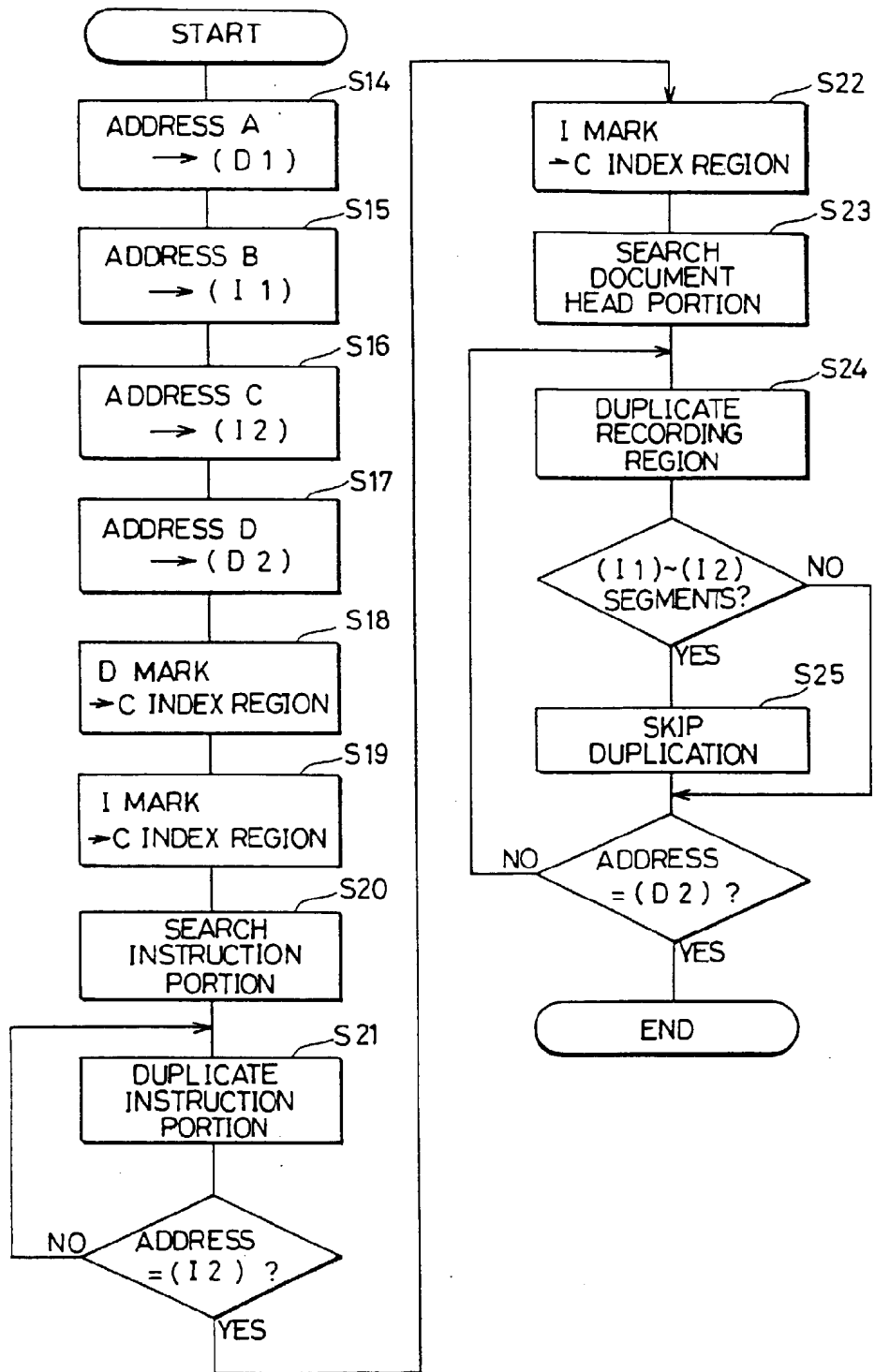


FIG. 8

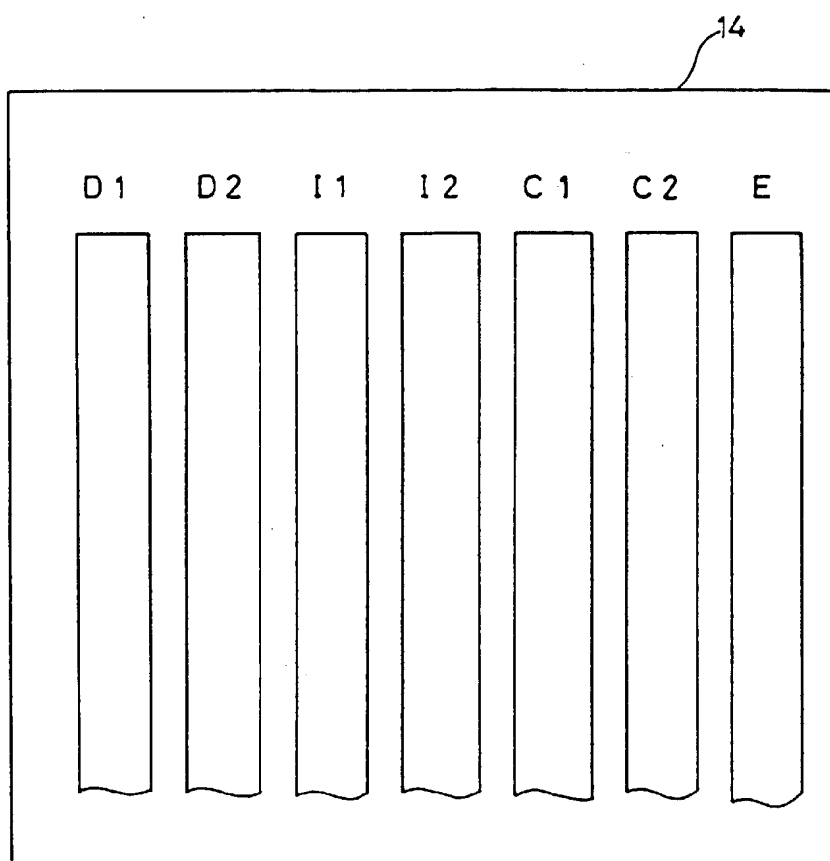
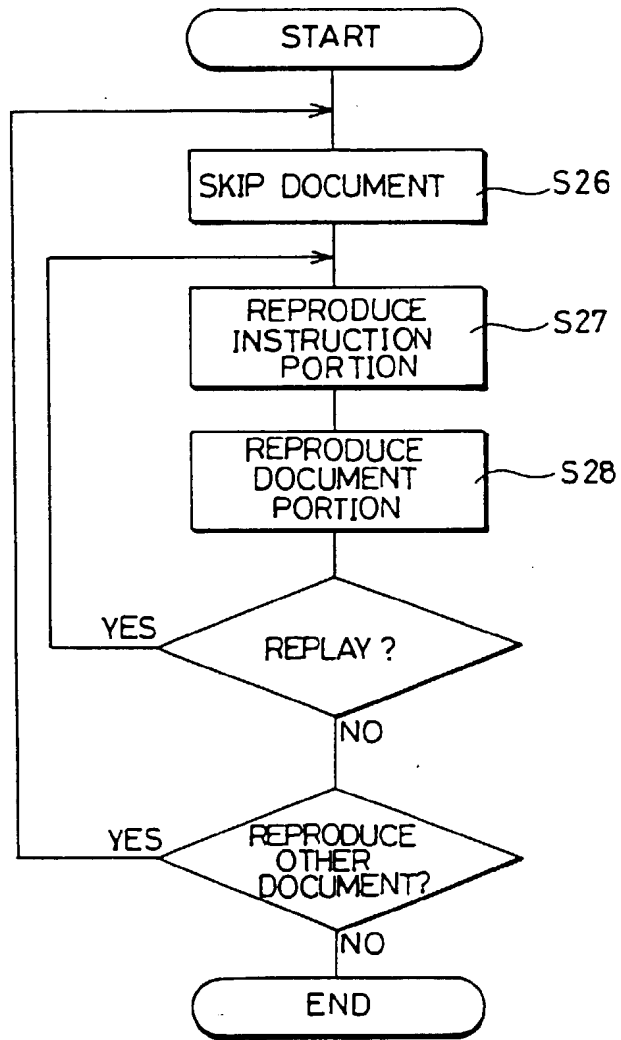




FIG.9



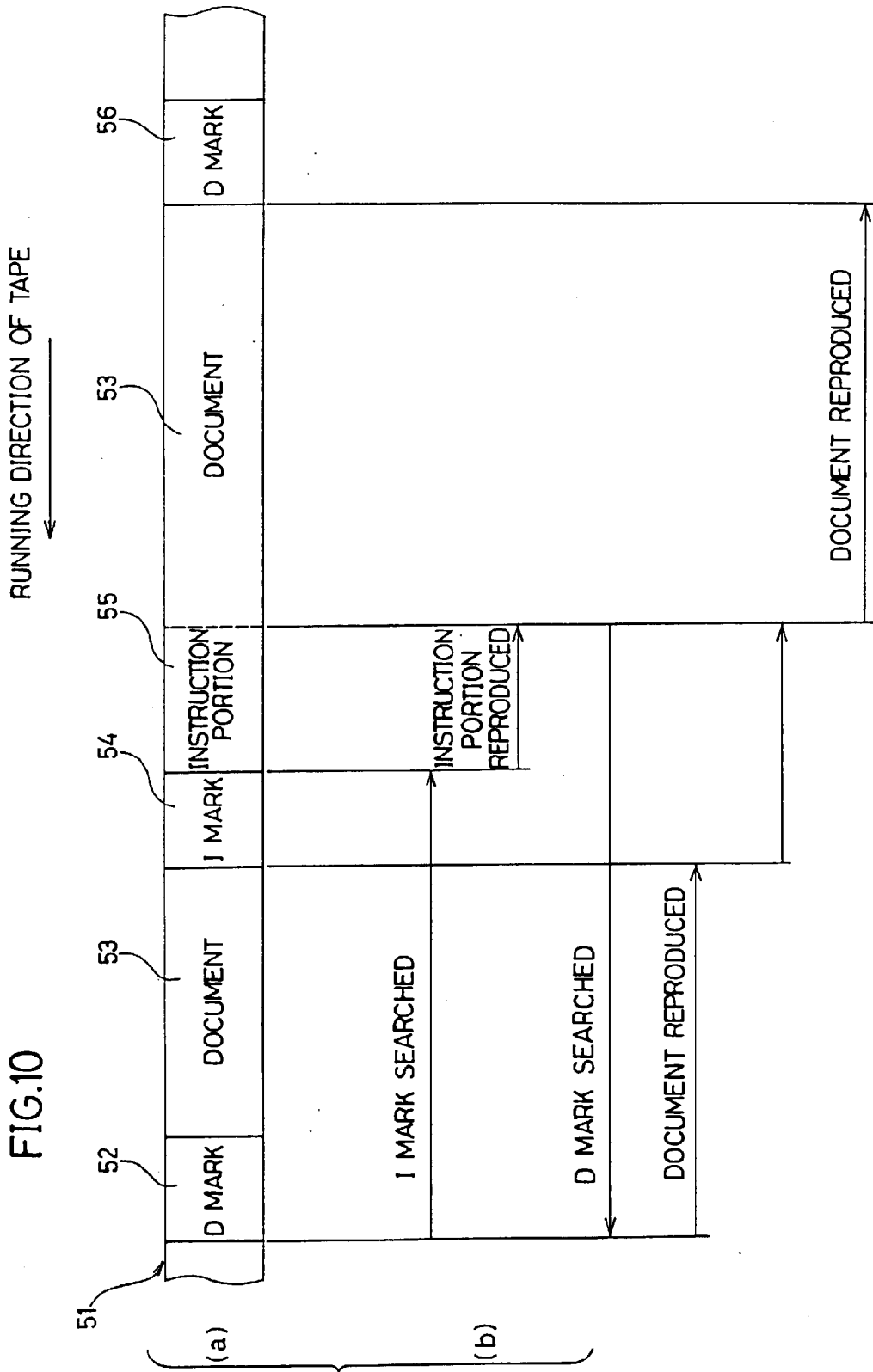
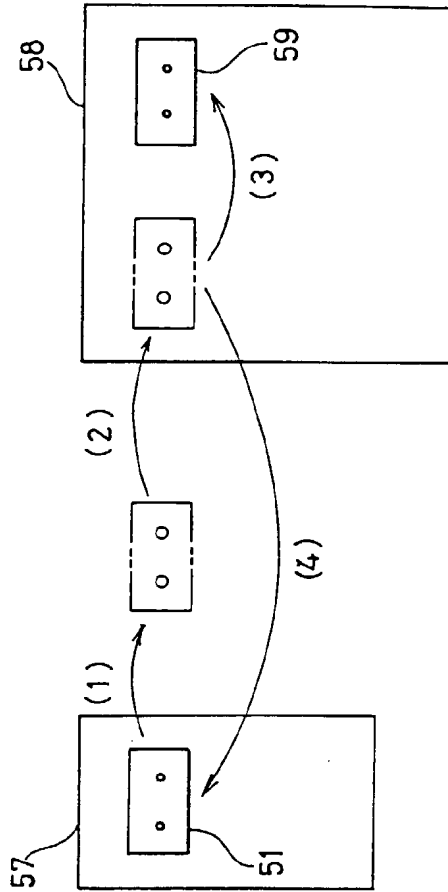
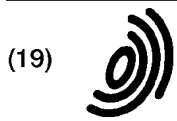


FIG.11





Europäisches Patentamt  
 European Patent Office  
 Office européen des brevets



(11) EP 0 809 221 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:  
 26.11.1997 Bulletin 1997/48

(51) Int. Cl.<sup>6</sup>: G07F 17/16, G07F 19/00,  
 G06F 17/60

(21) Application number: 97107454.7

(22) Date of filing: 06.05.1997

(84) Designated Contracting States:  
 DE FR GB NL SE

• Hejza, Leo A.  
 Sunnyvale, CA 94087 (US)

(30) Priority: 23.05.1996 US 652778

(74) Representative:  
 Zangs, Rainer E., Dipl.-Ing. et al  
 Hoffmann Eitle,  
 Patent- und Rechtsanwälte,  
 Arabellastrasse 4  
 81925 München (DE)

(71) Applicant:  
 SUN MICROSYSTEMS, INC.  
 Mountain View, CA 94043 (US)

(72) Inventors:  
 • Poggio, Andrew A.  
 Palo Alto, CA 94306 (US)

(54) Virtual vending system and method for managing the distribution, licensing and rental of electronic data

(57) A virtual vending machine manages a comprehensive vending service for the distribution of licensed electronic data (i.e., products) over a distributed computer system. The distributed computer system includes a group of client computers, a group of vendors that contribute the products to the virtual vending machine for distribution, and a server computer for operating the virtual vending machine. The virtual vending machine distributes licenses for the electronic data for the complete product or for components thereof and for a variety of time frames, including permanent licenses and rental period licenses. The virtual vending machine provides client computers with the capability to obtain information regarding the available products and the associated license fees and rental periods, to receive the product upon receipt of a corresponding electronic payment, and to reload the product during the term of the license. The virtual vending machine provides vendors with the capability of establishing a particular vending service that includes point-of-sale electronic payment and a means to communicate with the client computers to which licensed electronic data has been distributed.

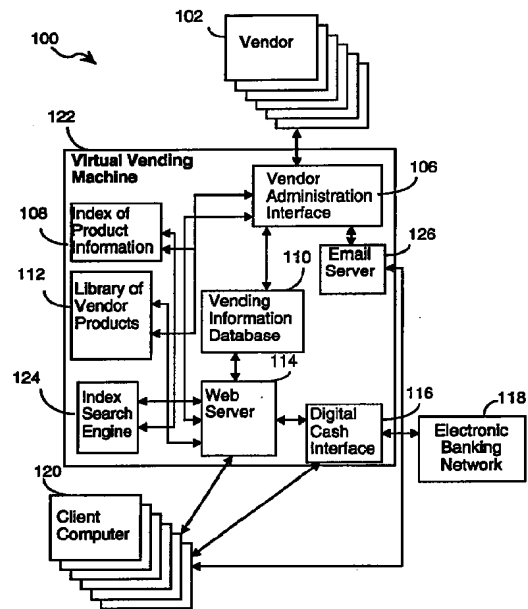


FIG. 1

EP 0 809 221 A2

## Description

The present invention relates to systems and methods for managing the distribution of licensed electronic data including the distribution of applications, application components, and computer readable data on either a permanent or time-limited rental basis.

## BACKGROUND OF THE INVENTION

The interconnection of various computer systems has provided a new medium for the distribution of computer software. Currently, networked computer systems are used to distribute computer software without any usage restrictions or a license fee. A number of "try and buy" systems also exist which enable users to try certain software programs in a limited time period without incurring a license fee. The "try and buy" systems typically limit the rights of the users of the trial versions by enclosing "time bombs" or "usage metering" schemes which limit the lifespan of the program to the trial period. The objective of the "try and buy" system is to allow the user to test the program before the user purchases it. Typically, the user can purchase the software at a retail store. Alternatively, the software can be downloaded to the user over the network and the user, in turn, mails the license fee to the vendor.

The success of these systems is due in part to the fast access that the network provides in acquiring the software. However, these systems are limited in the vending services that they provide. Specifically, the current systems do not provide any capability to acquire separate components of a software product or the capability to rent the software (or any machine transmitted information) or components thereof for a limited time period. Typically, a user acquires a license for a software product for the lifetime of the product. However, a user may have a need to use the product for a short time period with no need for it thereafter. For instance, a user may need to rent the latest version of a tax preparation software product each April. As the tax code changes annually, the user may prefer to rent the latest version of the software for one month prior to April 15th instead of purchasing the complete package each year.

Moreover, the current systems do not provide a capability for managing the redistribution (or reloading) of licensed computer software during the license period. This capability is essential for computer systems with limited or no secondary storage.

Therefore, the aim of the present invention is to account for the abovementioned limitations. Accordingly, it is a goal of the present invention to provide a virtual vending machine which fully utilizes electronic-network services in the procurement of electronic data on either a permanent or rental license basis.

It is a further goal of the present invention to provide a system and method as described above for the distribution of electronic data upon receipt of electronic payment of the associated license fee.

It is yet another goal of the present invention to provide a system and method as described above which provides a facility for reloading electronic data during the licensed period.

Another goal of the present invention is to provide a system and method which provides vendors of electronic data with a medium for distributing the electronic data to users interconnected by a communications link and to receive the appropriate license fees in an automated manner.

Other general and specific objects of this invention will be apparent and evident from the accompanying drawings and the following description.

## SUMMARY OF THE INVENTION

The present invention pertains to a virtual vending machine which manages a comprehensive electronic vending service for the distribution of licensed electronic data over a distributed computer system. The distributed computer system includes a group of client computers, a group of vendors, and at least one server computer which executes the virtual vending machine. The electronic data offered for procurement by the virtual vending machine includes any form of computer readable data that the vendor has the legal right to distribute. Further, the electronic data can be acquired as a complete product or as separate components thereof. There are also various license options available which can include procuring a license for a permanent time period or on a time-limited or rental basis.

The virtual vending machine provides the vendors with a mechanism to market, to distribute, to receive payment for the vendors electronic data, and to communicate with the users of the vendor's electronic data with minimal intervention by the vendor.

Users of the virtual vending machine are provided with a central repository of electronic data that can be procured in an expedient manner. The virtual vending machine provides the users with product information for the electronic data which details the operational requirements for the product as well as the associated license fees. The product information can be searched by the user using various keywords. Further, the electronic data can be electronically purchased by the user and repeatedly reloaded during the license period. Notifications or other announcements concerning the product are automatically forwarded to the user by the vendor.

The virtual vending machine can include several components which operate on a server computer. A vending information database is used to track the electronic data made available by the vendors and the sales transactions that occur. A Web server provides the users with Web pages (e.g., with product and pricing information) for each of the electronic data available for procurement. The electronic data is categorized by several search keywords for use by a search engine to retrieve a requested Web page. Vendors interact with a vending administration interface to establish a vending

service for their particular electronic data. Point-of-sale electronic payment is facilitated by a digital cash interface which is connected to an electronic banking network. An electronic mail server is utilized to forward communications from the vendors to the users of the vendor's electronic data.

BRIEF DESCRIPTION OF THE DRAWINGS

Additional objects and features of the invention will be more readily apparent from the following detailed description and appended claims when taken in conjunction with the drawings, in which:

Fig. 1 is a block diagram of an embodiment of a distributed computer system incorporating the present invention.

Fig. 2 is a block diagram of the virtual vending machine in a preferred embodiment of the invention.

Figs. 3A and 3B depict the vending information database used to store information about licensable products and sales information in a preferred embodiment of the invention.

Fig. 4 is a block diagram of the client computer in the distributed computer system of Fig. 1.

Fig. 5 is a schematic representation of an exemplary virtual vending machine Web page used to facilitate the distribution of the vendor products for licensing.

Fig. 6 is a schematic representation of an exemplary Web page used to obtain information on the procurement of a license for a vendor product.

Fig. 7 is a flow chart of an embodiment of the method for processing a request to license a vendor product in accordance with the present invention.

Fig. 8 is a schematic representation of an exemplary Web page used to obtain information on reloading a previously licensed product.

Fig. 9 is a flow chart of an embodiment of the method for processing a request to reload a previously licensed product in accordance with the present invention.

Fig. 10 is a flow chart of an embodiment of the method for processing service requests from the vendor in accordance with the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

For the purposes of this document, the term electronic data encompasses all forms of computer readable data, including but not limited to machine executable modules (e.g., applications, applications program, application components) and information content products (e.g., digitized video, voice data, chapter of books, and mailing lists). Further, the terms electronic data, vendor product, and product are used interchangeably.

Figs. 1 and 2 illustrate the preferred embodiment of the computer system of the present invention. Referring to Figs. 1 and 2, there is shown a distributed computer system 100 having many client computers 120. Each client computer 120 can be connected to at least one server computer 212 through a network interconnectivity means 202, preferably the Internet. The present invention is not limited to the use of the Internet as other types of communication connections can be used. While most client computers 120 are desktop computers, such as Sun workstations, IBM compatible computers and Macintosh computers, virtually any type of computer can be a client computer. One or more users (not shown) can be associated with each client computer 120. It should be noted that the present invention is not limited to a distributed computer system. It may be practiced without the specific details and may be implemented in various computer systems and in various configurations, or makes or models of tightly-coupled processors or in various configurations of loosely-coupled microprocessor systems.

In the preferred embodiment, there can be at least one specially designated server computer referred to as the virtual vending machine 122. The virtual vending machine 122 can be used to manage the distribution of electronic data and components thereof on a variety of license terms between the client computers 120 and the vendors 102. Specifically, virtual vending machine 122 can be used to provide information on the various vendor products and components thereof that are available for distribution; provide information on the associated licensing fees and rental options; receive orders for a particular product; obtain electronic payment for a particular product; distribute the particular product to the client computer 120 initially and repeatedly within the licensed period; and provide the vendors 102 with a communications channel to the licensed users of their product.

The virtual vending machine 122 can include a central processing unit (CPU) 204, a memory 210 (i.e., fast random access memory as well as non-volatile memory, such as disk storage), a user interface 206, and a communications interface 208 for communication with the client computers 120 and the vendors 102 via the communications network 202.

Referring to Figs. 1 and 2, in the memory 210 of virtual vending machine 122, there can be stored the following components:

- an operating system 214;
- Internet access procedures 216;
- web server procedures 114;
- Web pages 220;
- a vending information database 110;
- a library of vendor products 112;
- digital cash interface procedures 116;
- vendor interface administration procedures 106;
- an index of the product information 108;
- an index search engine 124;
- an encryption and formatting module 218;
- electronic mail (email) server procedures 126; and
- electronic invoices 222.

A more detailed description of these components is provided below.

In the preferred embodiment, the virtual vending machine 122 can utilize a World Wide Web Server 114 (Web Server) to facilitate the management of the vending services. The Web Server 114 interacts with the client computers 120 utilizing standard World Wide Web (WWW) protocols. However, the present invention is not limited to this particular type of information server. Other information servers can be used, such as but not limited to, gopher servers, WAIS (Wide Area Information Servers) servers, other Internet database servers, or the like.

The Web Server 114 responds to requests from users for information and orders for a vendor product. The Web Server 114 interacts with other system components in the virtual vending machine 122 in order to process the user's request. The virtual vending machine 122 can include a vending information database 110, a library of vendor products 112, a vendor administration interface 106, an index search engine 124, and a digital cash interface 116. The vending information database 110 can contain product and sales information for each available vendor product. The library of vendor products 112 can be a repository for the available vendor products. The vendor administration interface 106 can interact with the vendors 102 in establishing a particular vending service for the vendor's products. The index search engine 124 can be used to perform searches on the available vendor products offered by the virtual vending machine 122. The digital cash interface 116 can provide the point-of-sale cash payment for the license fees associated with the vendor products. A more detailed description of each of these components will be presented below.

The distributed computer system 100 can be linked to numerous vendors 102 which provide the virtual vending machine 122 with products for distribution to the users associated with the client computers 120. The vendors can be any party in communication with the network 202 and who has the right to legally distribute the electronic data. Accordingly, the vendor can be a user associated with a client computer 120, a user associated with a server computer 212, online information service providers, or any other type of licensed dis-

tributor.

The vendors 102 interact with the virtual vending machine 122 through a vendor administration interface 106. The vendor administration interface 106 services requests from the vendors 102 which can include: requests to establish a vending service (i.e., make a vendor product available for distribution, license or rent, by the virtual vending machine); requests to update a vending service (i.e., update the vendor product and/or its documentation); requests to discontinue a vending service; and requests to communicate with the users of the vendor's product.

The distributed computer system 100 can further include a digital cash interface 116 for obtaining point-of-sale electronic payment for the license fee associated with a particular vendor product. The digital cash interface 116 is connected to an electronic banking network 118 which is a communications link to financial institutions such as banks, automatic clearing houses, and the like. Digital cash interface 116 interacts with the user and the virtual vending machine 122 in obtaining the pertinent payment information and forwards the transaction to the appropriate financial institution through the electronic banking network 118.

Digital cash interface 116 can be a digital cash server such as the CyberCash server. However, the present invention is not limited to this type of point-of-sale electronic payment scheme. Others can be used which provide an appropriate point-of-sale electronic payment method, which can include but is not limited to, such systems as First Virtual Holdings, DigiCash, Checkfree, and the like. Further, the present invention is not constrained to credit card payment transactions but can include all forms of electronic payment, including but not limited to, debit transactions, electronic funds transfer, and other types of cash transactions.

Figs. 3A and 3B depict the structure of the vending information database 110 in the preferred embodiment. The vending information database 110 maintains product information for each vendor product that is offered by the virtual vending machine 122 and tracks sales data for each product purchased. The vending information database 110 contains an entry 302 for each vendor product and can contain the following information:

- a product identifier 304, which can be any alphanumeric character string (such as the product name) that uniquely identifies the product;
- the number of copies of the vendor product available for sale or rental 306 (i.e., the number of licenses authorized by the product's vendor, minus the number of licenses granted so far);
- a pointer to the location of the vendor product in the library of vendor products 308;
- product information 310 which can include the following information:
  - \* vendor information 312, which contains data on the particular vendor which supplied the vendor

- product, preferably the vendor's name and network address;
- \* Web pages 314, which provide information on the product including but not limited to a general description, the version number, hardware and software requirements and restrictions, and the like; and
  - \* category and keywords 316, which denote classifications that are used in referencing and searching the vendor products available in the virtual vending machine 122;
- sale and/or rental license fee schedules 318, which indicate the licensing fees for the vendor product and the separately-acquired components on a purchasable and/or rental basis;
  - a schedule of components 320 that are part of the vendor product and can be purchased or rented independently;
  - sales information 322, which can include an entry for each license of the vendor product 302 purchased through the virtual vending machine 122, where each entry 324 can include the following:
    - \* license number 326;
    - \* buyer identifier and security code 328, which uniquely represents the buyer;
    - \* product option 330, which indicates the particular product and/or component acquired;
    - \* purchase option 332, which indicates whether the particular product and/or component was purchased or rented;
    - \* reload count 334, which is a count of the number of times the product has been redistributed to the user within the rental or license period;
    - \* time stamp 336; and
    - \* network address 338, which indicates the network address of the buyer.

Referring to Figs. 2 and 3, there is an indexing structure known as the index of product information 108 which is associated with the Web pages for each vendor product. The index 108 is used to provide quick access to reference or search information on the various vendor products available for license by the virtual vending machine 122. As vendor products and their associated Web pages are inserted and deleted into the vending information database 110, the index structure 108 is updated to reflect the change. The indexing structure 108 is used by the index search engine 126 in response to requests by the user and will be described in more detail below.

It should be noted that the present invention is not constrained to this particular design or format of the vending information database 110 and the index 108. Alternate database formats and indexing structures can be utilized so long as they provide similar functionality.

Referring to Fig. 4, there is shown a block diagram

of the client computer 120 in the distributed computer system 100. The client computer 120 can include a central processing unit (CPU) 402, a user interface 404, a memory 408, and a communications interface 406 for communication with the virtual vending machine 122 via the communications network 202. The memory 408 of the client computer 120 can be used to store the following:

- operating system 410;
- Internet access procedures 412;
- web browser 414;
- client encryption keys 416;
- decryption module 418 for decoding encrypted electronic data received from the virtual vending machine; and
- a repository of rented and purchased vendor products 420.

Referring to Fig. 5 there is shown a schematic representation of an exemplary virtual vending machine home Web page 220 of the Web server 114, accessible by a user using client computer 120. The Web page 220 includes menu selection buttons for: searching the various categories of vendor products 506; viewing information about the available vendor products 508; viewing the licensing fee schedules for the vendor products 510; initiating the purchase of a license for a vendor product on a permanent or limited time period basis 512; requesting the reloading of a previously acquired vending product 514; requesting access to various vendor services 516; and obtaining help on the virtual vending machine 518.

The vendor products can be classified into categories 502. The categories 502 can be classified by product types (e.g., compilers, Java applications, Web browsers, screen savers, digitized music scores, video data, device drivers, or non-software categories such as books, still photos, phone directories, music, movies, etc.), by vendors (e.g., Microsoft, Sun, IBM, etc), or any other classification scheme. Associated with each category can be menu buttons displaying the particular category 502. For each category, there can be a corresponding selection button for the title of each vendor product within the category 504. It should be noted that the present invention is not limited to the particular design depicted in the exemplary Web page. Others can be used which provide similar functionality.

If the user wants to perform a search of the various vendor products or categories that are available, the user selects the perform category search menu button 506. A search Web page (not shown) will be downloaded to the user which will guide the user on the available search capabilities and search keywords. The index search engine 126 will receive the user's search criteria and perform the search utilizing the index of the product information 108.

If the user wants to access information describing a particular product, the user selects the button 504 cor-



responding to the title of the product and the view product information menu button 508. A first Web page (not shown) associated with the selected product is then downloaded to the user. Subsequent Web pages of product document are accessed by the user using standard hypertext linking provided by the client computer's Web browser and hypertext links in the product documentation.

Similarly, if the user chooses to access the license fee schedule for a particular product, the user selects the button 504 corresponding to the title of the product and the menu button 510 for viewing the license fee schedule. Another Web page (not shown) is then transmitted to the user which contains the license fee schedule for the particular product.

Fig. 6 is an exemplary Web page 600 for the purchase or rent of a selected product. The Web page 600 can be accessed by selecting the button for the title of the vendor product 504 and the purchase / rent product menu button 512. Fig. 7 is a flow chart depicting the method 700 executed by the web server 114 in response to a user's order initiated through Web page 600. Referring to Figs. 6 and 7, the Web page 600 can contain menu buttons which select the product and license options that the user prefers. By selecting menu button 602 the user selects the license option (i.e., to purchase a permanent license to the specified product) and by selecting menu button 604 the user selects the rent option. For the purposes of this document, the license purchase option indicates that a license for the product is acquired in perpetuity. The rent option indicates that a license for the product is acquired for a limited time period.

Web page 600 can also contain menu buttons for indicating the following:

- whether the entire product 606 is being licensed, or just specified components thereof 608;
- the expiration date of the rental period 610, if the rental option 604 is selected;
- a buyer identification and security code 612;
- the total license fee 618; and
- an explicit verification of the sale by the user 620.

The user selects the appropriate menu buttons and enters the appropriate information in the displayed fields which is received by the web server 114 (step 702). The method proceeds to verify that a license is available for the desired license option by checking the number of available licenses 306 in the vending information database 110 (step 704). If no licenses are available (i.e., the stock of authorized licenses has been depleted), the method informs the user that the virtual vending machine is temporarily out-of-stock of licenses for the particular product (step 706).

Otherwise (step 704-Y) the method proceeds to collect a form of electronic payment for the license fee (step 710). Preferably, the web server 114 forwards an invoice 222 to the user associated with a client compu-

ter 120. The user adds a credit card number (or other form of payment authorization) to the invoice, which is then encrypted and forwarded back to the web server 114. The web server 114 attaches a confirmation number to the invoice and the entire invoice is encrypted and transmitted to the digital cash interface 116. The digital cash interface 116 reformats the invoice into the appropriate format for transmittal to the electronic banking network 118 which processes the transaction.

The digital cash interface 116 awaits for an indication from the electronic banking network 118 signifying successful completion of the payment transaction (i.e., credit card or electronic funds transfer transaction). This indication is forwarded to the web server (step 712). If the payment transaction fails (714-N), the user is so informed and the purchase transaction is aborted (715). If the payment transaction was successful (714-Y), the method decrements the count of the available licenses 306 in the vending information database 110 (step 716). If the remaining number of available licenses 306 is zero (or less than zero), the method informs the vendor that additional licenses are needed (step 716).

The method then proceeds to format the purchased product for transmission to the user (step 718). Preferably, rental products are formatted to include a time bomb or other disabling device which will disable the product at the end of the rental period. In addition, the formatted product is encrypted before it is transmitted to the user utilizing the encryption and formatting module 218. The product can be encrypted utilizing any of the well-known encryption techniques, such as but not limited to DES, RSA, and the like. More generally, the product is encrypted so that it can be decoded only by the user or client who paid for the product. Lastly, the sale is recorded in the sales information entry 322 of the vending information database 110 (step 720).

The user's system decodes the received electronic data product using its decryption module 418 and stores the licensed electronic data in its repository 420.

In alternate embodiments, the payment transaction could be handled in other ways, depending on the electronic payment methods that are commercially available. For instance, the virtual vending machine could request that the requesting user pay it a specified amount of funds, after which the user would perform a separate transaction, using an appropriate electronic banking network or service provider, to pay the specified funds to the virtual vending machine. The virtual vending machine, upon receipt of confirmation from the electronic banking network or service provider that the payment had been made, would then transmit the electronic data to the client computer.

Referring back to Fig. 5, another vending service offered to the user is that of reloading. Reloading is the retransmission of a previously purchased product within the licensed or rental period. This option is highly desirable to users associated with client computers 120 that have minimal or no secondary storage (i.e., non-volatile

storage such as disk storage). The main memory of the user's computer may not provide a suitable alternative to store the licensed product. The reloading option is chosen by selecting the buttons for the appropriate title for the product 504 and the reload menu button 514.

Fig. 8 depicts an exemplary Web page 800 which illustrates the required information for requesting a reload of a vendor product and Fig. 9 illustrates the method 900 for performing the reload function. Referring to Figs. 8 and 9, a user enters his/her buyer identification 802 and security code 804 and indicates the desired product 806 and/or component(s) to be reloaded 808. The Web server 114 receives this information (step 902) and proceeds to check whether the user has a current license for the specified product. This check can be made by searching the sales information 322 stored in the vending information database 110 (step 904). If the check indicates that there is no current license for the requested reloaded product by the user, the process informs this to the vendor (step 906).

Otherwise, the product is formatted for transmission to the user and then transmitted (step 908) as previously described in reference to Fig. 7, and the reload count 334 in the vending information database 110 is updated to reflect this additional retransmission (step 910). The number of reloads for a particular user and product is tracked in the event the vendor requests such information.

Referring once again to Fig. 5, another function provided by the virtual vending machine 122 is to service vendor requests, which is invoked by the selection of menu button 516. These requests can be for the establishment of a vending service, to discontinue a vending service for a product, to update a product or its documentation, to authorize additional licenses, or to channel a communication to the users of a product through electronic mail. For the purposes of this application it is assumed that the vendor has the right to legally distribute the product. When a vendor selects this service, the web server 114 transmits to the vendor a Web page (not shown) which informs the vendor of the various vendor services that are provided and the appropriate information that is required to perform the service. The vendor, in turn, transmits to the Web server 114 the required information and the vendor administration interface 106 services the request.

Fig. 10 is a flow chart illustrating some of the steps the vendor administration interface 106 can take in servicing the vendor's requests. Preferably, the vendor administration interface 106 is a server process that monitors requests from the vendors (step 1002). Upon receipt of a request, the vendor administration interface 106 proceeds according to the type of request (step 1004). For a request to establish a vending service (i.e., add a vendor product to the virtual vending machine), the vendor administration interface 106 can receive from the vendor the following information:

- product identifier;

- the number of copies for sale and for rent;
- the vendor products and separately-acquired components thereof;
- vendor information such as vendor id and network address;
- category and search terms for each of the vendor products;
- Web pages describing the product; and
- sale and rental license fees.

The vendor administration interface 106 prepares an entry for this product in the vendor information database 110 based on the information received (step 1006). The product and components thereof are inserted into the library of vendor products 112 and the index of the product information 108 is updated accordingly (step 1014).

For a request to discontinue a vendor product, the vendor administration interface 106 can receive from the vendor the product and vendor identifier. The vendor administration interface 106 deletes the products and components thereof from the library of vendor products 112 and from the index of product information 108 (step 1008), deletes the entry for this product in the vendor information database 110, and updates the index of product information accordingly (step 1018).

If a vendor's request is to authorize the addition of more licenses, the vendor administration interface 106 updates the vending information database 110 for the product with the additional number of licenses 306 (step 1010).

Furthermore, the vendor can communicate with the users of the product through the virtual vending machine's email server. For example, a vendor can request the distribution of a notification to all or some of the licensed users of a product (e.g., to distribute an announcement for an update or new version of the vendor product). In this case, the vendor administration interface 106 receives the notice and the notification criteria and formats a mailing list of the licensed users (step 1012). The mailing list and the notice is forwarded to the email server 126 which formats the message and distributes it to the appropriate users (step 1022).

The vendor administration interface 106 and digital cash interface 116 can be used to periodically send sales information and associated payments to the product vendors.

The above mentioned system and method describes a virtual vending machine which provides a comprehensive vending service for the distribution of any form of electronic data (i.e., vendor product) over a network of interconnected computer systems. The virtual vending machine is beneficial since it provides fast access to the latest version of electronic data. It also provides the ability to acquire components of a vendor product and to acquire the product or components thereof on a rental basis. From the vendor's perspective, the virtual vending machine is advantageous since it provides a means to market the product, a means to

communicate with the licensed users, and a means to receive payment with minimal intervention by the vendor. From the users perspective, the virtual vending machine is advantageous in providing a central repository for obtaining the latest version of a product and to acquire the associated license for a preferred duration. The reloading capability is distinctly useful since it provides the users with the capability of accessing the product as often as needed during the license period.

While the present invention has been described with reference to a few specific embodiments, the description is illustrative of the invention and is not to be construed as limiting the invention. Various modifications may occur to those skilled in the art without departing from the true spirit and scope of the invention as defined by the appended claims.

Further, the method and system described hereinabove is amenable for execution on various types of executable mediums other than a memory device such as a random access memory. Other types of executable mediums can be used, such as but not limited to, a computer readable storage medium which can be any memory device, compact disc, or floppy disk.

#### Claims

1. A method for managing a virtual vending machine for procuring electronic data over a distributed computer system for a plurality of rental periods, the distributed computer system comprising of a plurality of vendors, a plurality of clients, and at least one server interconnected by a communications link, said method comprising the steps of:

obtaining the electronic data from the vendors for distribution by the virtual vending machine to the clients;  
receiving a request from one of the client to acquire one of the electronic data for rental during one of the rental periods;  
procuring electronic payment for the electronic data from the client; and  
upon successful receipt of the electronic payment, transmitting the electronic data to the client via the communications link.

2. The method of claim 1,  
receiving a request from the client to retransmit the electronic data;  
upon verifying that the rental period associated with the requested electronic data has not expired, retransmitting the requested electronic data to the client without obtaining additional electronic payment.

3. The method of claim 1,  
said electronic data transmission step including modifying the electronic data so as to automatically disable use of the electronic data

upon expiration of the rental period, and encrypting the modified electronic data prior to transmission thereof to the one client so as to disable use of the electronic data by clients other than said one client.

4. The method of claim 1,  
receiving a communication from one of the vendors for distribution to a set of clients that have acquired the electronic data; and  
transmitting the communication to the set of clients.

5. The method of claim 1,  
wherein the electronic data comprises information content products and machine executable modules.

6. The method of claim 1,  
prior to said receiving step, providing the one client with rental pricing information.

7. A method for distributing products over a network of computer systems, said network comprising a virtual vending machine for distributing the products, and a plurality of users for acquiring the products, said method comprising the steps of:

transmitting the products to the virtual vending machine from vendors connected to the network;  
transmitting a request to the virtual vending machine from one of the users to rent one of the products during one of a plurality of rental periods;  
procuring electronic payment for the rental of the product; and  
transmitting the product to the user upon completion of the electronic payment.

8. The method of claim 7,  
upon request by the user, retransmitting the product to the user within the rental period.

9. The method of claim 7,  
said product transmission step including modifying the product so as to automatically disable use of the product upon expiration of the one rental period, and encrypting the modified product prior to transmission thereof to the one user so as to disable use of the product by users other than said one user.

10. The method of claim 7,  
transmitting communications from one of the vendors to a set of the users that have received the vendor's product.

11. The method of claim 7,  
prior to said step of transmitting a request to

the virtual vending machine from the one user, transmitting rental pricing information to the one user.

12. The method of claim 7, 5  
 wherein the products comprise information content products and machine executable modules.
13. A virtual vending machine for managing the procurement of licenses for vendor products on a distributed computer network, said distributed computer network comprising a plurality of client computers in communication with the virtual vending machine and a plurality of vendors contributing the vendor products for distribution by the virtual vending machine, said virtual vending machine comprising: 10  
 15  
 a memory device for storing the vendor products, a subset of the vendor products each comprising a complete product having components available for individual licensing, wherein a subset of said vendor products and components are available for licensing by users associated with the client computers on a permanent basis and on a limited time period rental basis; 20  
 a processor for executing a server process, the server process for managing the procurement of licenses for the vendor products and components; and 30  
 a communications link to an electronic funds provider and to the client computers for acquiring payment for the licenses and for transmitting the licensed vendor products and components to the client computers upon receipt of the payment. 35
14. The virtual vending machine of claim 13, 40  
 wherein the server process stores and provides access to product information for the vendor products available for procurement by the virtual vending machine.
15. The virtual vending machine of claim 13, 45  
 wherein the server process stores and provides access to licensing fee information for the vendor products available for procurement by the virtual vending machine. 50
16. The virtual vending machine of claim 13, including: 55  
 an electronic mail server, executable by said processor, for providing communications between a specified vendor and selected client computers that have previously acquired licenses for a vendor product associated with the specified vendor.

17. The virtual vending machine of claim 13, a vendor administration interface, executable by said processor, for managing requests by the vendors for service by the virtual vending machine in the distribution of the vendor's vendor products.

18. The virtual vending machine of claim 13, including:

formatting and encryption instructions, executed by said processor, for modifying the vendor products so as to automatically disable use of the vendor products upon expiration of specified rental periods, and encrypting the modified vendor products data prior to transmission thereof to respective ones of the client computers so as to disable use of the electronic data by other ones of the client computers.

19. A computer readable storage medium configured to direct the operation of a server computer to manager the distribution of electronic data in a distributed computer system, the distributed computer system comprising of a plurality of client computers having users associated therewith and at least said one server computer, said computer readable storage medium comprising:

a server for managing the distribution of electronic data to the client computers, said server providing the client computers with product information on the electronic data, for procuring orders for the electronic data, and for transmitting the electronic data to the client computers; a library for storing the electronic data; a vending information database for storing the product information on the electronic data available for distribution over the distributed computer system, said electronic data available for distribution for a plurality of license fees, each license fee having an associated time period for which use of the electronic data is authorized; a vendor administration interface for acquiring the electronic data from a plurality of vendors connected to the distributed computer system; and a digital cash interface, coupled to the server and an electronic banking network, for obtaining point-of-sale electronic payment of the license fee associated with licensing use of the electronic data for a specified time period.

20. The computer readable storage medium of claim 19, including:

an index of the product information stored in the vending information database; and an index search engine, utilizing said index of the product information, for allowing users to

search the electronic data using various key-words.

21. The computer readable storage medium of claim 16,

an electronic mail server for providing electronic communication between the vendors and the client computers.

5

10

15

20

25

30

35

40

45

50

55

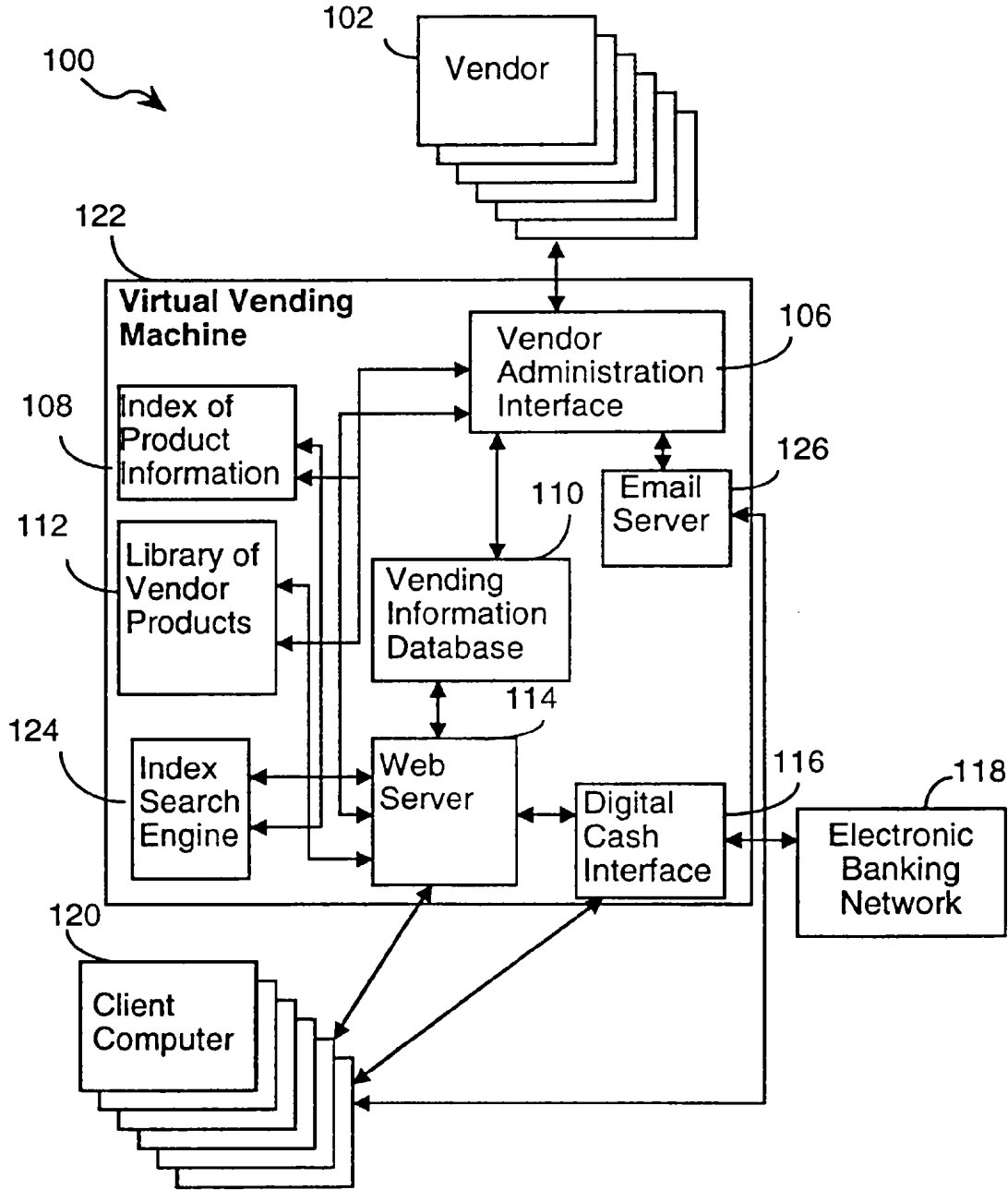


FIG. 1

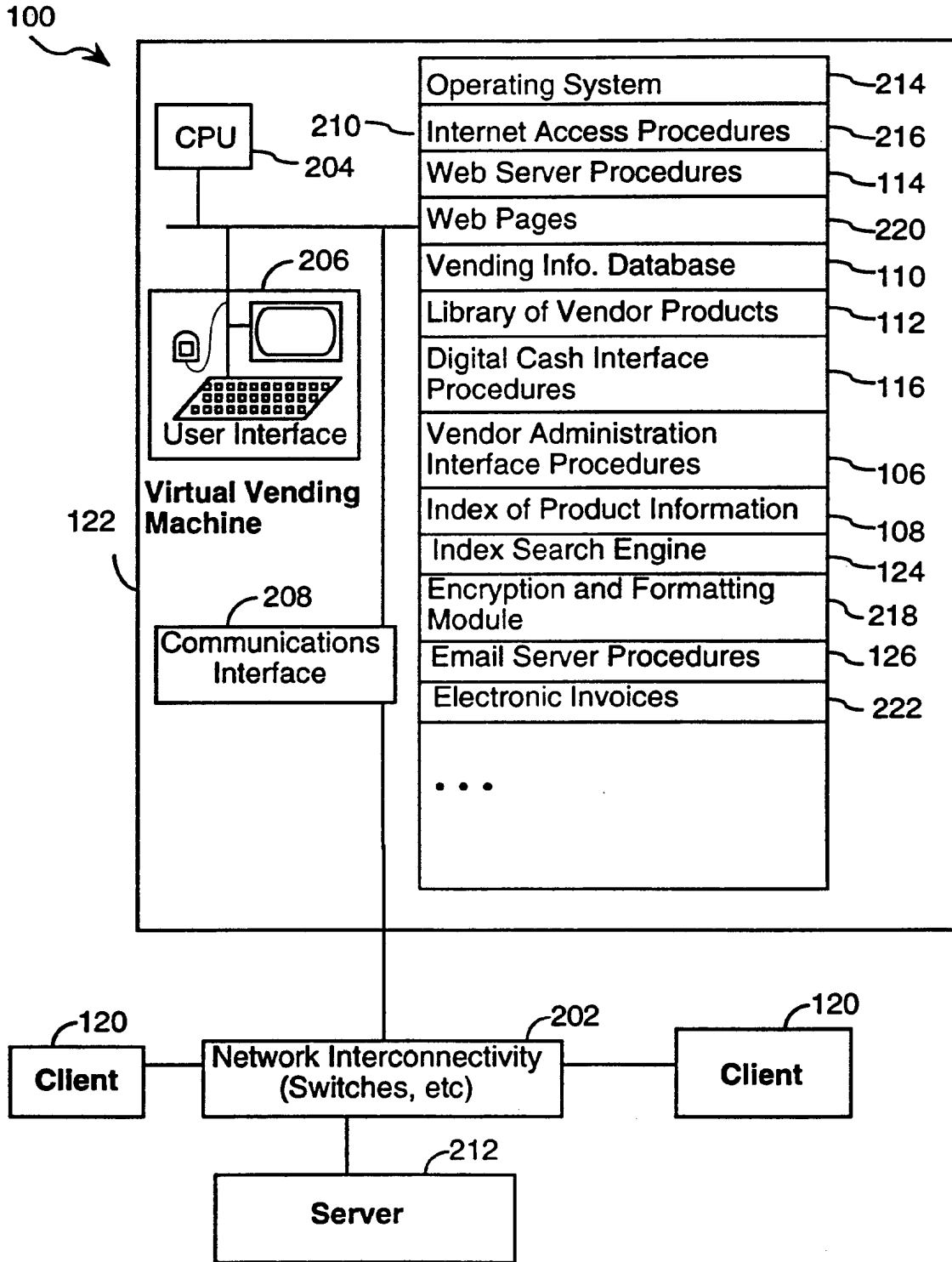


FIG. 2

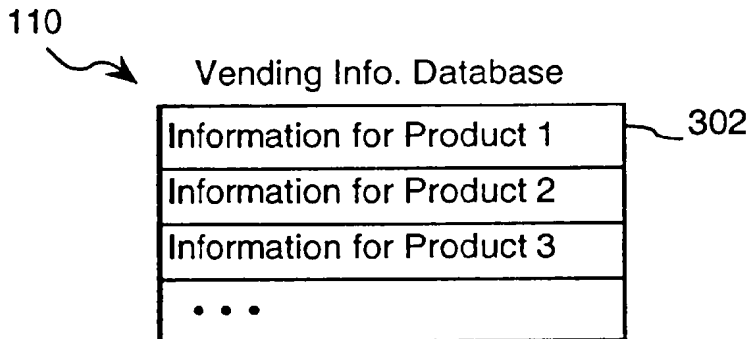


FIG. 3A

Information for Product 1

302

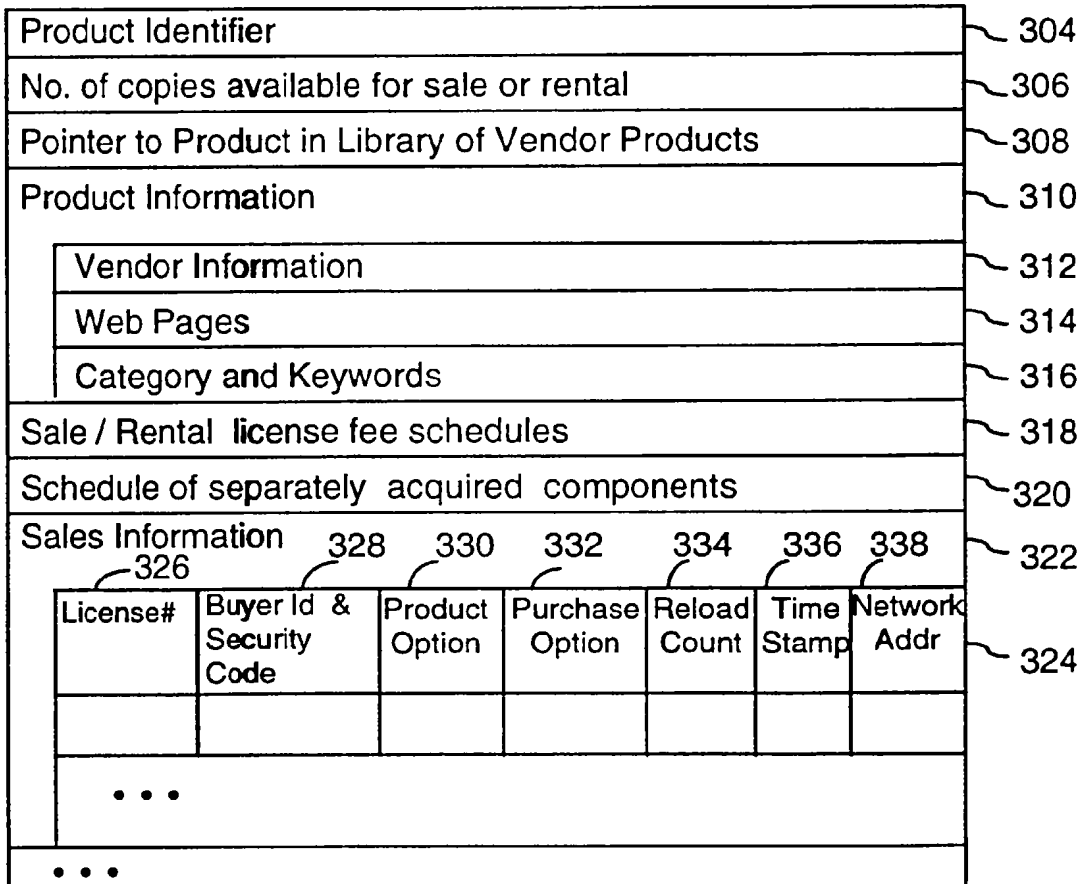


FIG. 3B



Client Computer  
120

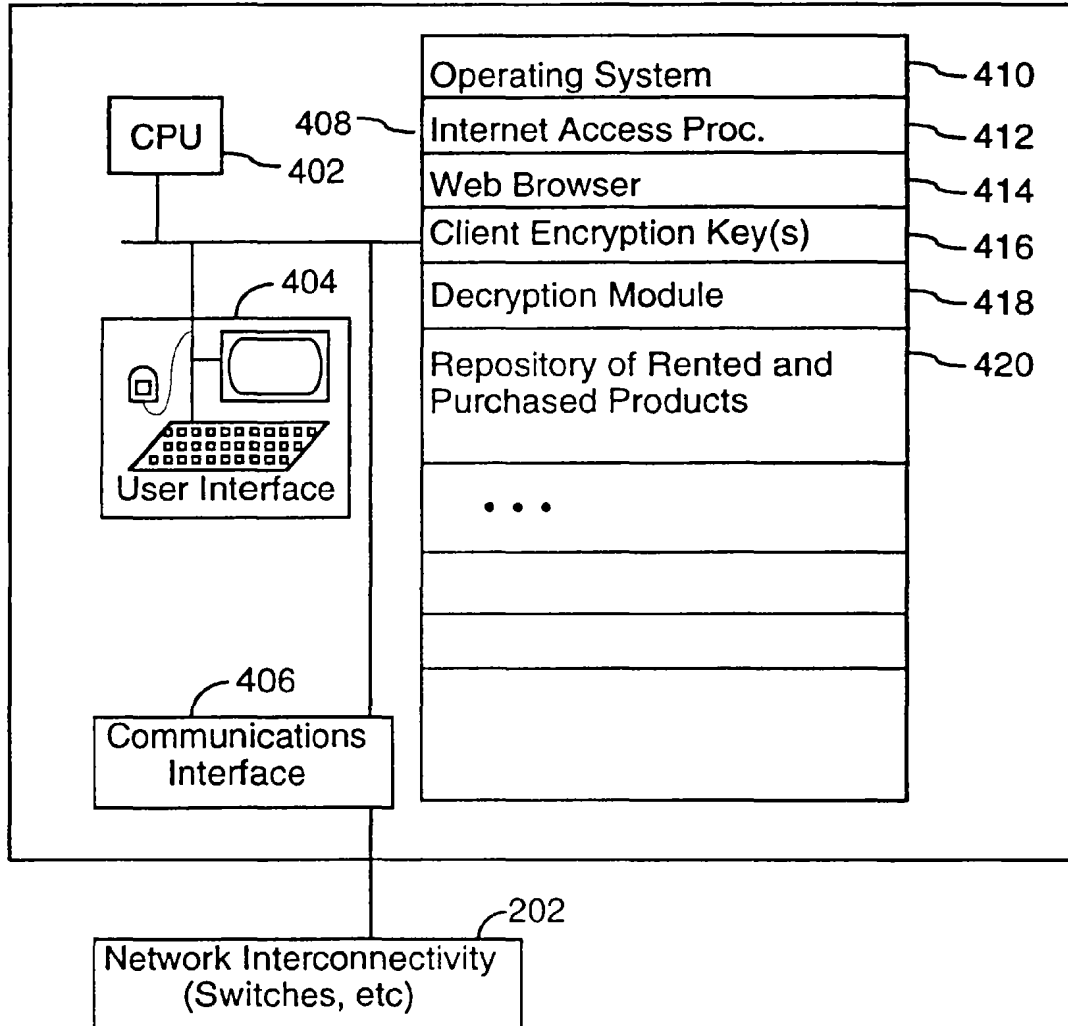


FIG. 4

Virtual Vending  
Machine Web Page  
220

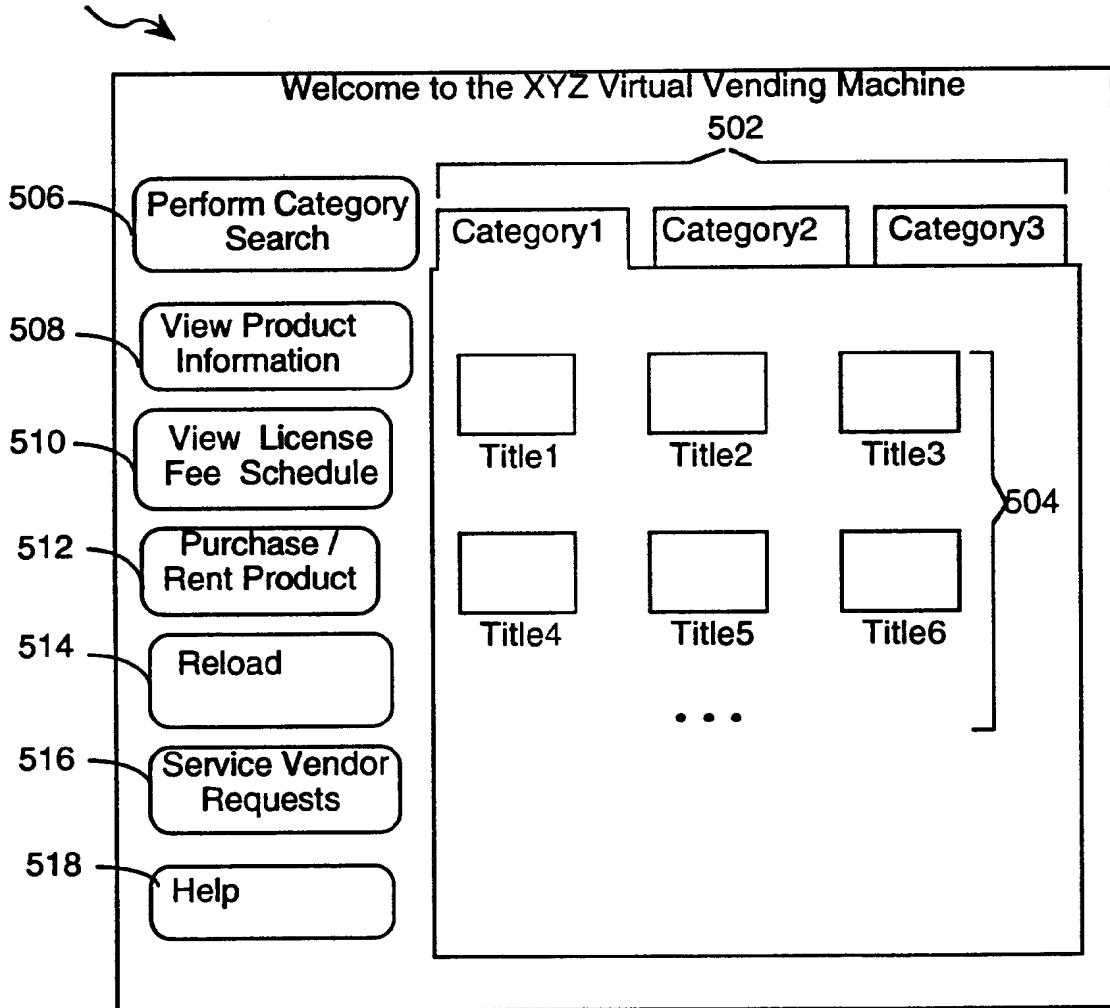


FIG. 5

600

Purchase or Rent of Title1

Select license option:

Expiration date of rental period:

Select product option:  
  
component 1  
component 2  
...  
component n

Buyer information

Total license price: \$

Verify sale:

FIG. 6

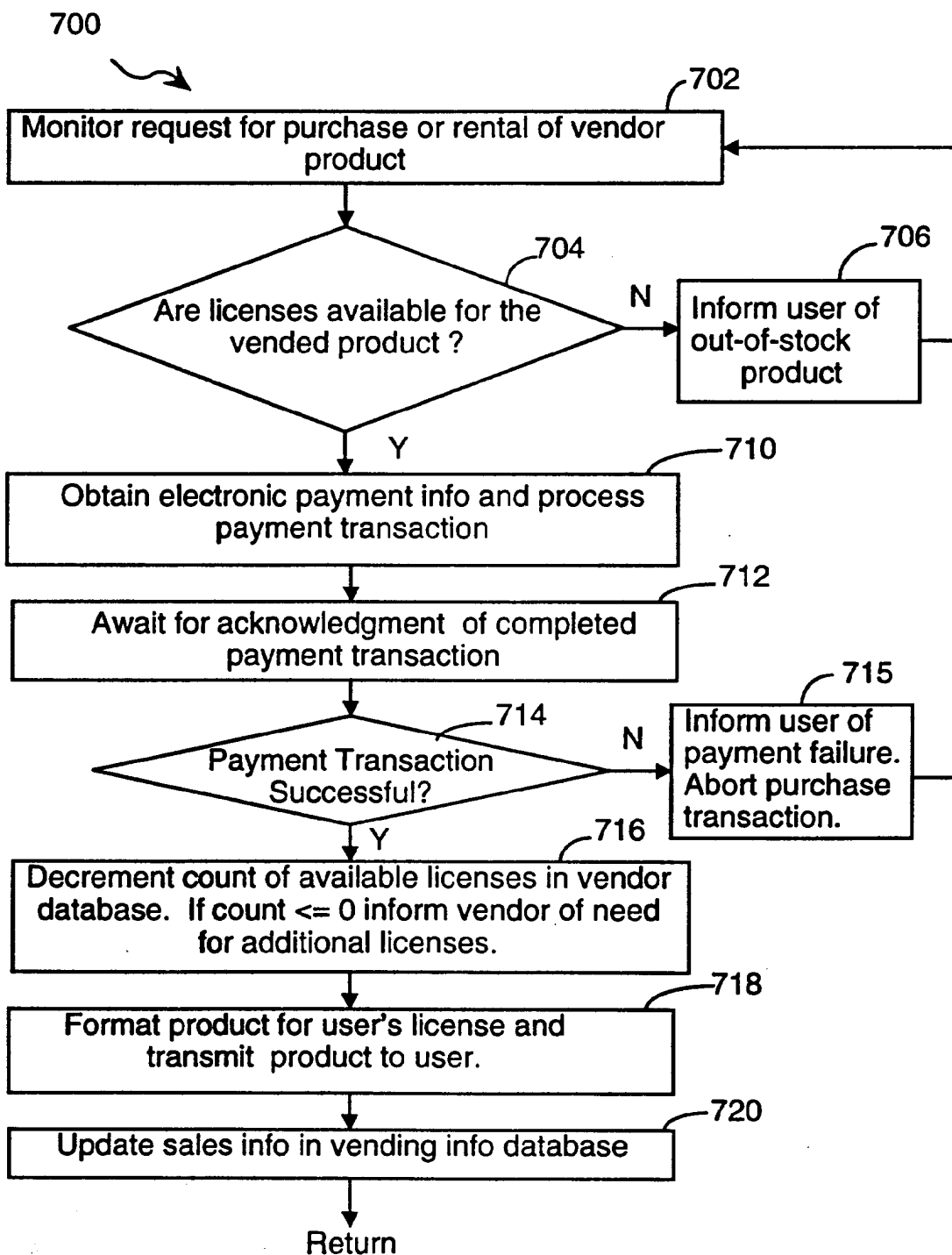


FIG. 7

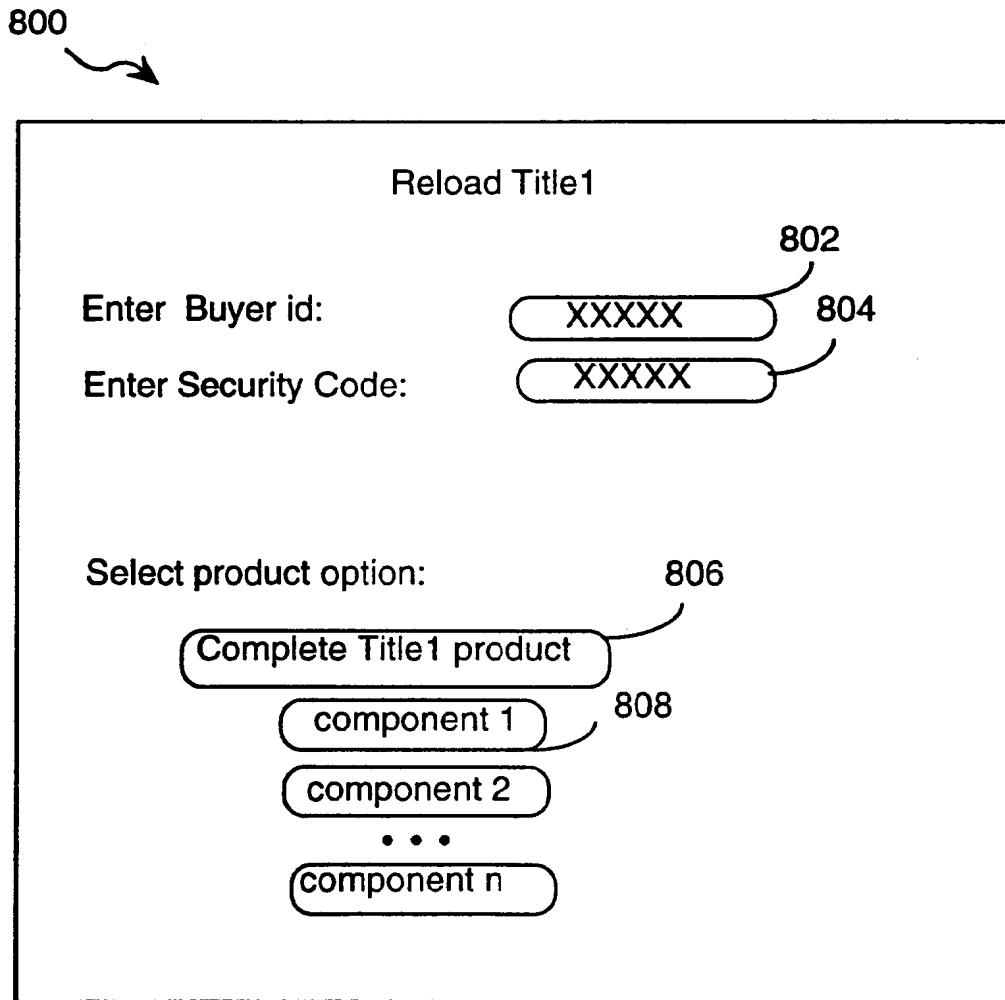


FIG. 8

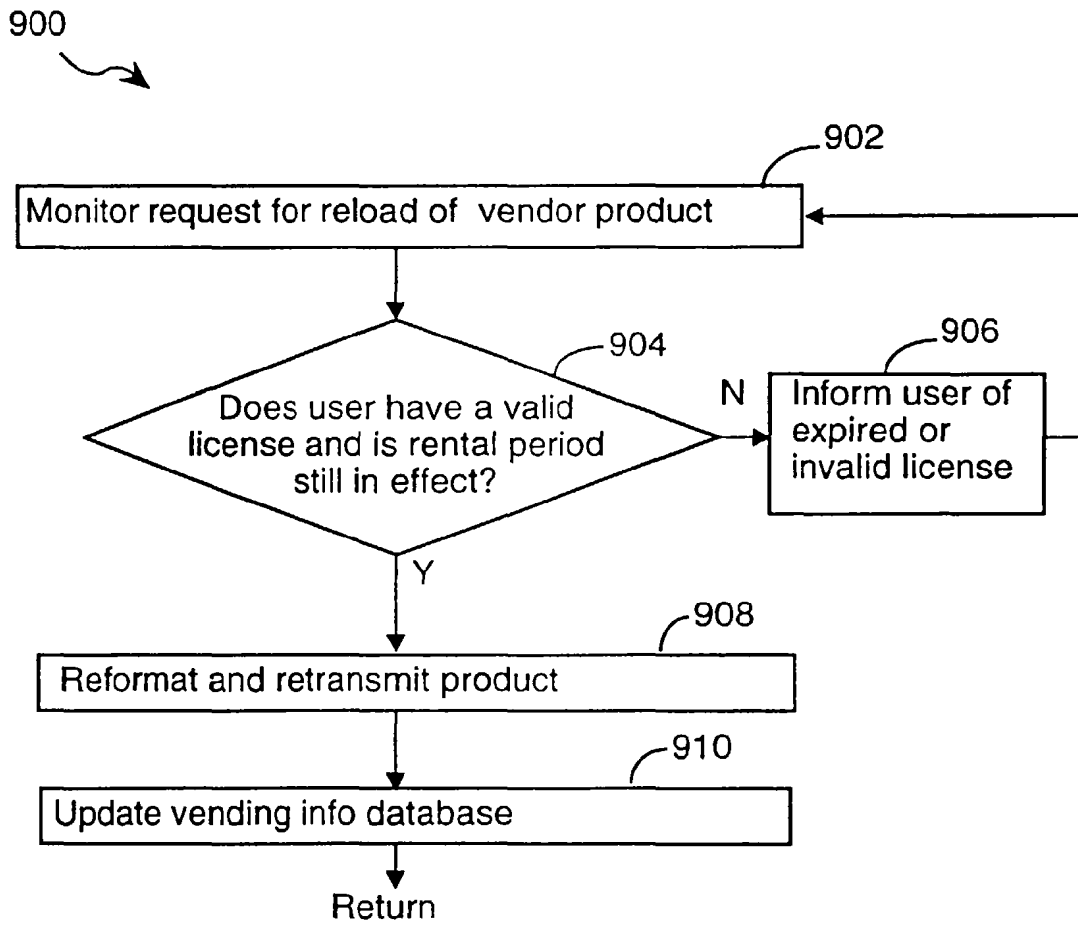


FIG. 9

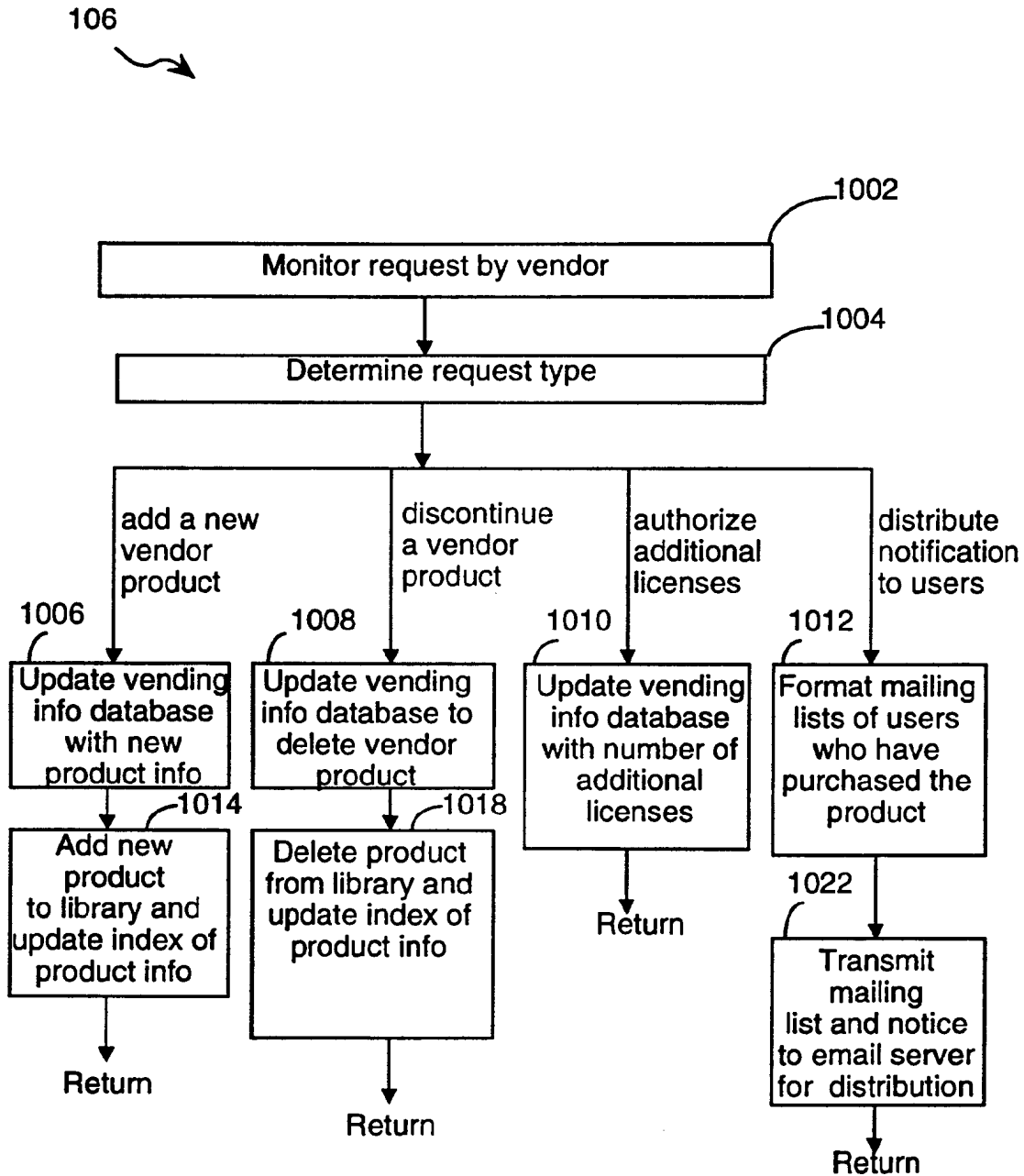
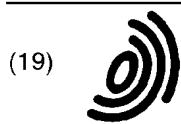


FIG. 10



Europäisches Patentamt  
 European Patent Office  
 Office européen des brevets



(11)

**EP 0 819 287 B1**

(12)

**EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:  
**03.11.1999 Bulletin 1999/44**

(51) Int Cl.<sup>6</sup>: **G07F 7/10, G06K 19/07**

(86) International application number:  
**PCT/BE95/00017**

(21) Application number: **95909594.4**

(87) International publication number:  
**WO 96/25724 (22.08.1996 Gazette 1996/38)**

(22) Date of filing: **17.02.1995**

**(54) INTEGRATED CIRCUIT CONTROLLED TRANSACTION MANAGEMENT SYSTEM**

DURCH INTEGRIERTE SCHALTUNG ÜBERWACHTES  
 TRANSAKTIONSVERWALTUNGSSYSTEM

SYSTEME DE GESTION DE TRANSACTIONS COMMANDE PAR CIRCUIT INTEGRE

(84) Designated Contracting States:  
**AT BE CH DE DK ES FR GB GRIE IT LI LU MC NL  
 PT SE**  
 Designated Extension States:  
**LT SI**

• **JOHANNES, Peter**  
**B-3010 Kessel-Lo (BE)**

(43) Date of publication of application:  
**21.01.1998 Bulletin 1998/04**

(74) Representative: **Bird, Ariane et al**  
**Bird Goen & Co,**  
**Termerestraat 1**  
**3020 Winksele (BE)**

(73) Proprietor: **Europay International S.A.**  
**1410 Waterloo (BE)**

(56) References cited:  
**EP-A- 0 190 733**                      **WO-A-87/07062**  
**WO-A-94/10657**                    **FR-A- 2 657 445**  
**FR-A- 2 667 171**

(72) Inventors:  
 • **HEYNS, Guido**  
**B-3210 Linden (BE)**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

**EP 0 819 287 B1**



**Description**

**[0001]** The present invention relates to an integrated circuit controlled transaction management system intended to execute a transaction between an integrated circuit card (ICC) and a terminal connected or not to a central unit, a transaction consisting of at least one execution of the following sequence :

1. creating a communication link between the ICC and the terminal ;
2. performing a compatibility check to ensure that the ICC and the terminal are mechanically and electrically compatible ;
3. selection of an application supported both by the ICC and the terminal, that means the selection of a computer program and the associated data set that defines the transaction in terms of the specific ICC and terminal combination present ;
4. execution of said application on the ICC and terminal system, and
5. termination of the transaction, which optionally includes breaking of the communication link between the ICC and the terminal.

**[0002]** Document WO 92/13322 describes a secured method for loading a plurality of applications in a microprocessor memory ICC, containing means for creating a communication link in an ICC and terminal system.

**[0003]** There are several types of transactions between an ICC and a terminal :

the terminal may control access to places where only ICC holders may have access to ; in so-called financial transactions the ICC can be loaded with tokens representing consumption goods obtainable at a terminal site (e.g. frequent flyer miles, telecommunication units, etc...), or the ICC may act as a depository of bank account information which allows more general financial transactions ; or the ICC may be used as data storage, e.g. as an identity ICC or medical record storage.

**[0004]** Known features of said ICC and terminal system are :

1. The terminal hardware (i.e. the processor and the peripherals, which at least include the ICC communication device) is accessible via the terminal operating system. Terminal operating systems are vendor specific.
2. Each terminal that participates in certain types of standardised transaction types (e.g. international financial transactions) supports, for those transactions, a common standard allowing the ICCs to perform applications in a standard way with terminals from any vendor. By way of example, international financial transactions are currently based on the inter industry standards as defined in ISO 7810/7811/7812/7813/7816.
3. Each provider of standardised transactions on a terminal has to provide an application, i.e. a program and the associated data set, or an application specification, defined in terms of a common standard.
4. Some parties provide applications or application specifications that are only partly build on a common standard. For special requirements which are outside the scope of the common standard, said parties need to rely on the terminal operating system.
5. Other parties provide applications or application specifications, which are proprietary to them or which are not based on any common standard. In this case they solely rely on the terminal operating system to perform the transaction.
6. Each application program needs to be compiled and linked separately for each terminal type. This means that specific software has to be resident in the terminal for each application .
7. Applications define large sets of terminal parameters governing the rules of their acceptance. These parameters may need to be shared with other applications.
8. Application software must be physically installed in each terminal.
9. Different versions of application software defining the same transaction may be required on the terminal during more or less extended conversion periods.

**[0005]** The features associated with said known ICC and terminal system loaded with multiple applications, impose heavy constraints on the terminal hardware, which must be able to store and to manage all possible application software and the assorted data sets. Moreover, a considerable logistic effort is indispensable to manage the distribution and the maintenance of all the software in all the terminals. Those features have the following drawbacks :

- \* Changing terminal software specifications or parts thereof, changing application software specifications or parts thereof or changing the implementations of a specification or parts thereof or creating new applications requires to develop new software for each target terminal type and to load this new software in each target terminal. Moreover, certification against all ICC types in circulation at that moment and against those scheduled for future release is required ;

- \* Restricted flexibility because even minor changes to a common standard have to be agreed between all parties that use it ;
- \* Every application requires storage capacity on the terminal, which is limited ;
- \* Common standards are not complete enough to support all proprietary needs ;
- 5 \* The applications need to be implemented carefully so that neither their programs, nor their parameters interfere with each other ;
- \* This approach reduces the ICC to a mere memory device, as it is not possible to give the ICC the control over each type of terminal due to the plethora of different operating systems in use.

10 **[0006]** The above mentioned drawbacks result in a lack of flexibility of said ICC and terminal system. Hence the time to market new, upgraded or improved applications is extremely long, in the order of several years as all ICCs and all terminals are affected.

**[0007]** FR-A-2667171 further discloses an integrated circuit controlled transaction management system which uses an interpreter on the ICC which deals with the execution of an application, said interpreter on the ICC being able to access and to use at least a part of the ICC memory and at least a part of the ICC peripherals.

15 **[0008]** A problem to be solved is the lack of flexibility of the system.

**[0009]** The present invention aims to ease the management of all possible applications with all possible ICCs on all possible terminals. This purpose is achieved by means of an ICC transaction management system of the type described in the preamble of the enclosed claim 1, which is remarkable by the features of the characterising portion of claim 1, by using an interpreter which deals the solution proposed, thus involving the uses interpreters both or either on the ICC or on the terminal with the execution of an application either on the ICC, or on the terminal, or on both whereby the interpreter in the terminal is able to access and to use at least a part of the terminal memory and a part of the terminal peripherals, e.g. keyboard, display, printer, modem.

20 **[0010]** Indeed, an interpreter performs the interpretation between a program written in a compact high level and universal language and the language specific to operate the terminal or the ICC. For all practical purposes an interpreter consists of a program which reads an input stream (the interpreter on the ICC reads the input stream coming from the terminal and the interpreter on the terminal reads the input stream coming from the ICC) and of one or more dictionaries, whereby a dictionary is a collection of words, each referring to executable statements. The interpreter language is independent of the ICC and terminal system, and may e.g. be FORTH (see ANSI standard : X3J14 Secretary, c/o FORTH Inc. 111 Sepulveda Blvd. Suite 300, Manhattan Beach, CA 90266).

25 **[0011]** A first advantage of using an interpreter in an ICC controlled transaction management system according to the invention, is the possibility to store new applications or parts thereof or upgrades or improvements to existing applications or parts thereof on the ICC coded in an interpreted language. This allows to reduce the time to market new applications or to upgrade or improve existing applications or parts thereof.

30 **[0012]** Time or effort required to market new, upgraded or improved applications is reduced to the time or effort required to load them in terms of the interpreter language in the ICC, which may require loading new, improved or upgraded dictionaries on the ICC. In this way the ICC has control over the application. No time or effort is required to update terminals. Even when changes to terminal dictionaries must be made, it is sufficient to load the new, upgraded or improved definitions in the ICC during an introductory or reconversion period until the new upgraded or improved definitions are available on the terminal. It is possible to implement the ICC and terminal system in such a way that the new , upgraded or improved definitions in the ICC are transferred to the terminal during a transaction and stored permanently in the terminal memory thereafter .

35 **[0013]** Management of terminal functionality is reduced to the installation once of the same interpreter program and the same interpreter language dictionary, hereafter referred to as interpreter core dictionary, either during the manufacturing process of the terminal or thereafter . It is possible to upgrade or improve the interpreter after installation of the terminal, e.g. by means of on-line down-loading or through an ICC . Optional additional dictionaries, e.g. proprietary dictionaries or common standard dictionaries may be loaded on the terminal.

40 **[0014]** A second advantage of using an interpreter in an ICC controlled transaction management system according to the invention is that the support for many applications on the terminal is reduced to the availability on the terminal of the interpreter program and the interpreter core dictionary and identifications of the supported applications. Additional dictionaries are optional.

45 **[0015]** A third advantage of using an interpreter in an ICC controlled transaction management system according to the invention is the possibility for the ICC to fully define and hence control the application.

50 **[0016]** The present invention provides the possibility to efficiently manage many applications on many fundamentally different terminals and the possibility to install new or improved or upgraded applications or parts thereof in a very efficient way, to have an extremely short time to market of new, upgraded or improved transactions and to allow the ICC to control the transaction.

55 **[0017]** Positive implications of the above are:

- \* Changing terminal software specifications only affects the interpreter implementation on that terminal. The only effort needed to maintain compatibility with existing applications is to ensure that the interpreter program and the interpreter core remain implemented correctly. Hence only one software needs to be recertified, and only against one specification, namely the interpreter definition. ICCs need not to be recertified as the interpreter language used in the application retains the same specification.
- \* The need for common standards is reduced to the availability of the interpreter as each standard function can be coded in the interpreter language and stored in the ICC.
- \* Introducing new, improved or upgraded applications needs not to affect dictionaries that have to be stored on the terminal, as all applications and related dictionaries are defined in terms of the interpreter language and can be loaded on the ICC.
- \* The application data sets are all managed by the interpreter, which eases their management.
- \* The ICC can take actively part in the execution of the application program or parts thereof by also implementing an interpreter program and core dictionary on the ICC. If the ICC is a mere memory ICC, it can still control the application by completely storing it, i.e. the terminal acts completely according to the ICC definitions.

**[0018]** Some applications may require specific security services, e.g. data integrity, ICC authentication, terminal authentication or data confidentiality. These can be provided with state of the art techniques as defined e.g. in ISO 10202.

**[0019]** According to a first particularity of the invention, an application consists of one or more functions, each function consisting of a controlling part referred to as the header of the function and an executable part referred to as the body of said function. The header determines which bodies have to be executed and under which conditions. Both parts of the function are able to be independently stored in a dictionary. Functions may be defined in terms of other functions, i.e. functions may be nested.

**[0020]** A body which is stored in a dictionary is accessible via its body name, and a header stored in a dictionary is accessible via its header name. This does not prevent in any way to program a function in the interpreter language, it merely offers the possibility to write compact and yet flexible applications by carefully mixing body names, header names and interpreter language code. Functions themselves can also be stored in dictionaries, referred to by means of their header names. This reference method allows to define each function in four ways:

1. Both the header and the body can be interpreter language code ;
2. The header can be interpreter language code while the body is activated through its body name ;
3. The header is defined through its header name, while the body is fully expanded interpreter language code ;
4. Both the header and the body are stored as references, header name and body name respectively.

**[0021]** The invention allows the presence of several types of dictionaries in the ICC and terminal system:

1. the interpreter core, a mandatory dictionary;
2. a number of optional dictionaries including definitions relating to :

- a) certain types of standardized transactions, e.g. the dictionary containing all functions defined in ISO/IEC 7816 used in international financial transactions, referred to as the standard dictionary ;
- b) proprietary transactions, requiring non standard definitions, referred to as proprietary dictionary ;

**[0022]** The dictionary defined on the ICC may contain new, improved or upgraded functions or parts thereof. Those dictionaries normally take precedence over terminal dictionaries. However the security of some applications may prohibit the redefinition of certain words in certain dictionaries. Security features can be provided through the specific protection mechanisms available in state of the art interpreter implementations.

**[0023]** The invention allows to store an application efficiently on the ICC and allows for flexible execution on the ICC and terminal system. Indeed, the following storage scenarios are possible thanks to the invention:

1. The transaction fully adheres to a standard. This means that the ICC only has to store the function name of the application, which is defined in the standard dictionary on the terminal;
2. If the transaction is proprietary and the application is defined on the terminal it communicates with, the ICC only has to store the function name of the application, which is defined in the proprietary dictionary on the terminal;
3. If the transaction is proprietary and the application is not defined on the terminal it communicates with, the definition of the application must then be stored on the ICC, in the ICC dictionary. The functions of the application can use body names and header names of both the standard and the proprietary dictionaries, but can also include

interpreter language code.

Example 1 :

5 [0024] Assuming an application with the following header (given in pseudo-code) :

```

    if (x=1) then func_a(y)
                else if (x_2) then func_b(y)
10                else func_c(y)

```

whereby func\_a, func\_b and func\_c are defined in the terminal proprietary dictionary. Assuming func\_a(y)=y+x, in that dictionary. Then the header as presented above is all that needs to be stored in the ICC to be able to execute it. In this case there is no need for an ICC dictionary. Now, assuming the interpreter implementation allows ICC dictionaries to take precedence over terminal dictionaries, and assuming the application provider wants to redefine func\_a(y), into func\_a(y)=y-x. In this case he can still use the same header, and he now has the choice to either update all proprietary dictionaries in all terminals, or to include the new definition in the ICC dictionary. This new definition will then be used during the execution of the application.

20 [0025] The invention allows that ;

- a) a ICC dictionary can be used to add to, improve or upgrade terminal dictionary definitions. A mechanism to do this is e.g. provided in the FORTH language, where the words defined last can redefine earlier dictionary entries.
- b) some dictionaries, e.g. the interpreter core or the standard dictionary for some applications, may be protected against erasure and against redefinitions. Techniques to achieve such protection are state of the art; an example is presented in patent WO90/05347.

[0026] The following execution scenarios are possible thanks to the invention:

1. The terminal executes the application program or parts thereof, whereby the ICC only acts as a data container and possibly as a storage device for the proprietary application program, or parts thereof.
2. Both the ICC and the terminal execute parts of the application. For security reasons it might be required that certain data do not leave the ICC, hence all manipulations involving such data must be executed by the ICC. Hence the ICC and the terminal communicate results of data manipulations instead of the data itself.
3. The ICC executes the application, whereby the terminal only needs to contain application identifications it supports. In this case the terminal may be used as a mere storage device, e.g. the terminal can provide the ICC with a dictionary that contains definitions of functions in terms of the interpreter language that are used during the execution of the application by the ICC.

40 [0027] This allows the ICC to use definitions without having to store them.

[0028] The above means that the invention brings following advantages :

1. The flexibility to define, improve or upgrade applications very easily and quickly by storing them on the ICC, relying on the terminal interpreter for execution and relying on the terminal interpreter core dictionary for definitions.
2. The flexibility to store applications in a compact way on the ICC using dictionaries on the terminal.
3. The flexibility to execute the application in either the ICC, the terminal or both ICC and terminal, depending on the availability of processing power in the ICC and the terminal.
4. The flexibility to allow multiple ICCs to participate in a transaction. The interpreter can be implemented in a terminal with multiple ICC readers.
5. In such a system it is possible to provide applications, either stored on one or more ICCs, a terminal or any combination of terminal and ICCs, that perform ICC to ICC transactions. In this case the terminal could be very simple, only providing the communication means between the ICCs and possibly providing some dictionaries to reduce the storage requirements on the ICCs. The ICCs could also provide resources to each other.
- 55 5. The flexibility to control the transaction from both the ICC, the terminal or both the ICC and the terminal. The transaction is the result of the execution of an application and hence is fully determined by the application program and the associated data set. As such control of the transaction or parts thereof is determined by the contribution from the ICC, the terminal or both the ICC and the terminal. When the transaction is fully determined

by a terminal resident application the card can only contribute to the application with a data set it contains and then undergoes the transaction. When the transaction is fully determined by the ICC resident application, the terminal contributes to it with its data set and undergoes the transaction. The terminal and the ICC can also perform the transaction as equals, whereby both determine and perform the transaction. It may occur that the ICC and terminal system is connected to a central unit from which it requests additional services, in which case the central unit may dynamically contribute to the application. E.g. the ICC can force the terminal to connect to its central unit and request the update of data on the ICC. The control of the application does not need to be strictly on the ICC or on the terminal.

**[0029]** In an initial step an application has to be selected for execution on the ICC and terminal system. This selection is trivial when the ICC and the terminal have no application or exactly one application in common. When multiple applications are supported both by the terminal and by the ICC, the current practice is to let the ICC holder or the terminal operator define interactively which application is chosen. This is not precluded by the invention which also provides an intelligent mechanism to select the application, depending on ICC parameters, terminal parameters and ICC capabilities and terminal capabilities.

Indeed, after insertion of the ICC in the terminal and after the ICC has satisfied all compatibility checks, the first action the terminal undertakes is to check whether the ICC supports an application it knows. In order to find this out, the terminal will try to consecutively select one of its resident applications. If an application is present on the ICC, the ICC contains the description of the application. According to the invention, a possible body in the application header is an application select function. This application select function is to be executed by the interpreter with arguments determined by the ICC. This means that with an application supported by the terminal and defined in the ICC, the selection of one of the many applications only defined on the ICC is made possible. Since the bodies of an application selection function may be application select functions, the application may be selected recursively.

Example 2 :

**[0030]** The following example is considered :

The ICC contains the following applications: Euro, Euro-Debit, Euro-Credit, Us-Debit, Us-Credit. The terminal only knows the application Euro. When the terminal inspects the ICC, the result of the select application function will be Euro and its related data.

The definition of application EURO can be stored either on the terminal or in the ICC. Assume it is stored in the ICC, then it could be defined as follows (in pseudo code) :

```

start
if (ICC amount <100)
    then if (terminal is located in Europe) then select application Euro-Debit else if (terminal is located in US) then
select application US-Debit else abort transaction
        else if (terminal is located in Europe) then select application Euro-Credit else if (terminal is located in US) then
select application US-Credit else abort transaction
end transaction,
wherein

```

\* not underlined text means the header, and underlined text means a body.

**[0031]** In this case, the terminal only knowing EURO can select applications defined in the ICC.

**[0032]** Any implementation of the present invention entails the following effort :

1 If the ICC is to be used as a mere memory ICC:

- a) implementing a secure interpreter on the terminal, with its interpreter core dictionary ;
- b) defining and implementing dictionaries for the application ;
- c) implementing the application in the interpreter language, possibly making use of available dictionaries ;
- d) implementing a mechanism to use the ICC dictionaries.

2. If the ICC takes an active part in the execution of the application:

- a) implementing a secure interpreter and its core dictionary on the terminal and implementing a secure interpreter and its core dictionary on the ICC .
- b) defining and implementing dictionaries for the applications ;

- c) implementing the application in the interpreter language, possibly making use of the available dictionaries ;
- d) implementing a mechanism on the terminal to use ICC dictionaries.
- e) implementing a mechanism on the ICC and the terminal to manage the execution of the applications on the ICC and terminal system
- 5 f) implement a mechanism on the card to use terminal dictionaries.

[0033] The invention is obviously not limited to a transaction management system using a card . Many changes may be made in the shape, the arrangement and the constitution of the integrated circuit carrier , without departing from the scope of the invention , e.g. a key or a badge .

**Claims**

- 1. An integrated circuit controlled transaction management system intended to execute between an ICC and a terminal connected or not to a central unit, a transaction consisting of at least one execution of the following sequence :
  - 1. creating a communication link between the ICC and the terminal ;
  - 2. performing a compatibility check to ensure that the ICC and the terminal are mechanically and electrically compatible ;
  - 20 3. selection of an application contained in the ICC and the terminal, that means the selection of computer program and the associated data set that defines the transaction in terms of the specific ICC and terminal combination present ;
  - 4. execution of said application on the ICC terminal system, and
  - 25 5. termination of the transaction, which optionally includes breaking of the communication link between the ICC and the terminal,

wherein said system uses an interpreter which deals with the execution of an application on the ICC, whereby this optional interpreter in the ICC is able to access and to use at least a part of the ICC memory and at least a part of the ICC peripherals,  
30 characterized in that said system further uses at least one interpreter both or either on the terminal or on the ICC, whereby the interpreter in the terminal is able to access and to use at least a part of the terminal memory and at least a part of the terminal peripherals.

- 2. Transaction management system according to claim 1, characterized in that each application consists of a number of functions , each function consisting of controlling part referred to as the header and an executable part referred to as the body of said function, both parts of said function possibly being independently stored in a dictionary.
- 3. Transaction management system according to claim 1, characterized in that functions may be nested.
- 40 4. Transaction management system according to anyone of claims 1 to 3, characterized in that a function in the application description is a "select application function" which is executed by the interpreter with arguments determined by the ICC, so that the application select may be executed recursively.
- 5. Transaction management system according to anyone of the previous claims , characterized in that the interpreter in the ICC is able to access and to use at least a part of the ICC memory and at least a part of the associated ICC peripherals.
- 6. Transaction management system according to one of the previous claims, characterized in that the interpreter in the terminal is able to access and to use at least a part of the terminal memory and at least a part of the terminal peripherals.
- 7. Transaction management system according to one of the previous claims, characterized in that the ICC is a mere memory ICC which undergoes the transaction as determined by the terminal .
- 55 8. Transaction management system according to one of the claims 1 to 6, characterized in that the ICC determines the transaction and the terminal which needs only to recognise an application on the ICC and able to select it, undergoes the transaction.

9. Transaction management system according to one of the claims 1 to 6, characterized in that the ICC and the terminal both determine and perform the transaction.
- 5 10. Transaction management system according to claim 8, characterized in that the terminal is a pure interface device between a number of ICCs.
11. Transaction management system according to one of the claims 7 to 9, characterized in that each ICC contains a differently personalised application.
- 10 12. Transaction management system according to one of the previous claims, characterized in that an interpreter is implemented in a terminal with many ICC readers, and provided with applications, either on the ICC, terminal or both, that perform combination of transactions.

15 **Patentansprüche**

1. Ein von einer integrierten Schaltung gesteuertes Transaktionsverwaltungssystem zur Ausführung von Transaktionen zwischen einer Chipkarte und einem Terminal, das entweder mit einer Zentraleinheit verbunden ist oder nicht, wobei eine Transaktion mindestens aus einem Ausführen der folgenden Schritte besteht:

- 20
1. Erstellen einer Kommunikationsverbindung zwischen der Chipkarte und dem Terminal;
  2. Durchführen einer Kompatibilitätsprüfung, um sicherzustellen, daß die Chipkarte und das Terminal mechanisch und elektrisch kompatibel sind;
  - 25 3. Auswahl einer in der Chipkarte oder in dem Terminal enthaltenen Anwendung, d.h. Auswahl eines Computerprogramms und des damit verbundenen Datensatzes, welche die Transaktion bezüglich der vorhandenen spezifischen Kombination der Chipkarte und des Terminals definiert;
  4. Ausführung der Anwendung auf dem Chipkarten-Terminalsystem und
  5. Beendigung der Transaktion, die wahlweise auch das Unterbrechen der Kommunikationsverbindung zwischen der Chipkarte und dem Terminal beinhaltet,

30 wobei das System einen Interpretierer einsetzt, der die Ausführung einer Anwendung auf der Chipkarte bearbeitet, wobei dieser fakultative Interpretierer in der Chipkarte mindestens auf einen Teil des Speichers der Chipkarte und mindestens auf einen Teil der Peripheriegeräte der Chipkarte zugreifen und diese einsetzen kann, dadurch gekennzeichnet, daß das System weiterhin mindestens einen Interpretierer auf dem Terminal und der Chipkarte oder auf dem Terminal oder auf der Chipkarte verwendet, wobei der Interpretierer im Terminal in der Lage ist, auf mindestens einen Teil des Speichers des Terminals und mindestens einen Teil der Peripheriegeräte des Terminals zuzugreifen und diese einzusetzen.

- 35
2. Transaktionsverwaltungssystem gemäß Anspruch 1, dadurch gekennzeichnet, daß jede Anwendung aus einer Zahl von Funktionen besteht, wobei jede Funktion aus einem Steuerabschnitt, der als Kopf bezeichnet wird, und einem ausführbaren Abschnitt, der als Körper der Funktion bezeichnet wird, wobei beide Teile der Funktion möglicherweise unabhängig voneinander in einem Wörterbuch gespeichert werden.
- 40
3. Transaktionsverwaltungssystem gemäß Anspruch 1, dadurch gekennzeichnet, daß Funktionen verschachtelt werden können.
- 45
4. Transaktionsverwaltungssystem gemäß einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß eine Funktion in der Anwendungsbeschreibung eine "Selekt-Anwendung-Funktion" ist, die vom Interpretierer mit von der Chipkarte bestimmten Argumenten ausgeführt wird, so daß das Anwendungsselektieren rekursiv ausgeführt werden kann.
- 50
5. Transaktionsverwaltungssystem gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Interpretierer in der Chipkarte in der Lage ist, auf mindestens einen Teil des Speichers der Chipkarte und mindestens einen Teil der Peripheriegeräte der Chipkarte zuzugreifen und diese einzusetzen.
- 55
6. Transaktionsverwaltungssystem gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Interpretierer im Terminal in der Lage ist, auf mindestens einen Teil des Speichers des Terminals und mindestens einen Teil der Peripheriegeräte des Terminals zuzugreifen und diese einzusetzen.

7. Transaktionsverwaltungssystem gemäß einem der vorgehenden Ansprüche, dadurch gekennzeichnet, daß die Chipkarte lediglich eine Speicherkarte ist, die sich der vom Terminal bestimmten Transaktion unterzieht.
- 5 8. Transaktionsverwaltungssystem gemäß einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Chipkarte die Transaktion bestimmt und sich das Terminal, das lediglich eine Anwendung auf der Chipkarte zu erkennen hat und in der Lage sein soll, diese zu selektieren, sich der Transaktion unterzieht.
9. Transaktionsverwaltungssystem gemäß einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Chipkarte und das Terminal beide die Transaktion bestimmen und diese ausführen.
- 10 10. Transaktionsverwaltungssystem gemäß Anspruch 8, dadurch gekennzeichnet, daß das Terminal ein reines Schnittstellengerät zwischen einer Zahl von Chipkarten ist.
11. Transaktionsverwaltungssystem gemäß einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, daß jede Chipkarte eine unterschiedlich personengepaßte Anwendung enthält.
- 15 12. Transaktionsverwaltungssystem gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß ein Interpretierer in einem Terminal mit zahlreichen Chipkartenlesegeräten implementiert ist und für welchen Anwendungen, die eine Kombination von Transaktionen ausführen, entweder auf der Chipkarte, dem Terminal oder beiden bereitgestellt sind.
- 20

### Revendications

- 25 1. Système de gestion de transactions commandé par circuit intégré et destiné à exécuter, entre une CCI et un terminal connecté ou non à une unité centrale, une transaction se composant d'au moins une exécution de la séquence suivante:
- 30 1. créer une liaison de communication entre la CCI et le terminal;  
2. réaliser un contrôle de compatibilité pour s'assurer que la CCI et le terminal sont mécaniquement et électriquement compatibles;  
3. sélection d'une application contenue dans la CCI et le terminal, c'est-à-dire la sélection d'un programme d'ordinateur et de l'ensemble de données associé qui définit la transaction en termes de la combinaison CCI-terminal spécifique présente;
- 35 4. l'exécution de ladite application sur le système terminal CCI, et  
5. l'achèvement de la transaction, qui comporte en option l'interruption de la liaison de communication entre la CCI et le terminal,
- 40 dans quoi ledit système utilise un interpréteur qui traite l'exécution d'une application sur la CCI, par quoi cet interpréteur en option dans la CCI peut accéder à et utiliser au moins une partie de la mémoire CCI et au moins une partie des périphériques de la CCI,  
caractérisé en ce que ledit système utilise en outre au moins un interpréteur sur le terminal et sur la CCI, ou sur l'un ou l'autre, l'interpréteur dans le terminal pouvant accéder à et utiliser au moins une partie de la mémoire terminal et au moins une partie des périphériques du terminal.
- 45 2. Système de gestion de transactions selon la revendication 1, caractérisé en ce que chaque application se compose d'un nombre de fonctions, chaque fonction se composant d'un champ de contrôle désigné l'en-tête et d'un champ exécutable désigné le corps de ladite fonction, les deux champs de ladite fonction étant peut-être mémorisés indépendamment dans un dictionnaire.
- 50 3. Système de gestion de transactions selon la revendication 1, caractérisé en ce que des fonctions peuvent être imbriquées.
- 55 4. Système de gestion de transactions selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'une fonction dans la description de l'application est une "fonction de sélection d'application" qui est exécutée par l'interpréteur avec des arguments déterminés par la CCI, de sorte que la sélection d'application peut être exécutée de façon récursive.



5. Système de gestion de transactions selon l'une quelconque des revendications précédentes, caractérisé en ce que l'interpréteur dans la CCI peut accéder à et utiliser au moins une partie de la mémoire CCI et au moins une partie des périphériques de la CCI associés.
- 5 6. Système de gestion de transactions selon l'une des revendications précédentes, caractérisé en ce que l'interpréteur dans le terminal peut accéder à et utiliser au moins une partie de la mémoire terminal et au moins une partie des périphériques du terminal.
- 10 7. Système de gestion de transactions selon l'une des revendications précédentes, caractérisé en ce que la CCI est une simple CCI de mémoire qui subit la transaction ainsi que déterminée par le terminal.
- 15 8. Système de gestion de transactions selon l'une des revendications 1 à 6, caractérisé en ce que la CCI détermine la transaction et le terminal, qui n'a besoin que de reconnaître une application sur la CCI et de pouvoir la sélectionner, subit la transaction.
- 20 9. Système de gestion de transactions selon l'une des revendications 1 à 6, caractérisé en ce que la CCI et le terminal tout deux déterminent et réalisent la transaction.
- 25 10. Système de gestion de transactions selon la revendication 8, caractérisé en ce que le terminal est un pur dispositif d'interface entre un nombre de CCI.
- 30 11. Système de gestion de transactions selon l'une des revendications 7 à 9, caractérisé en ce que chaque CCI contient une application différemment personnalisée.
- 35 12. Système de gestion de transactions selon l'une des revendications précédentes, caractérisé en ce qu'un interpréteur est réalisé dans un terminal avec de nombreux lecteurs CCI, et doté d'applications, soit sur la CCI, sur le terminal, ou sur les deux, qui réalisent une combinaison de transactions.
- 40
- 45
- 50
- 55



(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:  
06.05.1999 Bulletin 1999/18

(51) Int Cl.<sup>6</sup>: G06F 17/60

(21) Application number: 98308826.1

(22) Date of filing: 28.10.1998

(84) Designated Contracting States:  
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE  
Designated Extension States:  
AL LT LV MK RO SI

(72) Inventor: **Neilsen, Jakob**  
Atherton, California 94027 (US)

(74) Representative: **Read, Matthew Charles et al**  
Venner Shipley & Co.  
20 Little Britain  
London EC1A 7DH (GB)

(30) Priority: 31.10.1997 US 961984

(71) Applicant: **SUN MICROSYSTEMS, INC.**  
Palo Alto, California 94303 (US)

(54) Pre-paid links to networks servers

(57) The author or sponsor of a document on a server may provide a hyperlink to content that requires payment to view or download. The author or sponsor can prepay for access to that content in a manner that is transparent to the end user. In one approach the author's document is generated dynamically when a user requests it. During the generation process a payment

token is inserted into hyperlinks to payment-required content to which the author or sponsor desires to permit free access. When the user selects a pre-paid hyperlink the remote server attempts to validate the payment token. If the token is valid then the content is provided to the end user and the author or sponsor is billed. If the token is not valid an error message is displayed.

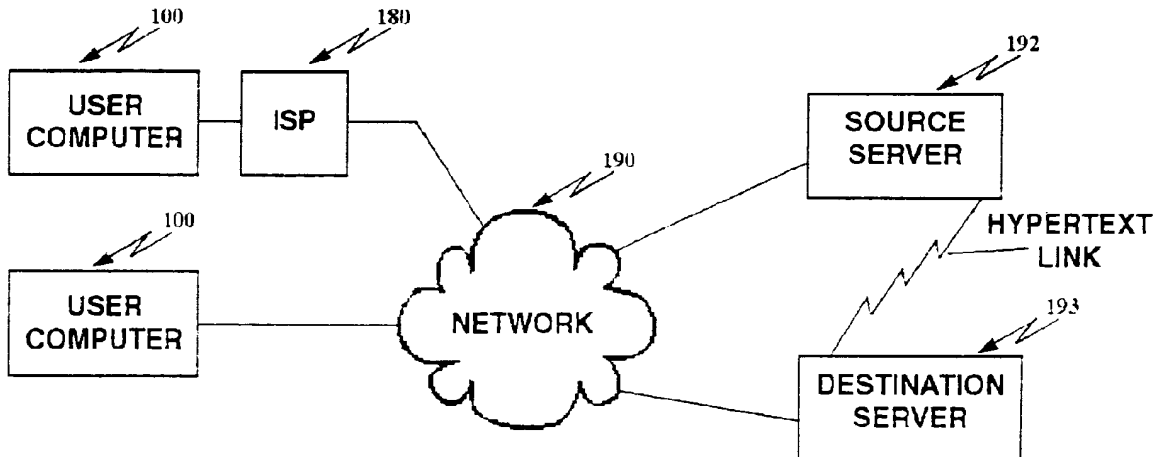


Figure 1D

**Description**BACKGROUND OF THE INVENTIONField of the Invention

[0001] This invention relates to computer systems and more particularly to information retrieval systems operating over a network such as the Internet.

Description of Related Art

[0002] Owners of electronic content that can be accessed via a computer network may charge a fee to view or download their content. For example, users may be required to pay for a subscription in order to access an online newspaper or magazine. Access to other types of content (i.e., software, music, and videos) may require the user to pay a one time fee in order to view or download it. Many examples of subscription and one time payment-required content can be found on the World Wide Web.

[0003] Payment for access to information may take any form, such as; credit cards, checks, electronic cash, and smart debit cards. Payments that require the transmission of data (e.g., credit cards, electronic cash, and smart debit cards) typically make use of an encryption technique. Many encryption techniques, such as public-private key cryptography, are known in the art.

The Problems

[0004] Sponsors of websites, or similar sources of information on networks may want to provide users with hyperlinks to other online content, some of which may require a payment to view or download. For example, a World Wide Web page author or sponsor may want to provide a hyperlink to a newspaper article that reported favorably on his product. Therefore, to encourage users to visit a payment-required site, such an author or sponsor would like, in some cases, to enable a visitor to his network server (hereinafter website) to access the payment-required content for free. This capability has not been available in the prior art.

SUMMARY OF THE INVENTION

[0005] The invention provides methods, apparatus, systems, and computer program products which allow a document author or sponsor to provide a hyperlink, by which users can access content for free by prepaying for the access. When a user requests a document using a hyperlink to payment-required content, a payment token and optional parameters are appended to the hyperlink definition. A payment token is a string of data that may include details about the account to charge for the content and when access to the content should expire.

[0006] When a user selects a payment-required hyperlink, the token and parameter information are transmitted to the destination server for processing. If the token is valid then the payment-required content is transmitted to the user.

[0007] The processes described above are transparent to the user. The original document appears normal to the user and the user may not know that access has been granted to payment-required content. In an alternative embodiment the user may be notified that free access has been granted to payment-required content courtesy of the original sponsor or author.

[0008] The foregoing and other features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The objects, features and advantages of the system of the present invention will be apparent from the following description in which:

[0010] **Figure 1A** is an illustration of a computer of a type suitable for carrying out the invention.

[0011] **Figure 1B** is a block diagram of an exemplary bus architecture suitable for carrying out the invention.

[0012] **Figure 1C** is an illustration of an exemplary memory medium for carrying program information and data for use in carrying out the invention.

[0013] **Figure 1D** is a block diagram of an exemplary network suitable for carrying program and data information useful for carrying out the invention.

[0014] **Figure 2** is a flow chart of an exemplary process for making payment-required content available to users for free in accordance with one embodiment of the invention.

[0015] **Figure 3** is a flow chart of an exemplary source page generation process for generating a server document with pre-paid links in accordance with one embodiment of the invention.

[0016] **Figure 4** is a flow chart of an exemplary payment token generation algorithm in accordance with one embodiment of the invention.

[0017] **Figure 5** is a flow chart of an exemplary destination server process for handling requested pre-paid content.

[0018] **Figure 6** is a flow chart of one embodiment of a process for checking the validity of a pre-payment token and issuing an appropriate response.

[0019] **Figure 7** is a flow chart of one embodiment of a process for honoring a valid pre-payment token.

[0020] **Figure 8** is a flow chart of one embodiment of a process for maintaining a server pre-payment token database.

[0021] **Figure 9** is an example of a hyperlink with a customer identifier parameter and a pre-payment token.

[0022] **Figure 10** is an example of a pre-payment to-

ken that includes the customer identifier, the token counter value, and the token expiration date and time.

#### NOTATIONS AND NOMENCLATURE

**[0023]** The detailed descriptions which follow may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are the means used by those skilled in the art to most effectively convey the substance of their work to others skilled in the art.

**[0024]** A procedure is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

**[0025]** Further, the manipulations performed are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein which form part of the present invention; the operations are machine operations. Useful machines for performing the operation of the present invention include general purpose digital computers or similar devices.

**[0026]** The present invention also relates to apparatus for performing these operations. This apparatus may be specially constructed for the required purpose or it may comprise a general purpose computer as selectively activated or reconfigured by a computer program stored in the computer. The procedures presented herein are not inherently related to a particular computer or other apparatus. Various general purpose machines may be used with programs written in accordance with the teachings herein, or it may prove more convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these machines will appear from the description given.

#### DESCRIPTION OF THE PREFERRED EMBODIMENT

**[0027]** **Figure 1A** illustrates a computer of a type suitable for carrying out the invention. Viewed externally in **Figure 1A**, a computer system has a central processing unit 100 having disk drives **110A** and **110B**. Disk drive indications **110A** and **110B** are merely symbolic of a number of disk drives which might be accommodated

by the computer system. Typically, these would include a floppy disk drive such as **110A**, a hard disk drive (not shown externally) and a CD ROM drive indicated by slot **110B**. The number and type of drives varies, typically, with different computer configurations. The computer has the display **120** upon which information is displayed. A keyboard **130** and a mouse **140** are typically also available as input devices. Preferably, the computer illustrated in **Figure 1A** is a SPARC workstation from Sun Microsystems, Inc.

**[0028]** **Figure 1B** illustrates a block diagram of the internal hardware of the computer of **Figure 1A**. A bus **150** serves as the main information highway interconnecting the other components of the computer. CPU **155** is the central processing unit of the system, performing calculations and logic operations required to execute programs. Read only memory (**160**) and random access memory (**165**) constitute the main memory of the computer. Disk controller **170** interfaces one or more disk drives to the system bus **150**. These disk drives may be floppy disk drives, such as **173**, internal or external hard drives, such as **172**, or CD ROM or DVD (Digital Video Disks) drives such as **171**. A display interface **125** interfaces a display **120** and permits information from the bus to be viewed on the display. Communications with external devices can occur over communications port **175**.

**[0029]** **Figure 1C** illustrates an exemplary memory medium which can be used with drives such as **173** in **Figure 1B** or **110A** in **Figure 1A**. Typically, memory media such as a floppy disk, or a CD ROM, or a Digital Video Disk will contain the program information for controlling the computer to enable the computer to perform its functions in accordance with the invention. Program and data information from such media is transmitted, in accordance with the invention, over a transmission link in the form of a carrier wave.

**[0030]** **Figure 1D** illustrates the use of computers of the type shown in **Figures 1A** and **1B** in a network environment. Such computers can be used as user computers (**100**, **100'**) or as servers (**192**, **193**), sometimes with nominal differences of configuration. A user computer may connect to the network **190** either directly (**100'**) or via a network service provider, such as an internet service provider **180**. Program and data information used in carrying out the invention can be transmitted as a carrier wave over the network(s).

**[0031]** **Figure 2** is a flow chart of an exemplary prepaid content hyperlink process in accordance with one embodiment of the invention. When a user requests a document that contains one or more links to content for which payment is required (**200**), the document is generated (**210**) by the source server **192**. The document can be generated by using a Java servlet or a common gateway interface (CGI) program. In any event, it is generated anew for each access. An exemplary document generation process is described in detail in conjunction with **Figure 3**. Once the source document has been generated it is transmitted and displayed to the user

**220.** While viewing the source document the user may decide to click on a link to remote content **230**. Remote content is, for example, any content that is not controlled by the sponsor of the page or document being accessed. For example, a link to an additional document that is part of the current site would not normally be considered a link to remote content.

**[0032]** If the user clicks on a link to remote content the access that is not pre-paid (regular link) then access to that content is handled using standard techniques known in the art **240**. If the user decides to click on a link to content for which a payment is required (payment-required content) then the address of the content (regular hypertext link), typically the universal resource locator (URL) or the address, and payment parameters associated with that link (if the link is a pre-paid link) are transmitted **250** to the appropriate destination server **193**. When the destination server **193** receives the URL and added parameters, it processes the request for content **260** and collects the payment, by, for example, storing digital cash or debiting the sponsor's account. The processing of requested content is discussed in detail in conjunction with **Figure 5**.

**[0033]** **Figure 3** is an exemplary flow chart that describes an exemplary the process used to generate a source document in accordance with one embodiment of the invention. In this example a template for a source document is searched for links to payment-required content **300** to which the document author or sponsor desires to provide free access. When one is found the program adds payment information to the link as a parameter **310**, thus making it a pre-paid link.

**[0034]** In a preferred embodiment using HTML, a pre-paid link would have the format **900** detailed in **Figure 9**. The site identifier would be followed by a specification of the desired page followed by a marker, such as a question mark, **910** which indicates that parameter values follow. The parameter values constitute exemplary payment information. A first parameter in this example is a billing account identifier **920**. Next a payment token is generated by the source server **320**. The token generation process is discussed in detail in conjunction with **Figure 4**. The payment token is then added to the pre-paid link **330**. In the preferred HTML embodiment the token is added to the billing account identifier **920** and is separated from it by a plus sign **930**. The process then repeats until the end of the document file has been reached.

**[0035]** **Figure 4** is a flow chart of an exemplary process for generating payment tokens in accordance with one embodiment of the invention. The exemplary payment token (e.g. **Figure 10**) is generated by adding a billing account identifier (**1010**) for an author or sponsor of a document on the server to an empty token **400**. The size, in characters, of the billing account identifier is preferably known to both the source and destination processes. In a preferred embodiment the billing account identifier would be left padded with zeros, if nec-

essary, in order to satisfy a fixed size requirement. The token counter is incremented by one and the new token counter value (**1020**) is concatenated to the billing account identifier. See step **410**. The token counter size is also preferably known to both the source and destination processes. In a preferred embodiment the token counter should be left padded with zeros, if necessary, to fulfill the size requirement. The token counter is a software counter or a hardware counter on the source server, which ensures that all tokens generated have a unique value. The token expiration data and time is calculated and this value (**1030**) is concatenated to the other components of the token (**420**). The length of time a token will remain valid may be previously agreed upon by the source and destination owners. The expiration date and time may be preferably calculated as the number of seconds after midnight from a predetermined date (i.e., January 1, 1997). The token number (see **Figure 10**) may be large, in which case it is then converted into a base 36 number in order to compress it (**430**). Base 36 numbers make use of the digits 0-9 and the letters A-Z. The base 36 number is preferably encrypted using the current site's private key **440**.

**[0036]** Public-key/private-key cryptography is a known technique for providing security when transmitting data over a communications network. Public-private key cryptography is based on a mathematical process that generates two keys where one key cannot be determined from the other. In use, the private key is known only to the user. Typically it is a long series of characters stored on the user's computer. The public key is "published", i.e. it is made available to anyone who wants it. When a user needs to send a secure transmission, the data is encrypted using one of the private or public keys. When the transmission is received the recipient can decrypt the data using the other of the private or public key. The originating site would typically encrypt with its private key and the pre-paid content provider would decrypt using the originating site's public key.

**[0037]** **Figure 5** is a flow chart of an exemplary destination server process for handling requests for content in accordance with an exemplary embodiment of the invention. The destination server (**193**) first determines if the requested content requires a payment **500**. This can be done by querying a database of payment-required URLs on the destination server. If the requested content does not require a payment then the destination server transmits the content to the user **510**. If the content requires payment to view or download it and the request has arrived from a pre-paid link, then the destination server parses the source site's billing account identifier and the payment token from the end of the URL (see **Figure 9**). This parse procedure can be done easily by looking for the characters between the question mark (**910**) and the plus sign (**930**) The destination server uses the source site's billing account identifier to find the source site's public key in a database **530**. The destination server uses the public key to decrypt the token **540**.

The token is then converted back into a base 10 number and the source site's billing account identifier, the token expiration data and time, and the token counter value are parsed out **550**. The parse procedure can be accomplished because the size of the customer identifier and token counter are known. The destination server then attempts to validate the token **560**. The token validation process is discussed in detail in conjunction with Figure 6.

**[0038]** Figure 6 is a flow chart of an exemplary token validation process in accordance with one embodiment of the invention. The token validation process, which runs on the destination (pre-paid content provider) server (**193**), first attempts to match the source site's billing account identifier included in the parameter (**920**) with the source site's billing account identifier included in the token (**1010**) **600**. If the two numbers do not match, an error message stating the token cannot be recognized will be displayed to the user **610**. Any error message given to the user will result in an option to return to the source document to try the link again or to pay for the content themselves **690**. If the billing account identifiers match, then the token validation program will check the expiration date and time against the current system date and time **620**. If the token has expired then a token has expired error message will be displayed to the user **630**. If the token has not expired then the token validation program will attempt to find the token counter in its database of previously honored tokens **640**. If the token counter is found in the database then a message stating that the token has already been used will be displayed to the user **650**. If the token counter is not found in the database then the token validation program will check to see if the source site has sufficient credit to pay for the transaction **660**. Since payment may take many forms the token validation program will first determine the payment type by accessing the customer's account information in the database. If, for example, the customer makes pre-payments then the validation program will determine if enough money remains in the account to pay for the transaction. In other cases the customer may have established credit, in which case the validation program may need to check the customer's credit limit. If the customer is not able to pay for the transaction then a message stating that pre-payments from the source site are currently not being honored, will be displayed to the user **670**. If the customer has the ability to pay for the transaction then the token is honored **680**. The token honored process is discussed in detail in conjunction with Figure 7.

**[0039]** Figure 7 is a flow chart of an exemplary process of a destination server honoring a valid token in accordance with one embodiment of the invention. When a token is honored the requested content is transmitted and displayed to the user **700**. In addition, the source site is billed in accordance with the payment arrangements made between the source and destination sites **710**. If, for example, the source site has established a

pre-paid account with the destination site then the payment for the transaction is subtracted from the amount of money in the pre-paid account. If, on the other hand, the destination site bills the source site on some regular basis then the number of transactions in the source site's account will be incremented by one. In addition to billing, the token counter and expiration time and date are stored in an honored tokens database **720** indexed, for example, by sponsor. As before, time is preferably stored as a number of seconds after midnight on a reference date. This database is used in the validation process **640**.

**[0040]** Figure 8 is a flow chart of an exemplary maintenance process for the honored tokens database. Since tokens should only be kept in the honored tokens database until their expiration time a maintenance program will need to be run on the database at a regular interval (i.e., every hour). First, the current time and date are determined from the system clock **800**. Next, the database is queried for tokens that have expired based on the current time **810**. Finally, expired tokens are deleted from the database **820**.

**[0041]** Although the present invention has been described and illustrated in detail, it is clearly understood that the same is by way of illustration and example only and is not to be taken by way of limitation, the spirit and scope of the present invention being limited only by the terms of the appended claims and their equivalents.

## Claims

1. Apparatus for permitting access to services for which a payment is required, comprising:
  - a. a network port; and
  - b. a computer, connected to said network port, configured to generate a document having a link to services on a network for which an access payment is required and to associate payment information with said link by which access to said services may be obtained without payment by a user following said link.
2. Apparatus of claim 1 in which said document is generated using one of a Java servlet and a common gateway interface program.
3. Apparatus of claim 1 in which said payment information includes one or more of a billing account identifier and a payment token.
4. Apparatus of claim 3 in which said token comprises one or more of a token number, an expiration date and expiration time.
5. Apparatus of claim 3 in which at least part of said payment information is encrypted.

- 6. Apparatus of claim 1 in which said services includes providing information.
- 7. Apparatus for permitting access to services for which a payment is required, comprising:
  - a. a network port; and
  - b. a computer, connected to said network port, configured to provide access to services under control of said computer upon receipt of payment therefore and to extract payment information from a connect received over said network port.
- 8. Apparatus of claim 7 in which said computer manages a database.
- 9. Apparatus of claim 8 in which said database contains account information about one or more customers authorized to provide pre-payment.
- 10. Apparatus of claim 9 in which said database contains information about tokens which have been honored.
- 11. Apparatus of claim 7 in which said computer is configured to check whether said payment information is valid.
- 12. A method of pre-paying for services accessed over a computer, comprising the steps of:
  - a. providing an element for performing the step of generating a document containing a link to a service provider; and
  - b. providing an element for performing the step of associating payment information with said link.
- 13. The method of claim 12 in which said service provider provides information for a fee.
- 14. A method of providing a service for a fee, comprising the steps of:
  - a. receiving an connect request containing payment information over a network; and
  - b. providing the service once said payment information is determined to be valid.
- 15. A system for providing a service for a fee, comprising:
  - a. a network;
  - b. at least one computer connected to said network and configured to generate a connect request containing payment information; and
  - c. at least one server connected to said network

configured to extract payment information received with a connect request and to provide a service when said payment information is determined to be valid.

- 16. The system of claim 15 in which said service includes providing information.
- 17. A computer program product, comprising:
  - a memory medium; and
  - a computer program stored on said memory medium, said program comprising instructions for generating a document containing a link to a network address and associating payment information with said link.
- 18. A computer program product, comprising:
  - a memory medium; and
  - a computer program stored on said memory medium, said program comprising instructions for receiving an connect request containing payment information over a network and providing a service once said payment information is determined to be valid.
- 19. A computer controlling product, comprising:
  - a memory medium; and
  - a document stored on said memory medium, said document containing a link for connecting to a remote computer said link containing payment information.
- 20. A computer controlling product, comprising:
  - a memory medium; and
  - a document template stored on said memory medium, said document template containing a slot for identifying information for connecting to a remote computer and payment information.

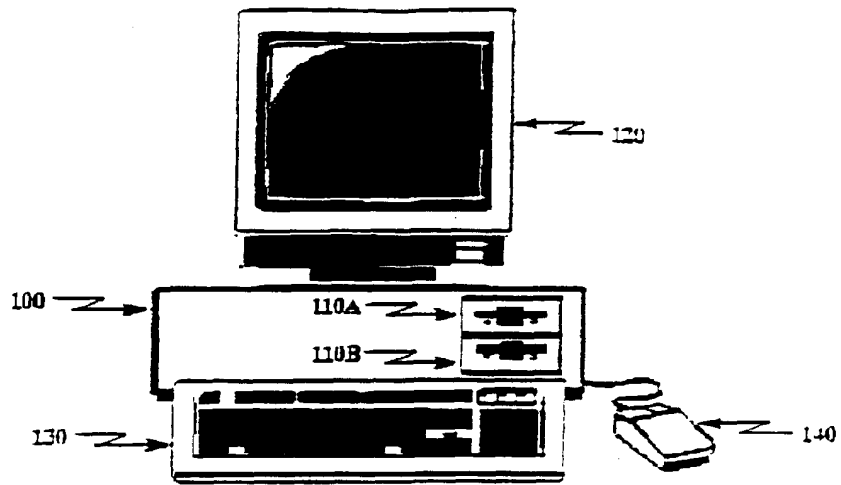


Figure 1A

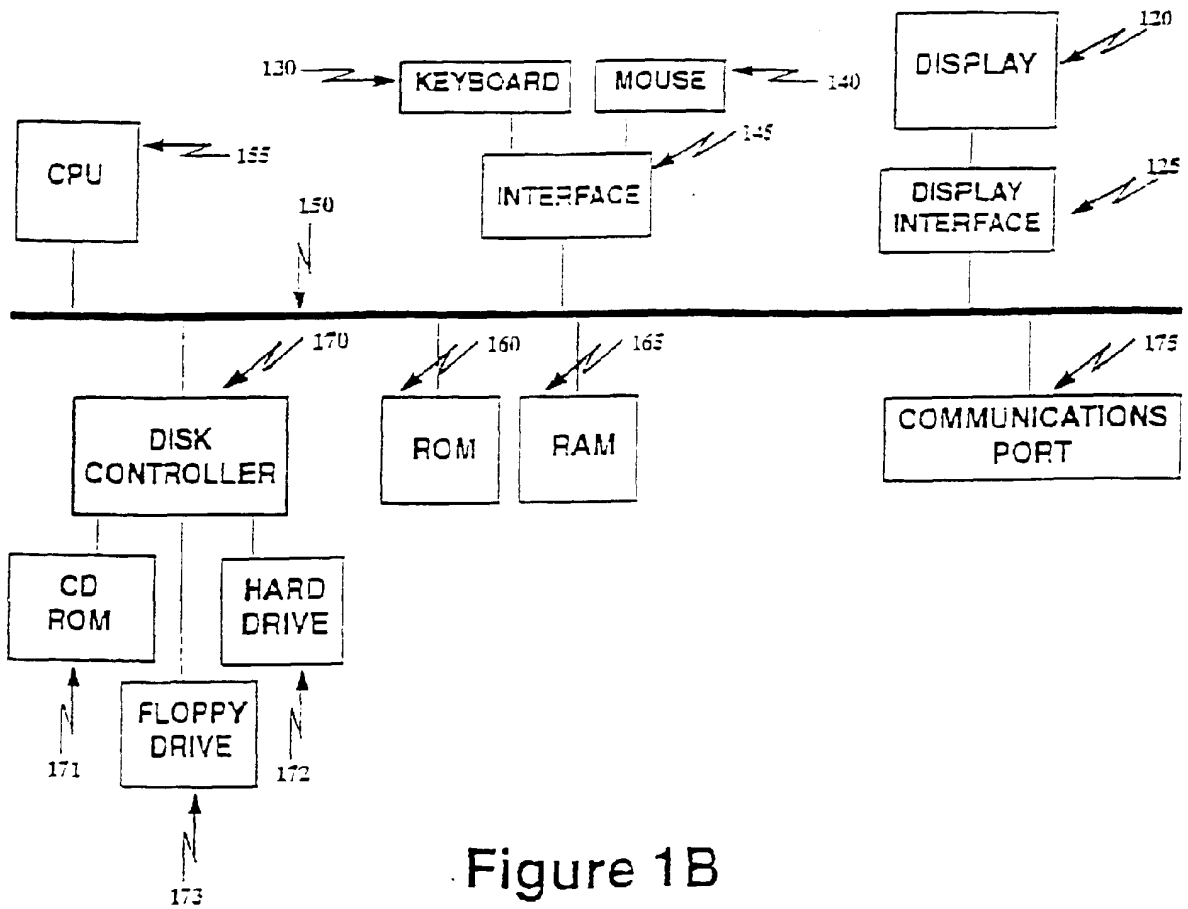


Figure 1B



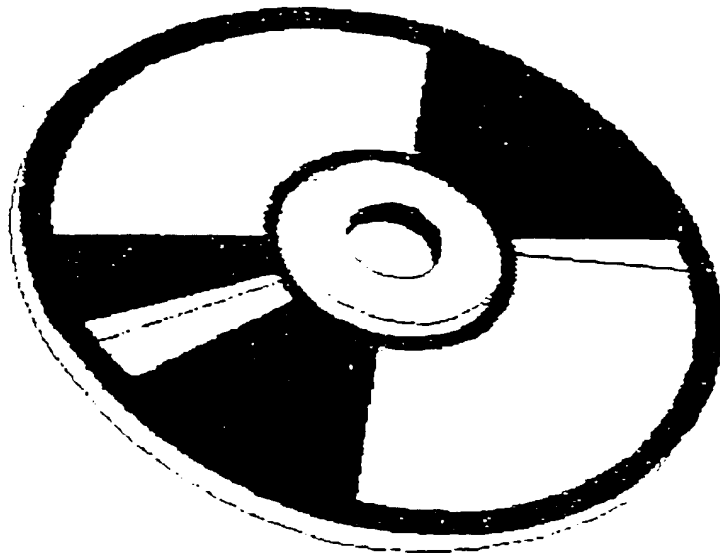


Figure 1C

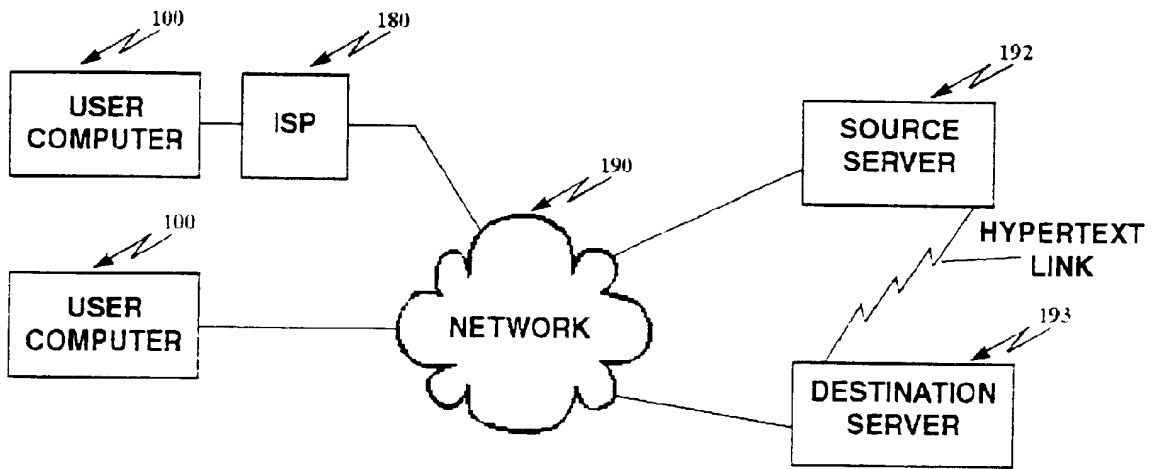


Figure 1D

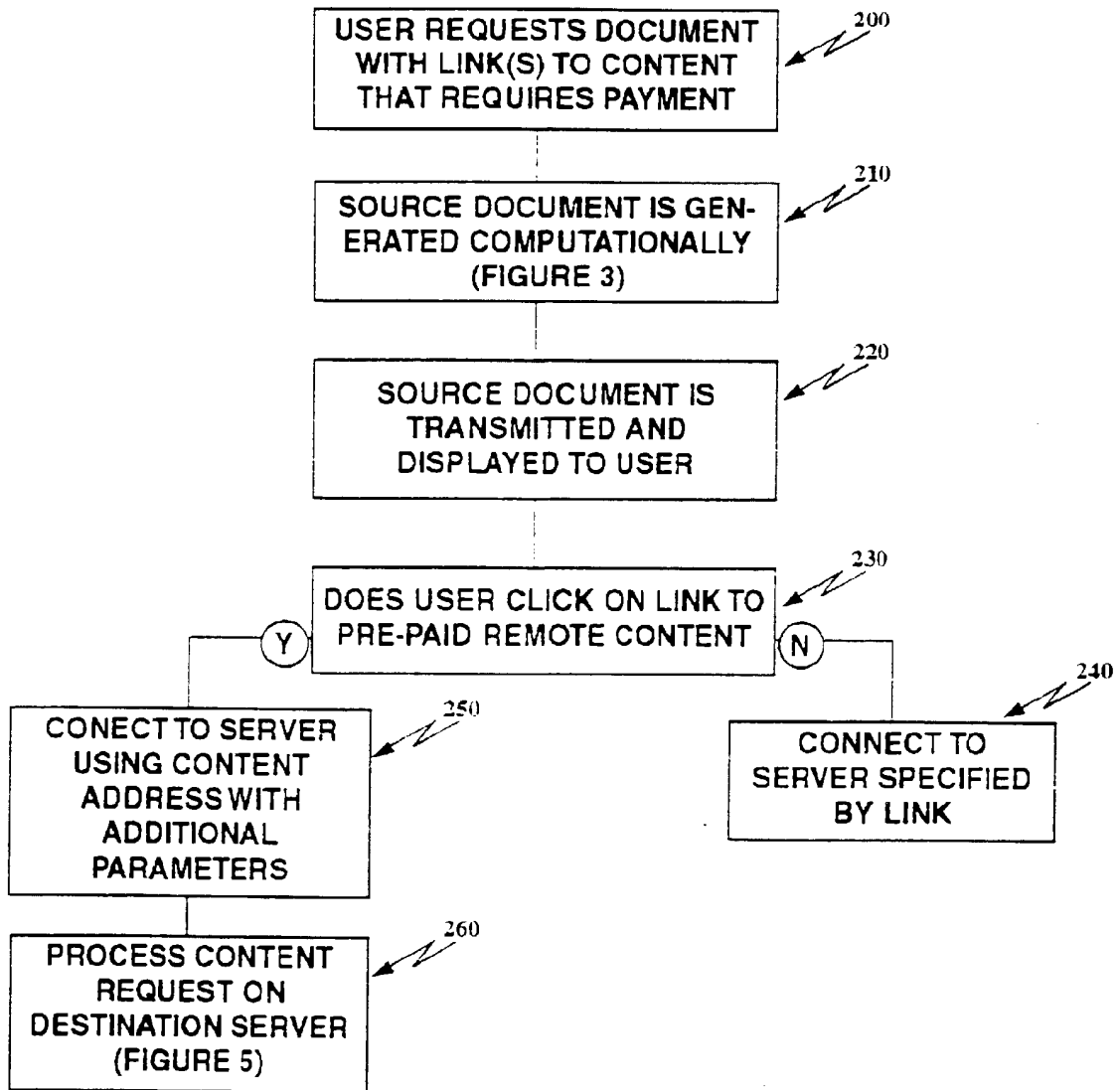
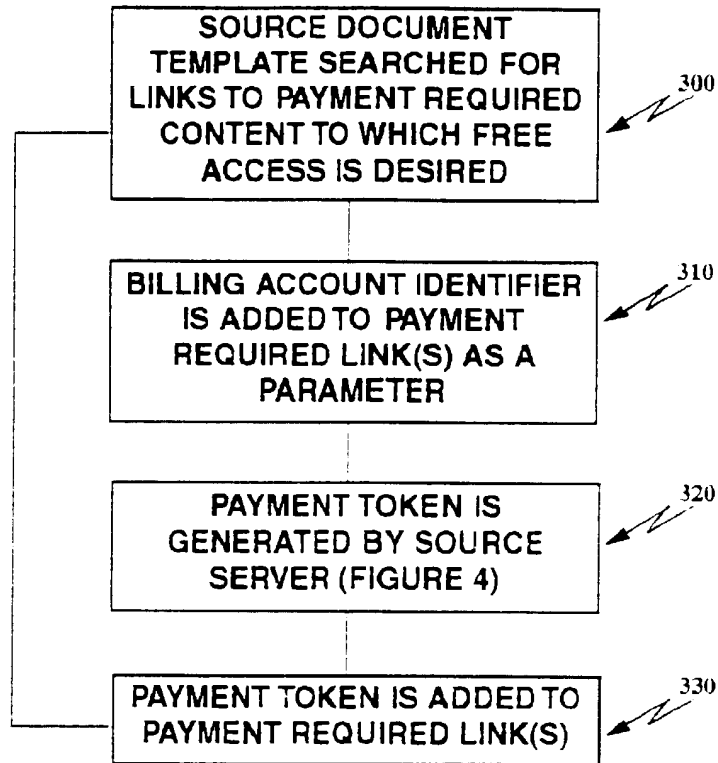
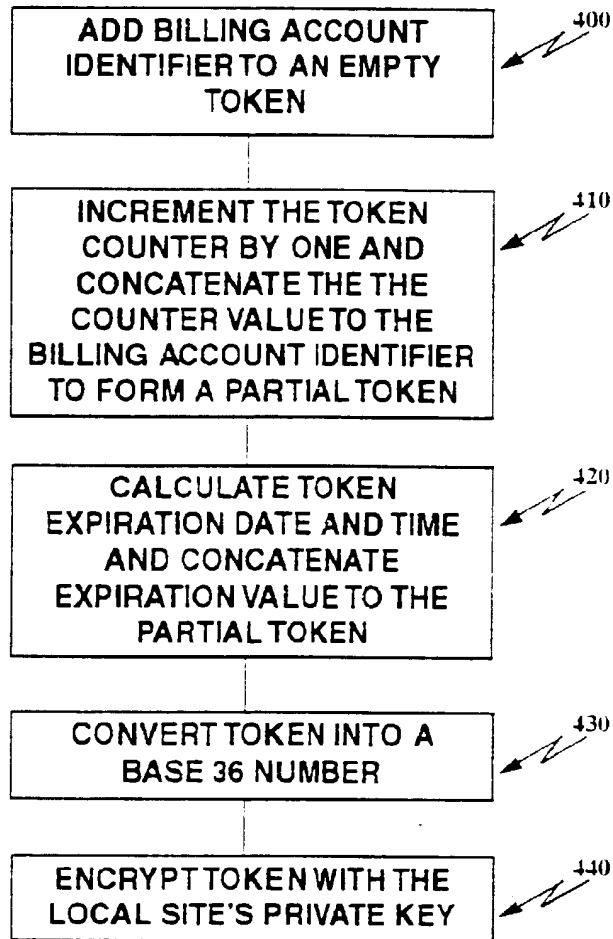


Figure 2



**Figure 3**



**Figure 4**

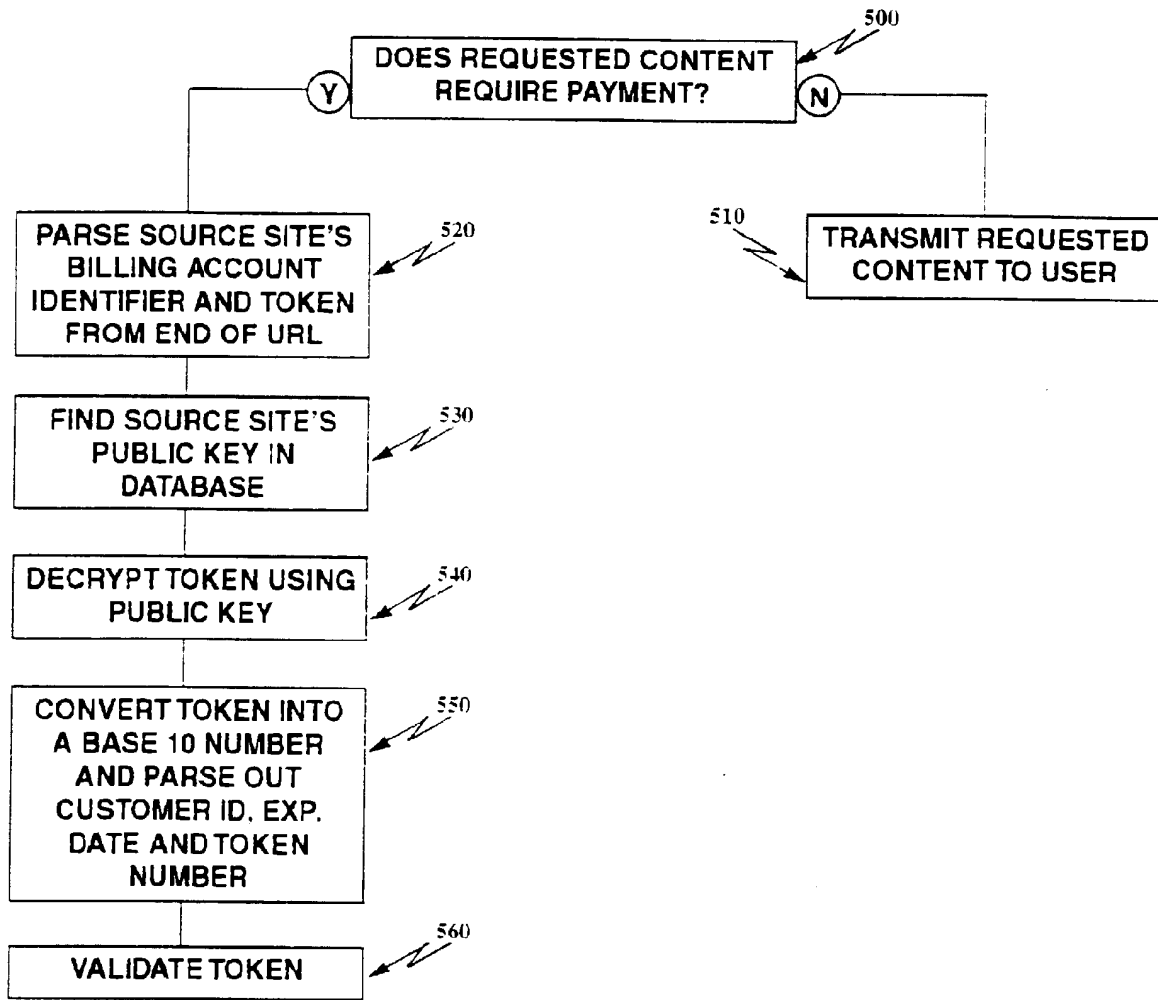


Figure 5

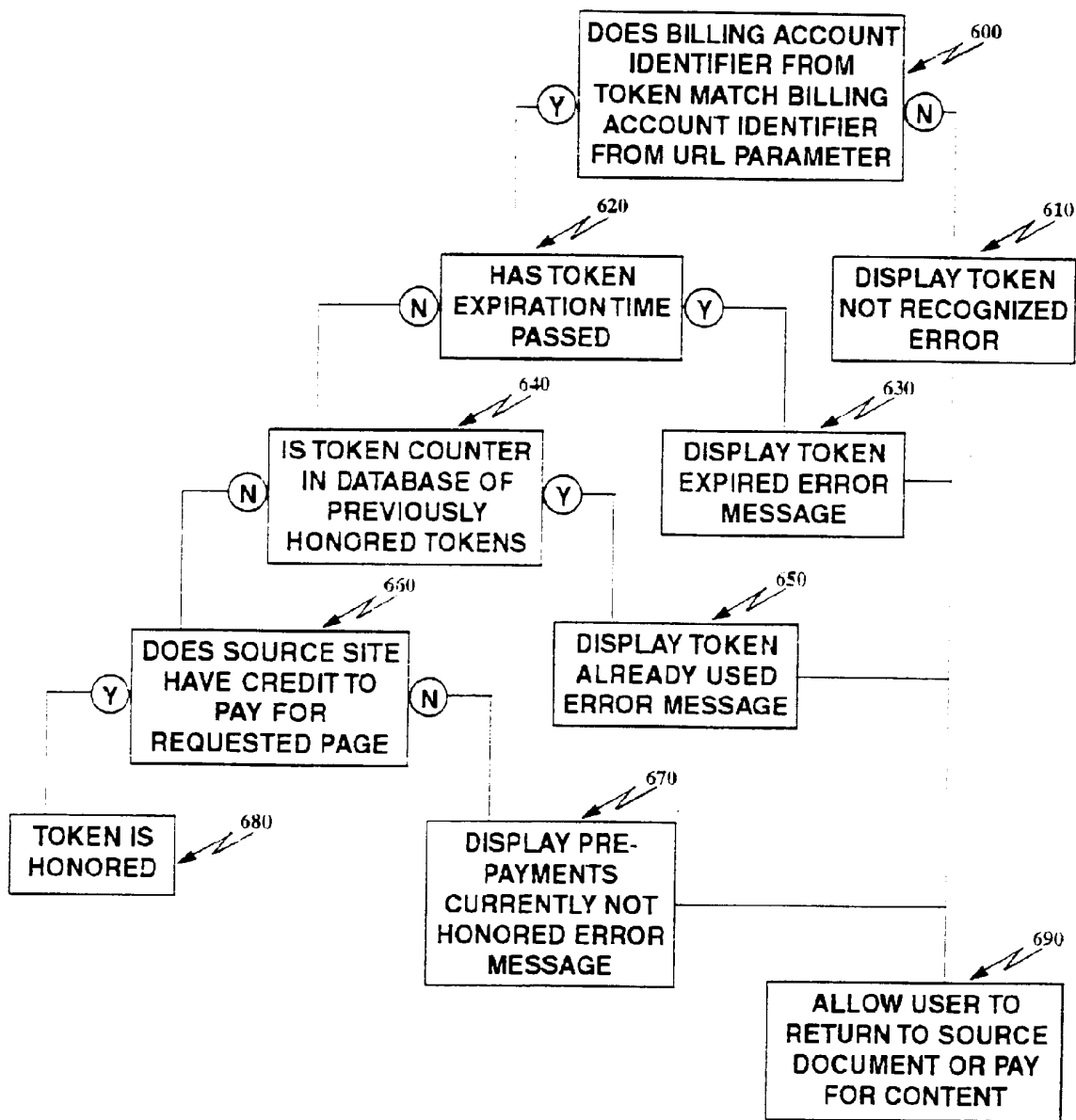
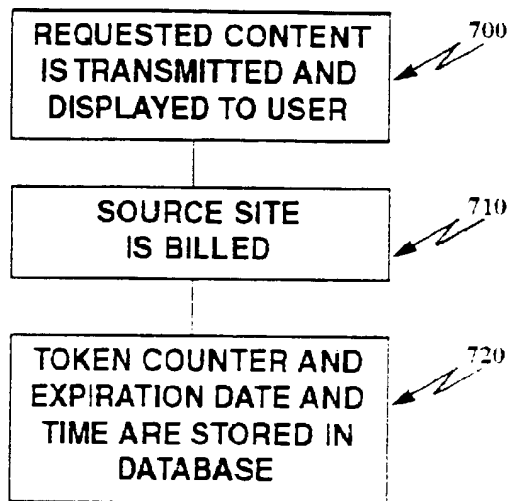
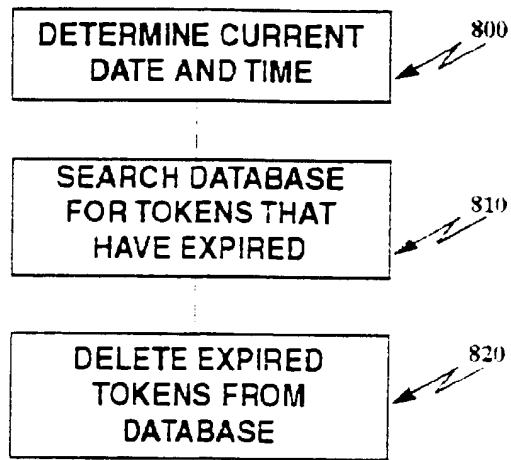


Figure 6



**Figure 7**





**Figure 8**

HREF = "http://www.payee.com/directory/page.html?12345+TOKEN"

The diagram shows the URL "http://www.payee.com/directory/page.html?12345+TOKEN" with four annotations: 900 points to the entire URL, 920 points to the path "/directory/page.html", 930 points to the query string "?12345+TOKEN", and 940 points to the token "+TOKEN".

**FIGURE 9**

0001234500005725920000

The diagram shows the number "0001234500005725920000" with three annotations: 1010 points to the first five digits "00012345", 1020 points to the next five digits "00005725", and 1030 points to the final five digits "920000".

**FIGURE 10**



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:  
**13.10.1999 Bulletin 1999/41**

(51) Int Cl.<sup>6</sup>: **G07F 7/10**

(21) Application number: **99200967.0**

(22) Date of filing: **26.03.1999**

(84) Designated Contracting States:  
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
 MC NL PT SE**  
 Designated Extension States:  
**AL LT LV MK RO SI**

- **Guzman, Marc A.**  
 California 92586 (US)
- **Boyd, Nik**  
 Los Angeles, California 90066 (US)
- **Smushkovich, Yosif**  
 Santa Monica, California 90403 (US)
- **Pinn, Fred**  
 California 91406 (US)

(30) Priority: **30.03.1998 US 79803**

(71) Applicant: **Citicorp Development Center, Inc.**  
**Los Angeles, California 90066 (US)**

(74) Representative: **Hynell, Magnus**  
**Hynell Patenttjänst AB,**  
**Patron Carls väg 2**  
**683 40 Hagfors/Uddeholm (SE)**

(72) Inventors:  
 • **Pan, Jack C.**  
**California 91748 (US)**

(54) **Method and system for managing applications for a multi-function smartcard**

(57) A method and system for managing applications for a multi-function smartcard makes use of a resident master application and one or more monitor applications installed on the smartcard microcomputer to authorize downloading of new applications to the smartcard and to manage applications on the smartcard. New applications are installed on the smartcard using a security mechanism of the monitor application. When a new application is installed, it is provided, for example,

with an operation key, cardholder information, and a digital certificate. The new application is registered in a software registry of the smartcard according to an object-oriented classifications, a copy of the registry is stored in an electronic deposit box, and the electronic deposit box is updated with operational data for the new application. The new application selectively shares one or more objects with objects of other applications on the smartcard on a restricted or unrestricted basis.

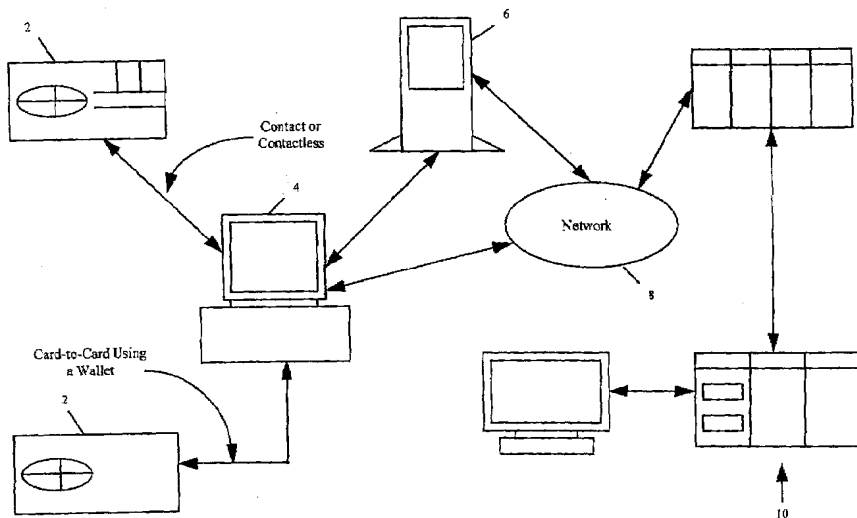


FIG. 1

EP 0 949 595 A2

## Description

### Cross-Reference to Related Applications

[0001] This application claims the benefit of U.S. Provisional Application No. 60/079,803 filed March 30, 1998.

### Field of the Invention

[0002] The present invention relates generally to smart cards, and more particularly to a method and system for managing applications for a chip-based smartcard which has processing capability and storage capacity for more than one smartcard function.

### Background

[0003] Single-function magnetic stripe cards, having a magnetic stripe on a plastic card, have been in use for many years. Such cards are based on magnetic stripe technology that can hold, for example, up to 40 characters of data on three tracks, including such information as the cardholder's name, account number, and expiration date. Existing credit, debit, and pay phone cards are magnetic stripe based.

[0004] Single-function chip cards having, for example, an 8-bit microprocessor chip, such as 8051 or 6805, embedded in the plastic card offer limited processing capability and memory storage capacity, such as 1 to 2K E<sup>2</sup>PROM. Such cards support a single function, such as stored value, and offer better security via tamper-resistant hardware and reduced on-line transaction and infrastructure costs over magnetic stripe cards. The contents of such cards are fixed at the time of issuance.

[0005] Multi-technology hybrid cards blend more than one card technology into a single card. Technologies that are applied to such cards include magnetic stripe, 2-D bar code, optical stripe, and chip. The rationale behind such a combination is to leverage the processing power of a chip with either the backward compatibility of the magnetic stripe or the storage capacity of the 2-D bar code or optical stripe. With regard to the chip-optical combination, a combination reader is capable of reading and writing both the chip and optical stripe portions of the card.

[0006] Other cards combine contact and contactless technologies. Contactless cards are the functional equivalent of contact cards but use radio frequency technology to interact with the card reader instead of being inserted into a device. A card with contactless technology transmits transaction data and records the data that it receives when passed within either one millimeter (close coupling), 8-10 centimeters (proximity), or 0.5-1 meter (vicinity) of the reader. With contactless cards, transaction times are reduced 20 to 30 times as compared to cards requiring insertion into a device. Such combination cards offer the convenience, performance,

and reliability of a contactless card, along with the security and functionality of a contact card. These cards have gained popularity as facility access and mass transit applications, such as bus, train, subway, and ferry, and have emerged as viable smartcard applications, especially when they are combined with payment methods on a single card.

[0007] While static multi-function chip cards are capable of handling multiple functions that were masked into E<sup>2</sup>PROM at the time of card initialization, they are static because applications and functions are fixed once the card is issued.

[0008] The smartcard industry has been around since the 1970s. However, with the exception of Europe, most of the world has not gone much beyond trials and pilots. For example, financial institutions, such as banks, have introduced stored value cards, such as VISA CASH and MONDEX, to customers and merchants in pilot programs. In such pilot programs, stored value cards have been tested in densely populated areas to help reach a critical mass of acceptance in the marketplace of consumers and merchants and to establish interoperability at merchant point of sale (POS) terminals.

[0009] While the increasing rate of smartcard usage is encouraging, it is also evident that single-function smartcards, such as stored value or pay phone cards, are a hard sell in the United States. This is mainly due to the convenience of cash and the ubiquity of credit card usage. Hence, stored value applications, at best, can be considered applications that are necessary elements of any real world smartcard programs, but are not sufficient in themselves to create a critical mass of smartcard acceptance.

[0010] Since its inception in the 1970s, a first movement in the smartcard industry began at the genesis of the technology, when a chip-based plastic card was developed to replace its magnetic stripe counterpart. Such a card offered added security and reduction in costs associated with on-line transactions and their underlying infrastructure support. A second movement can begin in the smartcard industry with the advent of a dynamic, multi-function smartcard.

[0011] The United States had little active involvement in the first movement, because of the establishment in the telecommunications infrastructure and the ubiquity of credit card usage. However, the United States can be a leader in the second movement, because of reliance by the electronic commerce industry on the smartcard to offer much needed portability, security, encryption, and authentication. Development of technologies, such as a Java card platform can allow the smartcard industry to realize the advantage of "write once, run anywhere" in which an application needs to be written only once and can then run on any card from any manufacturer.

### Summary of the Invention

[0012] It is a feature and advantage of the present in-

vention to provide a method and system for managing applications for a multi-function smartcard, which allows cardholders to carry less cash and affords cardholders nomadic access to financial and other services at any time or place and via any device.

**[0013]** It is a further feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard, which enables cardholders to organize personal information.

**[0014]** It is an additional feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard, which allows cardholders to carry fewer cards and to use the same card to conduct a suite of applications.

**[0015]** It is another feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard, which offers cardholders a means to back up their valuable information on the card.

**[0016]** It is a still further feature and advantage of the present invention to provide a method and system for managing applications for a multi-function smartcard, which affords cardholders the ability to store all types of information, such as emergency information or insurance information on the card.

**[0017]** It is still another feature and advantage of the present invention to provide a method and system for managing applications for multi-function smartcard, which can be customized by cardholders selecting applications based on personal needs and preferences.

**[0018]** To achieve the stated and other features, advantages and objects of the present invention, an embodiment of the invention provides a method and system for managing applications for a multi-function smartcard, such as adding new applications or applets to the smartcard for a cardholder, which includes, for example, installing a monitor application for the new application on the smartcard microcomputer, authorizing download of the new application by the monitor application and by a master application resident on the smartcard, and downloading the new application to the smartcard microcomputer. Key hardware components of the system include for example, the smartcard embedded with a microcomputer, a terminal, a network, and a server, such as a financial institution server. Important aspects of the card application platform are the master application and the monitor application. The master application serves as an arbiter, a gatekeeper, and a message dispatcher on the smartcard, and the monitor application is a special applet supplied by an applet provider, which controls the installation of the provider's applet or applets on the smartcard.

**[0019]** In an embodiment of the present invention, the monitor application is installed, for example, by downloading the monitor application from a server, such as an electronic customization depot, which includes functionalities of either or both of an applet server and a mon-

itor application server. The monitor application is downloaded, for example, at a terminal, which is any one of a number of access devices, such as an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, a land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, or a combination contact and contactless reader. The monitor application is downloaded, for example, at the terminal from the server over a network, which is either public or proprietary. In any event, initializing the monitor application with a key provided, for example, by a server, either during initialization of the smartcard or after the smartcard has been issued, is an aspect of authorizing download of the new application. Another aspect of authorizing download of the new application is registering an application identifier for the new applications with the monitor application and subsequently with the master application for dispatching of messages.

**[0020]** In an embodiment of the present invention, a security aspect of downloading the new application to the smartcard is verifying the identification of the cardholder, for example, by an application on the smartcard microcomputer. Such identification is done, for example, by a PIN of the cardholder or with biometric data for the cardholder. The latter is performed, for example, by a scanner at the terminal, and the biometric data, such as the cardholder's finger print, is compared with a reference template on the smartcard. Another security aspect of downloading the new application is authenticating the smartcard, for example, by the server.

**[0021]** In an embodiment of the present invention, the cardholder is offered a selection of service options by the system, including the option to download a new application to the cardholder's smartcard. Upon selecting the option to download a new application, the cardholder is offered a list of qualified new applications, according to pre-defined parameters, from which to select. The pre-defined parameters include, for example, whether a particular new application is supported by business based on the relationship between the cardholder and the financial institution, and whether there is sufficient space on the smartcard microcomputer to accommodate a particular new application.

**[0022]** In an embodiment of the present invention, the cardholder makes a selection of a new card application from the list of qualified new applications, and the new application is downloaded to the smartcard from the Server, such as the electronic customization depot, which has either or both of applet server and monitor application functionalities. The new application is downloaded at the terminal, which is any one of the smartcard access devices, such as an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, a land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, or a combination contact and contactless reader.

[0023] In an embodiment of the present invention, the new application is downloaded over the network, which is public or proprietary, and installed on the smartcard microcomputer. The new application is installed using a security mechanism of the monitor application, and the new application is supplied with an operation key. The new application is also supplied with cardholder information, as well as a new digital certificate. The new application is registered in a software registry of the smartcard microcomputer, according to an object-oriented classification of the software registry. A copy of the smartcard registry is furnished to an electronic deposit box of the financial institution, and the electronic deposit box is updated with a copy of operational data for the new application. At least one object of the new application is selectively shared with at least one object of another application on the smartcard, and the selective sharing is one or both of restricted and unrestricted sharing by the new application.

[0024] Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention.

### Brief Description of the Drawing

#### [0025]

Fig. 1 is a schematic diagram which shows an overview of examples of the key components and the flow of information between the key components of the system for an embodiment of the present invention;

Fig. 2 is a chart which shows a sample of layered hierarchy in the smartcard platform for an embodiment of the present invention;

Fig. 3 is a schematic diagram which amplifies the flow of information shown in Fig. 1 and provides further detail regarding the process of selecting and securely downloading an applet onto the smartcard for an embodiment of the present invention; and

Fig. 4 is a flow chart which provides further detail regarding the process of selecting and securely downloading an applet onto the smartcard for an embodiment of the present invention.

### Detailed Description

[0026] As smartcard technology has evolved from the single function magnetic stripe card, the cost of each card technology is proportional to the capability it delivers. For example, a rough estimate of cost for various card technologies ranges about \$0.15 per card for single function magnetic stripe cards, about \$2.50 for a single function chip card, about \$3 per card for multi-technology hybrid cards, about \$4 for a static multi-function chip card, and about \$7 per card for contact-contactless

combination cards. A rough estimate of the cost of a multi-function chip card for an embodiment of the present invention is in the range of about \$9. Moore's law, which projects that chip processing power doubles while the cost reduces in half every 12 to 18 months, indicates that as the demand for a multi-function card rises over time, the corresponding cost will decline steadily as time passes.

[0027] In an embodiment of the present invention, a cross-industry multi-function smartcard can handle more than one application and can support the installation of new applications after the card has been issued. Application functions of a multi-function smartcard include, for example, payment vehicles, such as credit, debit, and stored value. Other functions of a multi-function smartcard include, for example, access keys for facility and network access, information manager for managing an individual's profile, demographic, and preference information, cryptographic engine for conducting encryption and authentication, and marketing tool for loyalty programs and coupons.

[0028] In an embodiment of the present invention, given the possible combinations of application functions, a multi-function smartcard serves as a bridge between the physical world and the virtual world. For example, a cardholder can use the same card to conduct purchases over the Internet and at merchant POS terminals. A smartcard infrastructure platform, such as a Java card platform, supports a multi-function card environment which is open, secure, multi-functional, dynamically downloadable, chip platform independent, and broad programmers based.

[0029] In an embodiment of the present invention, it is noted that the term multi-function and multi-application smartcards have different meanings to different groups of people. The differences are articulated as differences between a function and an application. A function is a generic concept, while an application is the actual realization of the concept in particular implementation. For example, electronic purse or stored value is a function, while, for example, VISA CASH or MONDEX purse is an application. The correspondence between the two is many-to-many, in that many applications can be classified into a single function, as in the case of electronic purse, and many functions can be embodied in a single application. For example, Visa's VIS application consists of both credit and debit functions. Therefore, a multi-function smartcard is defined, for example, as a chip-based plastic card equipped with the necessary processing capability and storage capacity to handle more than one smartcard function, and thus more than one application, which are either installed at the time of issuance or loaded during runtime.

[0030] In an embodiment of the present invention, a broad platform strategy is applied from end-to-end, allowing simultaneous download and upgrade of software, from the card to the terminal and, ultimately, to the server. The system provides a flexible distributed archi-

ture, whereby the intelligence or processing capability is distributed throughout the system. For example, depending on application needs and business requirements, migration of processing capabilities from a terminal, such as an electronic wallet, to the card or to the server is permitted. With such an end-to-end perspective, system-wide concerns such as security, performance, interoperability, and standardization are reflected and addressed.

**[0031]** In an embodiment of the present invention, industry-specific application templates or generic applications are created that can be derived or inherited to produce specialized applications. Templates facilitate reuse, enable customization, and promote interoperability. Standards and interoperability are tightly coupled, and standards enable interoperability. Toward that end, a reinvention of the EMV standard adds stored value to the existing debit and credit functions. Similarly, incorporation of smartcard capability in the Secure Electronic Transaction (SET) standard solidifies a chip-electronic commerce vision as the industry moves forward.

**[0032]** In an embodiment of the present invention, there are, for example, three areas of primary focus in the development of a card application platform. One such area is secure dynamic application download, which includes, for example, policies and mechanisms for securely installing card applications on a smartcard after the card has been issued. Another such area is on-card application interactions, which includes, for example, mechanisms for allowing card applications to discover and safely interact with each other. An additional such area is off-card application interactions, which includes, for example, mechanisms for supporting secure interactions between on-card and off-card applications and for supporting advanced system management.

**[0033]** In an embodiment of the present invention, a dynamic multi-function chip card has on-card infrastructure support to facilitate post-issuance download of new applications. It is dynamic because card applications can be added or deleted after the card is issued, and an embodiment of the present invention provides an end-to-end architecture to facilitate such an operation. Relationship cards, such as Bankcard and Citicard, have traditionally been the vehicle for extending services, for example, to customers of a financial institution, such as Citibank. A multi-function card provides a relationship card for the financial institution that integrates, for example, stored value (pay before), debit (pay now), credit (pay later), and Citicard (ATM access), with other cross-industry services as part of the financial institution's overall strategy to broaden and deepen the relationships with its customers. Further, by incorporating the credit functionality, such as Bankcard, as part of the relationship, the financial institution maintains its brand leadership while extending financial services relationship, for example, for Bankcards.

**[0034]** In an embodiment of the present invention, the multi-function smartcard affords nomadic access by the

portability and mobility of multi-function smartcards. Such cards are an essential part, for example, of a new distribution model, in that the cards are used for access at a multiplicity of delivery vehicles, such as the Internet, GSM phone, cable, and WebTV, over all distribution channels. With such nomadicity, a multi-function smartcard enables a customer to conduct financial services anywhere, anytime, and via any device.

**[0035]** In an embodiment of the present invention, a multi-function smartcard supports and maximizes the global position of a financial institution, such as Citibank, in consumer and business electronic commerce, as the financial institution's core business lies in the transfer of value or movement of money and the extension of credit and related services. Lack of security and resulting proneness to fraud inherent in magnetic stripe cards costs financial institutions millions of dollars each year. The tamper resistant hardware and on-card infrastructure support of smartcards offers added security and cost savings for issuers and customers alike.

**[0036]** In an embodiment of the present invention, a primary benefit offered by a multi-function smartcard is convenience. Such cards provide great value to consumers, for example, by allowing consumers to carry less cash, by affording consumers nomadic access to financial and other services anywhere, anytime, and via any device, and by helping consumers to organize personal information. Another benefit which such cards offer consumers is consolidation. Consumers are attracted by the idea of combining everything in one place or in one card. Consolidation allows consumers to carry fewer cards in their wallets and to use the same card to conduct a suite of applications. Such a card is truly the ultimate thin client. As more and more information is consolidated on the card, an issue arises about the potential loss of the card. The financial institution offers a means for its customers to back up their valuable information on the card, which puts the financial institution in a unique market differentiating position and further strengthens its relationship with its customers.

**[0037]** In an embodiment of the present invention, a further benefit afforded customers by such a card is information storage. The concept of storing information on the card is a powerful proposition to consumers. This not only saves time, as in the case of filling forms, but can also be lifesaving, as in the case of storing important emergency information, such as allergies to medications or insurance information. A still further benefit afforded to customers by such a card is customization. With the dynamic downloadability of the multi-function card environment, consumers are able to customize the card by selecting applications based on personal needs and preferences. This puts the control of the card back to the consumer so that the card truly reflects the consumer's personality and lifestyle.

**[0038]** An embodiment of the present invention moves from a terminal-centric world to a customer centered, smartcard-centric world in which the smartcard is

regarded as the ultimate thin client. The smartcard holds the cardholder's identity, such as biometrics, along with other payment and access vehicles that allow the cardholder to conduct transactions anywhere, anytime, and via any device. With such portability, the smartcard can truly enable nomadic access to the various services through both the physical and the virtual worlds.

**[0039]** In an embodiment of the present invention, interoperability means different things at different levels of an end-to-end architecture. In essence, it means that two or more applications or participants can use each piece of the infrastructure, such as the card itself, the terminals interacting with the cards, the electronic customization depot for card applications, the acquisition and card management systems, and the settlement systems. Interoperability is a foundation necessary for operating multi-function cards and is thus a very important feature of the multi-function smartcard in the electronic commerce industry. Interoperability is a vital feature at all levels and is in place, for example, in the card infrastructure, among card applications, at the terminal-to-card interaction, and within the network infrastructure.

**[0040]** In an embodiment of the present invention, at the card infrastructure level, the system has a standardized virtual machine interface and the supporting class libraries, such as provided by a Java card infrastructure. At the card application level, in order for applications from different service providers, that are either within an industry or across industries, to interact with one another, the system has a set of pre-defined interaction models at the terminal or network system, as well as in the card infrastructure, such as the Java card infrastructure. At the terminal level, terminals are powerful enough such that different cards with different applications can be read on more than one terminal type. For example, an airline loyalty terminal is able to read stored value cards to speed payment, and secure access applications work in electronic ticket, gate access environments. At the network infrastructure level, a network infrastructure supports multiple application messaging scheme and/or communication protocols, as well as application downloads.

**[0041]** In an embodiment of the present invention, a card platform, such as the Java card platform, serves as a standard for smartcard infrastructure. A card platform, such as the Java card platform, as the infrastructure for the smartcard is designed to achieve interoperability of applications both on the card and at the terminal. Specifically, a smartcard application designed for the Java card can run on or be added to any card supporting Java Virtual Machine (JVM) and Java class libraries. Similarly, interoperability at the terminal is achieved when the terminal has a low-level card agent or service provider that is capable of conversing with Java card applications on the other end. In such an environment, cards issued by different vendors seamlessly run on terminals from any vendors with varying capabilities.

**[0042]** In an embodiment of the present invention while financial services applications have been prototyped on the Java card 1.0 platform, for example, via Schlumberger's Cyberflex cards, cross-industry applications utilize the next generation smartcard platform, such as the Java card 2.0 specification. This platform serves to demonstrate the capability of such a multi-function card environment and to demonstrate how new applications can be added to the card post-issuance. Looking beyond the card infrastructure, an architectural innovation enables development of a coherent end-to-end application. A suite of platforms, such as Java platforms, is identified that are intended for different delivery devices and systems. In descending order of scope, such Java platforms encompass, for example, Java JDK, personal Java, embedded Java, Java wallet, Java card, and picoJava.

**[0043]** In an embodiment of the present invention, templates are the basic definition of applications which are essential in defining a generic application such as stored value, loyalty, or telecommunications. They are the basis on which can be built specific, branded versions of the application for a financial institution's customers. Templates are about function rather than branded identity. In a more technical sense, templates offer the foundation for building generic applications. Template facilitates reuse, thus shortening the development cycle. Specialized applications are enhanced from generic ones. Templates facilitate interoperability between applications, subject to firewalls. Therefore, it is advantageous to have a baseline stored value application that works in the same way across, for example, MASTER CARD/MONDEX, VISA, and EUROPAY.

**[0044]** In an embodiment of the present invention, industry-specific application templates, or generic applications are created that can be derived or inherited to produce specialized applications and achieve interoperability at the card application level. Card application development is coordinated by the use of templates. Templates facilitate reuse, enable customization, and promote interoperability. In order to facilitate the process, Smart Card Special Interest Groups, or SJGS (one per industry segment) are formed. Each SJG is responsible for individual industry template development. The task is similar to the work done by the travel industry, under the IATA Smart Card Subcommittee and LATA Resolution 791 to specify an Airline ICC.

**[0045]** In an embodiment of the present invention, standards and interoperability are tightly coupled, and standards enable interoperability. Toward that end, the EMV standard is re-invigorated to add stored value to the existing debit and credit functions. This enforces a unified electronic purse definition covering the functionality offered, for example, by VISA, PROTON, and other stored value products. Similarly, the SET standard incorporates smartcard capability to solidify a chip-electronic commerce vision as the industry moves forward.

**[0046]** In an embodiment of the present invention,



other standards that facilitate interoperability are, for example, Microsoft's PC/SC and NCI's Open Card Framework (OCF). Finally, financial institutions work closely with the telecommunications and set-top box industries to assure that the next generation GSM and the set-top box systems comprehend the needs of "nomadic" access to the various financial services, including home banking and electronic commerce. This is realized by cell phones and set-top boxes offering a two-card scenario, in that a user controlled smartcard provides secure identity in addition to customized applications, while an independent card issued by the specific industry controls the access to the underlying telecommunications or Internet services.

**[0047]** In an embodiment of the present invention, a smartcard has present and potential future capabilities in the electronic commerce age. However, in the age of Internet and electronic commerce, security threats continue to dominate the consciousness of the technology marketplace. In order to conduct secure exchange of purchasing orders and payment authorizations, public-key based financial transactions are of essence. For example, Secure Electronic Transaction (SET) has established itself as the leading standard in the electronic commerce world. Presently, certificates are an intrinsic part of the SET process. They are stored in the PC at the consumer end. Aside from security, lack of portability or mobility is a drawback for the approach. Hence, it is necessary to maintain separate certificates, for example, for use at home and in the office.

**[0048]** In an embodiment of the present invention, portability concern with a smartcard is resolved by putting the certificates on the card. Difficulties created by the present certificate size (around 1 K bytes) and the necessity for a chain of certificates to conduct an authentication process are alleviated as the capacity of the card and the industry standards evolve, such that holding certificates or some cryptograms as being proposed by EMV are as feasible as storing the cardholder's PIN. Alternatively, storing one or more private keys on the card, while leaving certificates on the PC, also provides an interim solution.

**[0049]** In an embodiment of the present invention, verification allows the card to uniquely verify the identity and authenticity of the cardholder. The most common verification mechanism is the use of PIN. However, the PIN mechanism is based on the secrecy of the information. If it is lost, stolen, or if the cardholder forgets, the mechanism becomes insecure or unreliable. Biometrics oriented verification offers high accuracy and confidence in identifying the owner without the burden of PIN memorization. The reference template or templates of the cardholder's biometrics, along with one or more verification algorithms is stored on the card, such that a person's personal identification never leaves the card. As an alternative to on-card template comparison, the exchange is secured between the card and the terminal. In addition, the two devices are mutually authenticated

to minimize the threat of exposing the confidential information in an unsecured environment.

**[0050]** In an embodiment of the present invention, the smartcard is equipped with either a high-performance microprocessor or a crypto co-processor to be capable of providing privacy, integrity, confidentiality, and non-repudiation for trusted transactions. This is accomplished through encryption (DES symmetric key or RSA public key based) and authentication (comparing digital signatures). In order to alleviate concerns about time consuming, computation intensive operations, such as the RSA public key operation, techniques such as Chinese Remainder Theorem (CRT) are applied to further accelerate the computation process. Alternatively, Elliptic Curve Cryptography (ECC) also offers comparable security with shorter key length. Ultimately, it is preferable to create private keys from within the card and use the keys to generate digital signatures using, for example, 16-bit and even 32-bit RISC processors rather than older 8-bit smartcard technology.

**[0051]** Information stored on the magnetic stripe or in the PC has been known to be insecure and easily counterfeited or stolen. In an embodiment of the present invention, the smartcard is regarded as the hardware token that offers tamper resistance to physical attacks. In addition, information is further protected against unauthorized access through configurable access control measures such as PIN entry or biometrics comparison for reading or writing files on the card.

**[0052]** In an embodiment of the present invention, the smartcard has encryption capability to secure a message exchange between the card and the terminal (or the host) by encryption or message authentication code generation (MACing) the data. Data is downloaded to the card for information update or configuration setting. Provision is made to allow uploading of data or tokens/tickets to a remote server for short-term storage or long-term backup, for example, for a cardholder who wishes to temporarily store his/her electronic tickets to a remote server before using them. Further, in order to allow the financial institution to restore a stolen or lost card, provision is made for customers to backup the information on the card.

**[0053]** In an embodiment of the present invention, the smartcard has the ability to download new applications after the card is issued. This goes above and beyond the normal loading of data to and from the card and allows the cardholder to customize the card functionality to meet his/her own preference. For card issuers, such as Citibank, this also enables, for example, software upgrade, addition of new applications, and introduction of security algorithms without having to re-issue the card. This is an attractive business proposition from the perspective of total cost of ownership.

**[0054]** In an embodiment of the present invention, a number of categories of card applications are provided which are not mutually exclusive. In migrating from a single-function card environment to a dynamic, multi-func-

tion card world, financial institutions and consumers may aggregate applications from one or more of the categories. For example, payment applications, such as debit, credit, and stored value can co-exist with such applications as loyalty program, facility access, and network access.

**[0055]** In an embodiment of the present invention, classification of applications into groups formulates a strategy which establishes a framework for developing applications within individual group or industry. For example, an information manager group is regarded as a generic template or, more precisely, a base class that, for example, can be enhanced to derive specialized applications, such as profile, demographic, and preference applications. Such a framework establishment is exploited to facilitate reuse and enable customization. In establishing a coherent interface across related applications, the accessibility to the grouped services for both on-card or off-card applications, such as an electronic wallet, is also maximized. Such a design principle lays the foundation in organizing applications for additional financial institution smartcard initiatives and drives toward standardization of interfaces for individual category or class of applications.

**[0056]** In an embodiment of the present invention, the stored value application offers a first view of what smartcard can offer as a cash replacement in an off-line environment. The payment applications are elements in a multi-function card environment. An integrated payment card includes all three payment methods, namely, debit, credit, and stored value, for consumers. The payment card serves as a bridge between the physical and the virtual worlds in the electronic commerce age. In addition to such open currency payments, other closed payment vehicles (in a form of barter) include, for example, electronic tickets and transit tokens (as a form of payment to the system), and theme parks tokens (used in a closed entertainment environment, such as GameWorks and Disneyland). Leveraging the stronger identification and verification capabilities, electronic benefits (another form of payment) are paid through the smartcard as well.

**[0057]** In an embodiment of the present invention, conducting secure and trusted transactions over the physical or virtual world requires, for example, a two-tier process of verification and authentication. The cardholder's identity is verified, and there is a mutual authentication between the card and the interacting device or server. In holding a cardholder's identity in the form of a PIN or a biometric template like finger print, the smartcard offers a means for secure access of facilities and networks by conducting or facilitating the verification process. The former requires the template matching algorithm to be resident, for example, on the card such that the verification is done locally.

**[0058]** In an embodiment of the present invention, once the cardholder's identity is successfully verified, the smartcard then performs mutual authentication with

a terminal or a remote server to ensure a trusted transaction. Given such capabilities, the card behaves as the access keys in both the physical world for facility access and the virtual world for network access and E-commerce transactions. A generic cryptographic framework is established as the foundation for developing cryptographic applications. Such a framework allows use of such services for both on-card and off-card applications to maximize reuse and shorten the time-to-market.

**[0059]** In an embodiment of the present invention, the smartcard enhances a trusted relationship between, for example, a bank and its customers, based on the secure storage of both value and information of the cardholder. Several types of information pertaining to a cardholder can be stored on the card. For example, personal identification, such as name, blood type, date and place of birth, mother's maiden name, address, and phone number can be stored. Profile and demographic information, such as marriage status, number of children and their ages, income level, and hobbies can also be stored. Further, preference information, such as language, frequent calling numbers, airplane seat assignment, and computer configuration can be stored on the card. Additionally, privilege and entitlement information, such as administrative status for computer and network access can be stored on the card.

**[0060]** In an embodiment of the present invention, the smartcard plays the role of an information manager on behalf of the cardholder that safeguards and manages the cardholder's personal information. This is important as consumer privacy is a leading concern in the smartcard and electronic commerce industries. Different kinds of information require different levels of security measures to authorize an access. Much of the trusted relationship between a financial institution, such as a bank, and its customers hinges on how well the financial institution manages its customers' personal information. A flexible yet secure information access mechanism is provided, such that applications like filling forms at a doctor's office can be automated without the concern of invasion of privacy.

**[0061]** In an embodiment of the present invention, the smartcard provides a marketing tool for both merchants and financial institutions by storing loyalty points or coupons for individual retailers. On-card loyalty applications provide cardholders flexible shopping benefits, including instant loyalty points reward and redemption, for both physical and Internet transactions. In addition, churches and schools can, for example, issue scrips to benefit their causes from the sales.

**[0062]** In an embodiment of the present invention, by allowing download of new applications after the card is issued, the smartcard offers a unique delivery channel in distributing customized services. The cardholder can determine the applications on the card and make adjustments as his/her lifestyle evolves. For example, the cardholder can delete rarely used applications and add new ones. The personalization capability is further am-

plified in conjunction with a multiplicity of delivery channels, such as cell phones, set top boxes, and network computers. Consumers are afforded added convenience and flexibility in conducting financial transactions and invoking services delivered through the smartcard.

**[0063]** Referring now in detail to an embodiment of the present invention, which is illustrated in the accompanying drawings, Fig. 1 shows an overview of the key components from a system-wide perspective of the architecture for an embodiment of the present invention. Referring to Fig. 1, the end-to-end architecture takes into account the issues and concerns from the card 2 to the terminal 4, to the front-end system 6, to the network 8, and, ultimately, to the back-end server 10. Such an end-to-end perspective is an important aspect of the system and enables reflecting and addressing system-wide concerns, such as security, performance, interoperability, and standardization. In this multi-function world, it is imperative to have such an understanding in order to gauge the needed performance and security for the card. This also enables addressing the interoperability and standardization concerns between the card 2 and the terminal 4, as well as between the terminal 4 and the back-end server 10. For example, the system architecture is designed such that security broken on one end can be remedied or minimized from the other.

**[0064]** Referring further to Fig. 1, five major components of the end-to-end architecture include, for example, the smartcard 2, the terminal 4, the front-end 6, the network 8, and the back-end servers 10. The card issuer has full control of the security measures both on the card 2 and at the back-end servers 10. The in-between terminals 4 and 6 and the networks 8 are regarded as insecure and are treated with special attention. On the other hand, intelligence or processing capability is distributed across the system. Depending on the application needs, intelligence is propagated from the card 2 to the terminal 4, and to the servers 10, or vice versa.

**[0065]** In an embodiment of the present invention, the smartcard 2, acting as the ultimate thin client, is the relationship card that is leveraged to further the trusted relationship between a financial institution, such as a bank, and its customers. In order to accomplish that, the card infrastructure supports the required multi-functionality and downloadability. An example of such a platform is Java card, which encompasses the virtual machine and the supporting class libraries. Fig. 2 is a chart which shows a sample of layered hierarchy in the card platform for an embodiment of the present invention. A card platform, such as the Java card platform, offers a layered hierarchy in its architecture. For example, a Java card virtual machine (JVM) 16 sits atop the card operating system 14 that is either proprietary or open, as in the case of Mondex's MULTOS.

**[0066]** In an embodiment of the present invention, the term applet means a smartcard application that is compact in size and downloadable over a public network. Referring to Fig. 2, a card architecture such as JVM 16

offers added security during runtime by providing bytecode verification to prevent unauthorized applets from being executed on the card. Bytecode is machine independent and is interpreted by the JVM 16. Sitting above the JVM layer 16 are the foundation class libraries 18, which offer the interface for building Java card applications. Such a framework based approach facilitates reuse and enables faster time-to-market for the application development. In order to further extend that vision, industry-specific and application-specific templates 20 are created, which are foundation class libraries that can be derived or inherited to produce specialized applications. Hence, interoperability is achieved at the card application level. Finally, at the top of the hierarchy is a suite of cross-industry applications 22 that co-exist harmoniously on the card 2.

**[0067]** In an embodiment of the present invention, a spectrum of terminals and access devices 4 have smartcard interfaces. These include ATMs, POS terminals, PCs with smartcard readers (either standalone or part of keyboards), personal digital assistants (PDAs), set-top boxes, cell phones, cable/satellite TV boxes, and various contact/contactless reader devices. The design provides a coherent architecture between the card 2 and the terminal 4, such that both card and terminal applications can be upgraded simultaneously to allow seamless migration. An electronic wallet residing, for example, on a PC or distributed over a network offers a vehicle for delivering payment services and information management over the Internet. The smartcard 2 is a natural extension of the wallet to physically contain some of the wallet functionalities. The smartcard 2 evolves as the physical embodiment of the wallet. Thus, a certain portion of the wallet functionalities are moved to the card 2, while others either stay on the terminal 4 or browser or move to the server. Distribution of intelligence across the network is realized in such a migratory fashion.

**[0068]** In an embodiment of the present invention, from an architectural perspective, the data of a wallet physically resides, for example, on the card 2 or in a remote server. The storage location is arranged based on the nature of the information and the constraint of capacity on the card 2. Regardless of the physical location, the information is accessible to the user transparently. In situations where the user wishes to have a conscious understanding of the actual data location so as to make a proper decision during transactions, the smartcard architecture facilitates such a decision-making process. Storing or backing up critical information on the server is a powerful mechanism to safeguard a cardholder's valuable information.

**[0069]** In an embodiment of the present invention, in the event that the card 2 is lost or stolen, a financial institution can confidently issue a new card with the original card information (not stored value) restored from the financial institution's servers. With this recoverability, the customers of the financial institution have a peace of mind, knowing that a trusted financial institution is se-

curing the information on their behalf. This, in turn, provides market differentiation for a financial institution, such as bank, as losing a card has become one of the top consumer concerns. In order to enable biometrics-based verification, a biometric scanning device, such as a fingerprint or hand geometry scanner, is installed at the terminal 4. The captured biometric data is compared with a reference template on the card 4 to verify the authenticity of the cardholder.

**[0070]** In an embodiment of the present invention, the front-end systems 6 serve as the front end to terminals 4. Their principal responsibility is to offer the necessary translation of message protocols between the terminal 4 and back-end servers 10. They often play the role of a middleware or gateway in a networking environment, such that smartcard-ready terminals 4 are transparent to back-end legacy systems 10. Networks 8 offer the plumbing in a distributed environment. Both public (open) and private (proprietary) networks are used in the system. The former include, for example, Internet, PLUS, Cirrus, and Star., whereas the latter includes, for example, Citishare.

**[0071]** In an embodiment of the present invention, in the financial services environment, back-end servers 10 deal with clearing and settlement functions. Several back-end services support operations in a dynamic, multi-function environment, such as Certificate Authority (CA), Electronic Customization Depot (ECD), Electronic Deposit Box (EDB), and Electronic Vault (EV). A financial institution can provide one or more of such services in order to provide market differentiation and to further the relationships with its customers. The particular services are devised logically according to their functions. More than one service can reside physically on the same server 10, depending on business needs and design decisions.

**[0072]** In an embodiment of the present invention, Certificate Authority (CA) is a trusted third party. It is responsible for issuing certificates to customers, merchants, and those who want to conduct public-key based transactions over the internet. Secure Electronic Transaction (SET) operations are certificate based. Thus, the CA inherently becomes an integral part of any secure transaction process. A financial institution can be a CA in order to maximize interactions with its customers.

**[0073]** In an embodiment of the present invention, an electronic customization depot behaves as an applet server and a monitor application server to offer a customer the options to customize the customer's card 2 by adding or deleting applets. As an applet server, it is the source for applet download and for card restoration. Each monitor application is responsible for establishing secure download of applets to the customer's smartcard 2. Load keys, for example, are stored in the monitor application to facilitate the operation. Counterparts of a safety deposit box and vault in the physical world are provided in a virtual world electronic deposit box and

electronic vault. Like a safety deposit box, whose purpose is to store customer's valuables in a trusted and secure environment, the electronic deposit box offers similar services to a financial institution's customers.

**[0074]** In an embodiment of the present invention, the financial institution stores or backs up valuable information on the smartcard 2 for a customer upon request. Collectively, electronic deposit boxes are aggregated within an electronic vault. In addition to holding customers' valuable information, including electronic tokens and tickets, an individual electronic deposit box also maintains a software inventory of each customer's card 2. With such an inventory, the financial institution is able to restore the card applications, for example, from the electronic customization depot, for a customer when the card is lost or stolen.

**[0075]** In an embodiment of the present invention, facilities are provided to support applications, such as secure dynamic application downloads, which are the policies and mechanisms needed to securely install card applications on the smartcard 2 after the card has been issued. Other such facilities include on-card application interactions, which are mechanisms for allowing card applications to discover and safely interact with each other. Additional such facilities include off-card application interactions, such as mechanisms for supporting secure interactions between on-card and off-card applications and advanced system management. On-card applications are frequently referred to as applets. Of necessity, applications installed on the smartcard 2 tend to be very small when compared with desktop, terminal, or mainframe applications and hence are called applets.

**[0076]** In an embodiment of the present invention, the smartcard application platform meets two overall security goals, namely, to ensure the security and integrity of the card's system components and to provide applets with scaleable mechanisms to ensure their own security and integrity. The overall security policy for the card 2 is that only authorized entities may have access to card resources; and this access is limited to the activities for which access has been granted. In order to insure that security goals of the financial institution are met, the card application platform includes several important elements, two of which are a master application and the monitor application. As a special system applet, the master application represents the card issuer. It provides global card services, including, for example, installing applets on the card 2, personalizing and reading global data, managing the card life cycle state, supporting external audits when the card is blocked, and maintaining a map of the monitor applications associated with each applet.

**[0077]** In an embodiment of the present invention, the system includes applets developed by other applet providers, as well as a financial institution's own applets. Thus, the card application platform supports the secure and confidential installation of applets from multiple providers. In order to support secure installation of applets,

the financial institution uses monitor applications. A monitor application is a special applet supplied by an applet provider. Each monitor application controls the installation of a provider's applet or applets. There can be multiple monitor applications on a card. Each monitor application represents a unique cryptographic relationship for a single applet provider. Using its unique combination of cryptographic mechanisms and keys, each monitor application manages the signature checking and decryption of applets loaded onto the card 2. Therefore, the installation and initialization of a monitor application on the card 2 is an essential step to support the secure download of a provider's applets.

**[0078]** Another important aspect of an embodiment of the present invention is the installation of the master application on the card 2, which functions in conjunction with the monitor application. The master application serves, for example, as an arbiter, a gatekeeper, and a message dispatcher on the smartcard 2. Direct application-to-application interactions on the card are not permitted. Instead, all interactions must go through the master application, serving as the arbiter, gatekeeper and message dispatcher on the card 2. The master application serves as an arbiter during inter-application communications. Any request initiated by one application is sent to the master application before it is routed to its destination application, for example, for preliminary checking to prevent bogus requests. Such a request can be, for example, a file access or a service rendition. In either case, it is up to the destination or receiving application to decide whether to honor the request.

**[0079]** The master application serves as a gatekeeper, for example, during dynamic application downloading to prevent unauthorized applications from being downloaded onto the card 2. In such capacity, the master application, working in conjunction with the individual monitor applications, performs necessary authentication and validation functions to ensure that the downloaded application originates from a legitimate source and that the content has not been altered.

**[0080]** The master application serves as a message dispatcher, for example, during terminal-to-card interactions. The message dispatching process is a simple, yet robust, message routing mechanism that ensures timely delivery of messages, while incurring little overhead. Each incoming message is routed sequentially to each application resident on the card 2, and each such application determines whether it is the intended recipient of the message. If so, the particular application processes the message and returns a "success" response. Otherwise, the application returns an "error" message, and the master application continues to forward the message to other applications on the card 2, until a "success" response is returned. Thereafter, subsequent messages are forwarded to the last successful application, until the particular application returns an "error" message, and the cycle is repeated.

**[0081]** Another important aspect of an embodiment of

the present invention is installation of a consolidated identification application (ID application) on the card 2. The ID application serves as a single placeholder for all personal profile related information to avoid duplication of data. When an application requires identification related information, the application submits its own identification and a clearance level, and the ID application determines the privilege, if any, to be given to the requesting application for data access. For example, a health care application can access the cardholder's blood type information, while a loyalty program cannot.

**[0082]** In an embodiment of the present invention, the installation and initialization of monitor applications can occur during card initialization. However, for maximum flexibility, the financial institution supports downloading and installing new monitor applications after the card 2 has been issued. To support this feature, a root monitor application is installed during card initialization and personalization. Subsequently, each downloaded monitor application allows the financial institution to download and install specific applets. Before the actual download and installation of an applet takes place, the appropriate monitor application authorizes the download of the applet. Therefore, before an applet is downloaded, an application identifier (AID) that identifies the applet must be registered with the appropriate monitor application, so that it can authorize the downloading of the identified applet.

**[0083]** Fig. 3 is a schematic diagram which amplifies the flow of information shown in Fig. 1 and provides further detail regarding the process of selecting and securely downloading an applet onto smartcard 2 for an embodiment of the present invention. Fig. 4 is a flow chart which provides further detail regarding the process of selecting and securely downloading an applet onto the smartcard 2 for an embodiment of the present invention. At S1, the smartcard 2 contains an applet that verifies the identity of the cardholder 24 with a PIN or a biometric, such as a fingerprint. At S2, from a selection of service options offered by the system, the cardholder 24 selects the option to download a new applet. The card 2 and the cardholder 24 must both be qualified before the system offers any applets for download. At S3, the system offers those applets supported by the business based on one or more relationships with the cardholder 24 and those applets that will fit in the space available on the card 2.

**[0084]** In an embodiment of the present invention, it is noted that space qualifications imposed on applets must account for the total space needed for each applet, including any other applets on which each applet depends. Thus, applets may be grouped into clusters. So, if one applet depends on another applet that has not yet been installed on the card 2, the card has enough space to accommodate all applets that form such a dependency cluster. At S4, the system presents a list of qualified applets to the cardholder 24, including, for example, brands that help identify the providers of the applets.

There are several kinds of disclosures to allow the cardholder 24 to make informed decisions during applet selection. Some representative examples include the total size of each applet, the space available on the card 2, and any other limitations inherent in the card infrastructure. For example, once an applet has been installed, it cannot be removed, nor can the allocated space be recovered.

**[0085]** In an embodiment of the present invention, at S5, the cardholder 24 selects an applet from the offered applet list. At S6, if a monitor application for the selected applet does not exist on the card 2, a new one is downloaded from the applet server in the electronic customization depot. At S7, if a new monitor application was added to the card, the new monitor application is initialized with any necessary key or keys, which are obtained from the security server in the electronic customization depot. At S8, the selected applet is downloaded from the applet server in the electronic customization depot 26 and installed, using the security mechanism provided by the monitor application and, for example, the gatekeeper functionality of the monitor application. At S9, the security server in the electronic customization depot 26 supplies the new applet with any key or keys necessary for its operation.

**[0086]** In an embodiment of the present invention, if the applet requires any customer information, it is obtained from the customer relationship facility 28. If the applet requires a digital certificate, it is obtained from the appropriate certificate authority 30. At S10, if the cardholder relationship supports it, the new applet is registered in the card software inventory. A copy of the card software inventory is maintained in the cardholder's electronic deposit box in the bank's electronic vault 32. In addition, the cardholder's electronic deposit box is updated with a copy of the applet's operational data, if any, but not any keys or certificates, which are reissued in the event of a lost card.

**[0087]** In an embodiment of the present invention, in order to create a secure and trusted environment, applets are isolated from each other. An applet firewall prevents one applet from accessing the contents and behavior of objects owned by other applets. However, some applets are allowed to communicate with each other in trusted ways. A smartcard, such as the Java card, provides two basic mechanisms for explicitly sharing objects between applets. One such mechanism is restricted sharing, and the other is unrestricted sharing. Restricted sharing allows an applet to grant specific other applets access to a shared object. Unrestricted sharing allows an applet to grant all other applets access to a shared object. In combination, these two basic mechanisms are used to implement selective object sharing. Some applets share selected information and services. For example, a payment applet interacts with a loyalty applet to add loyalty points as part of a payment transaction. However, the loyalty applet provider can restrict these interactions to applets from certain providers or

certain kinds of payment applets. To support this kind of selective interoperability, some of the applets have a mechanism for shared object registration.

**[0088]** In an embodiment of the present invention, applets can be downloaded and installed on the card 2 after the card has been issued. Therefore, an applet that already exists on the card 2 does not have any knowledge of a newly installed applet until the new applet registers itself with the pre-existing applet. Once the new applet identifies itself to the pre-existing applet, the pre-existing applet can grant the new applet access to its shared object or objects. Thus, the pre-existing applet or sharing applet supports registration of other applets for its shared object or objects.

**[0089]** In an embodiment of the present invention, in order to implement shared object registration, the sharing applet grants unrestricted access to a resource guardian. The resource guardian controls and grants restricted access to some guarded resource or resources, referred to as the sharing applet's shared object or objects. Some of the applets can also contain reusable foundation class libraries or groups of Java classes that are generic enough to be used by several kinds of applets. In order to retain control over the usage of some objects and thereby maintain trust, some of these libraries include shared object factories. A shared object factory creates a new instance of a library class on request for a specific client applet, and registers the new instance for access by the client applet.

**[0090]** In an embodiment of the present invention, some applets share information and services. However, giving the cardholder 24 the ability to select and dynamically download applets implies that the applets cannot be installed on the card 2 in a predetermined order. For example, a loyalty applet can be designed to support interactions with several kinds of payment mechanisms. When a new payment mechanism is installed on the card 2, it will likely want to discover whether any compatible loyalty applets are already on the card. Therefore, in order to allow dynamically loaded applets to discover during installation what other applets exist on the card 2, the card application platform includes an application registry.

**[0091]** In an embodiment of the present invention, the applications registry provides a shared object registration mechanism that supports linkage between applications based on their identification and based on their functionality or object-oriented classification. Thus, newly installed applets are able to discover whether another applet exists on the card 2 using an AID, and are also able to discover whether any other applet exists on the card that implements a specific functional interface or that was derived from a specific base class.

**[0092]** In an embodiment of the present invention, allowing applets to discover and link with each other based on their functionality gives them a much more flexible alternative to identification alone. It allows them to achieve a level of multi-functional integration beyond

the simple deployment of multiple functions on the smartcard 2. It also allows terminals to dynamically and intelligently adapt their interactions with the card 2 based on the functionality supported by the applications that actually exist on the card. In addition to facilities that support on-card interactions, card applications also have services to facilitate interactions with off-card applications, whether they reside on the card terminal 4 or on back-end systems 10.

**[0093]** In an embodiment of the present invention, security mechanisms related to dynamic application download are asymmetric in that they are applied in only one direction. A downloaded applet is decrypted and its integrity and authenticity are verified before it is installed on the card 2. However, the applets themselves have symmetric mechanisms for security. They have support, for example, for data encryption and decryption, digital signature generation and verification, and message authentication code (MAC) generation and verification. The card application platform includes a facility, such as cryptographic foundation classes, that supports packaging these diverse security mechanisms together for coherent, consistent and symmetric use, including services for key generation and key management.

**[0094]** In an embodiment of the present invention, as the cardholder 24 puts more and more kinds of information on the card 2, the value of the card to the cardholder naturally increases. Thus, the loss of the card 2 may represent a substantial loss for the cardholder 24. To reduce the significance of this loss, the system provides a mechanism for recovering the information contained on the card 2 in order to re-issue the card in the event of its loss. The financial institution provides a secure off-card information storage facility or electronic vault 32 that contains an electronic deposit box for each cardholder 24. Each electronic deposit box contains a copy of the contents of each card that the cardholder 24 registers with the bank, including a software inventory of the applets installed on the card 2, as well as a copy of the information managed by each of the installed applets.

**[0095]** In an embodiment of the present invention, applets of providers other than the financial institution can be installed on the card 2. The providers of such other applets have a legitimate interest in protecting their security keys and the data managed by their applets. In order to support applet data recovery, the applets on the card 2 and the electronic vault 32 cooperate by using a secure protocol for data exchange. In order to support applet provider secrecy, each applet uses encryption to prevent the copied data in the vault 32 from being examined. These electronic security mechanisms together mimic the physical security mechanisms used to store valuables in a safe deposit box. For example, it requires two keys to access the valuables stored in the deposit box, one of which belongs to the customer and one of which belongs to the bank. Thus, using symmetric mechanisms, each applet is able to produce a blinded

copy of its information during backup, and consume a blinded copy during restoration. The electronic vault 32 stores the blinded copy of the information for each applet.

**[0096]** In an embodiment of the present invention, the smartcard 2 is not limited to playing the role of a service provider in a client-server architecture, in which interactions between the card 2 and the terminal 4 are initiated by the terminal, with the card as a responsive device, but the system provides a more flexible architectural solution that includes the smartcard. On-card objects are allowed, for example, to initiate interactions with remote, off-card objects in the context of a distributed computing environment, which is supported by a card platform, such as Java card, with inclusion of, for example, the Java facility for remote method invocation (RMI).

**[0097]** In an embodiment of the present invention, in the context of distributed objects, mechanisms are provided by the system to support transparent object distribution. Thus, on-card objects are able to interact with off-card objects and vice-versa without explicit knowledge of their location. Such transparency simplifies the system design, allowing greater flexibility in locating objects, and Supports the deployment of migratory objects that can move from one place, such as the electronic vault 32, to another, such as the card 2. For example, an electronic ticket can be bought and stored in the electronic vault 32 until, when it is needed for use, it can be moved onto the smartcard 2 to allow off-line redemption.

**[0098]** In an embodiment of the present invention, replacement of deployed applets is supported by a card platform, such as Java card. Application identifiers (AIDs) are assigned and administered. An applet AID can be reused without change when deploying a new applet version. Alternatively, but less desirable, is a naming scheme for AIDs that includes a version identifier to guarantee uniqueness. A mechanism replaces the objects that have been created for an applet, for example, when some of the applet classes have changed their shapes. On-card mutation may be difficult or not possible given the card constraints. This consideration reinforces the value of the electronic vault 32 as a backup facility.

**[0099]** In an embodiment of the present invention, the old version of an applet may be removed entirely, including all its objects, and replaced with the new version, and the applet objects restored from backup copies that have been mutated in the electronic vault 32. A cleanroom software engineering approach for applet development applies rigorous process controls to the software development process, producing very high quality software, such as six sigma quality. The resource constraints of smartcards require that applets must be kept relatively small and simple. Thus, the rigorous process requirements of the cleanroom approach are not as burdensome as it is on large software projects.

**[0100]** Various preferred embodiments of the invention have been described in fulfillment of the various ob-

jects of the invention It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the art without departing from the spirit and scope of the present invention. Accordingly, the invention is only limited by the following claims.

### Claims

1. A method of managing addition of at least one new application to a multi-function smartcard for a cardholder, comprising:

installing a monitor application for the new application on a microcomputer of the smartcard; authorizing download of the new application by the monitor application and by a master application resident on the smartcard; and downloading the new application to the smartcard microcomputer.

2. The method of claim 1, wherein installing the monitor application further comprises downloading the monitor application from a server.
3. The method of claim 2, wherein the server further comprises an electronic customization depot.
4. The method of claim 3, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server.
5. The method of claim 1, wherein installing the monitor application further comprises downloading the monitor application at a terminal.
6. The method of claim 5, wherein the terminal further comprises a smartcard access device selected from a group consisting of an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, and a combination contact and contactless reader.
7. The method of claim 6, wherein downloading the new application further comprises downloading an application consisting of at least a portion of a plurality of functionalities for an electronic wallet from a server connected to the terminal, while allowing other portions of the functionalities for the electronic wallet to remain on at least one of the terminal and the server in a migratory fashion.

8. The method of claim 1, wherein installing the monitor application further comprises downloading the monitor application over a network.

9. The method of claim 8, wherein the network further comprises at least one of a public network and a proprietary network.

10. The method of claim 1, wherein authorizing the download further comprises initializing the monitor application.

11. The method of claim 10, wherein initializing the monitor application further comprises initializing the monitor application with a key provided by a server.

12. The method of claim 1, wherein authorizing the download further comprises registering an application identifier for the new application with the monitor application.

13. The method of claim 1, wherein downloading the new application further comprises verifying identification of the cardholder.

14. The method of claim 13, wherein verifying the identification further comprises verifying the identification by an applications on the smartcard microcomputer.

15. The method of claim 14, wherein verifying the identification further comprises verifying the identification with a PIN of the cardholder.

16. The method of claim 14, wherein verifying the identification further comprises verifying the identification with biometric data of the cardholder.

17. The method of claim 16, wherein verifying with the identification further comprises verifying the biometric data with a scanner at a terminal.

18. The method of claim 17, wherein verifying the biometric data further comprises comparing the biometric data with a reference template on the smartcard microcomputer.

19. The method of claim 18, wherein the biometric data further comprises fingerprint data for the cardholder.

20. The method of claim 1, wherein downloading the new application further comprises authenticating the smartcard.

21. The method of claim 20, wherein authenticating the smartcard further comprises authenticating the smartcard by a server.



22. The method of claim 1, wherein downloading the new application further comprises offering a selection of service options to the cardholder.
23. The method of claim 22, wherein downloading the new application further comprises selecting a service option to download a new application by the cardholder.
24. The method of claim 1, wherein downloading the new application further comprises offering a list of qualified new applications to the cardholder.
25. The method of claim 24, wherein the list of qualified new applications further comprises a plurality of new applications according to pre-defined parameters.
26. The method of claim 25, wherein the pre-defined parameters comprise at least one of a new application supported by business based on a relationship with the cardholder and a new application that fits in space available on the smartcard microcomputer.
27. The method of claim 26, wherein the pre-defined parameters further comprises the new application which, together with any other applications on which the application depends, fits as a dependency cluster in space available on the smartcard microcomputer.
28. The method of claim 24, wherein downloading the new application further comprises selecting the new application from the list of applications by the cardholder.
29. The method of claim 1, wherein downloading the new application further comprises downloading the new application from a server.
30. The method of claim 29, wherein the server further comprises an electronic customization depot.
31. The method of claim 30, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server.
32. The method of claim 1, wherein downloading the new application further comprises downloading the new application at a terminal.
33. The method of claim 32, wherein the terminal further comprises a smartcard access device selected from a group consisting of an automated teller machine, a merchant terminal, a personal computer, a personal digital assistant, a TV set-top box, a land phone, a cell phone, a digital phone, a cable TV box, a satellite TV box, a contact reader, a contactless reader, and a combination contact and contactless reader.
34. The method of claim 1, wherein downloading the new application further comprises downloading the new application over a network.
35. The method of claim 34, wherein the network further comprises at least one of a public network and a proprietary network.
36. The method of claim 1, wherein downloading the new application further comprises installing the new application on the smartcard microcomputer.
37. The method of claim 36, wherein installing the new application further comprises installing the new application using a security mechanism of the monitor application.
38. The method of claim 36, wherein installing the new application further comprises supplying the new application with an operation key.
39. The method of claim 36, wherein installing the new application further comprises supplying the new application with cardholder information.
40. The method of claim 36, wherein installing the new application further comprises supplying the new application with digital certificate.
41. The method of claim 36, wherein installing the new application further comprises registering the new application in a software registry of the smartcard.
42. The method of claim 41, wherein registering the new application further comprises registering the new application according to an object-oriented classification of the software registry.
43. The method of claim 41, wherein registering the new application further comprises furnishing a copy of the smartcard software registry to an electronic deposit box.
44. The method of claim 43, wherein furnishing a copy further comprises updating the electronic deposit box with a copy of operational data for the new application.
45. The method of claim 36, wherein installing the new application further comprises selectively sharing at least one object of the new application with at least one object of another application on the smartcard.
46. The method of claim 45, wherein selectively sharing

further comprises at least one of restricted sharing of the object by the new application and unrestricted sharing by the new application.

47. A system for securely adding at least one new application to a multi-function smartcard for a cardholder, comprising: 5
- means for installing a monitor application for the new application on a microcomputer of the smartcard; 10
  - means for associated with the installing means for authorizing download of the new application by the monitor application and by a master application resident on the smartcard; and 15
  - means associated with the authorizing means for downloading the new application to the smartcard microcomputer.
48. The system of claim 47, wherein the installing means further comprises means for downloading the monitor application from a server. 20
49. The system of claim 48, wherein the server further comprises an electronic customization depot. 25
50. The system of claim 49, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server. 30
51. The system of claim 48, the means for downloading the monitor application further comprises a terminal communicating with the server over a network. 35
52. The system of claim 47, wherein the means for downloading the new application further comprises a server. 40
53. The system of claim 52, wherein the server further comprises a an electronic customization depot. 45
54. The system of claim 53, wherein the electronic customization depot further comprises functionalities of at least one of an applet server and a monitor application server. 50
55. The system of claim 52, wherein the means for downloading the new application further comprises a terminal communicating with the server over a network 50

55

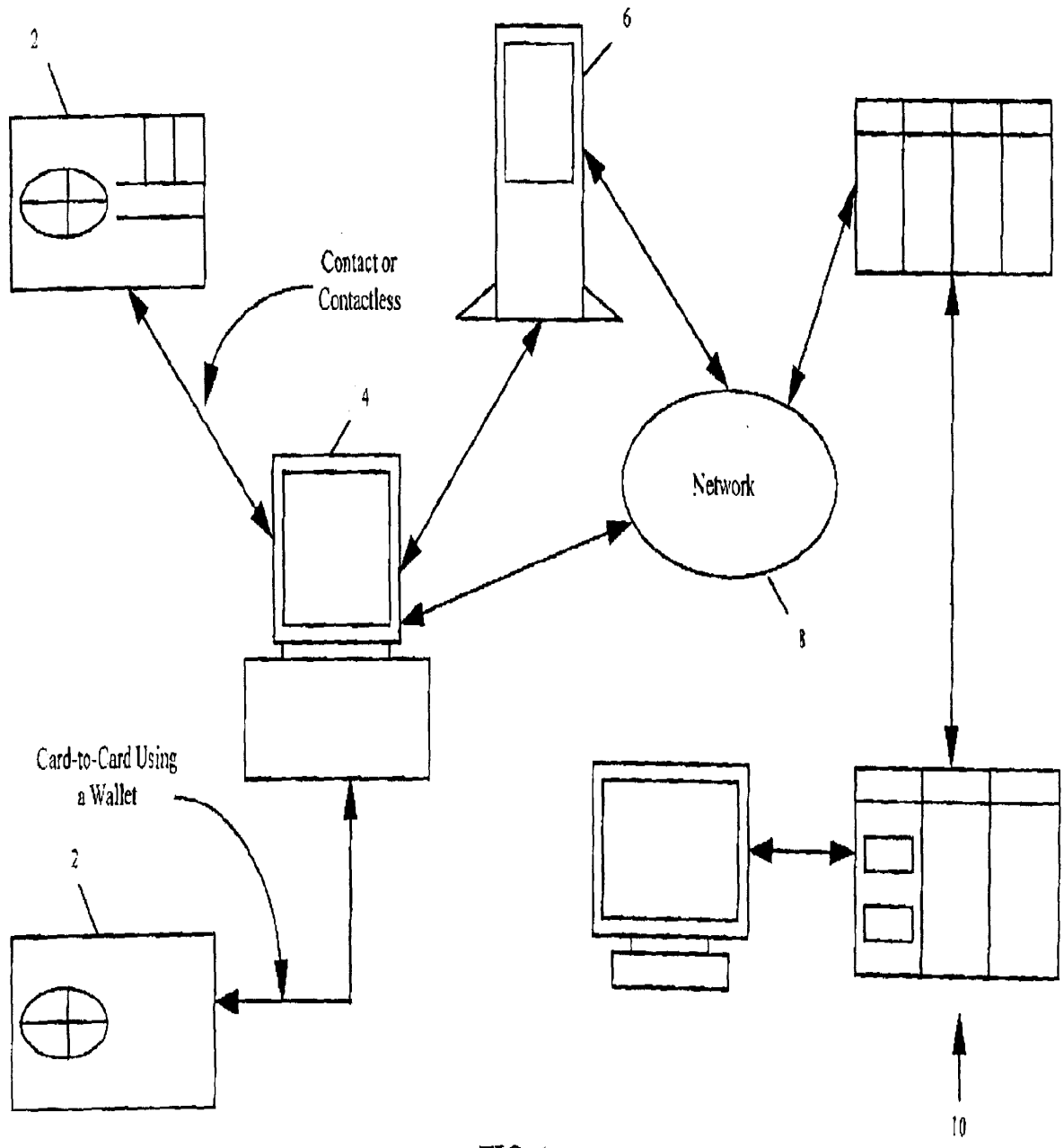


FIG. 1

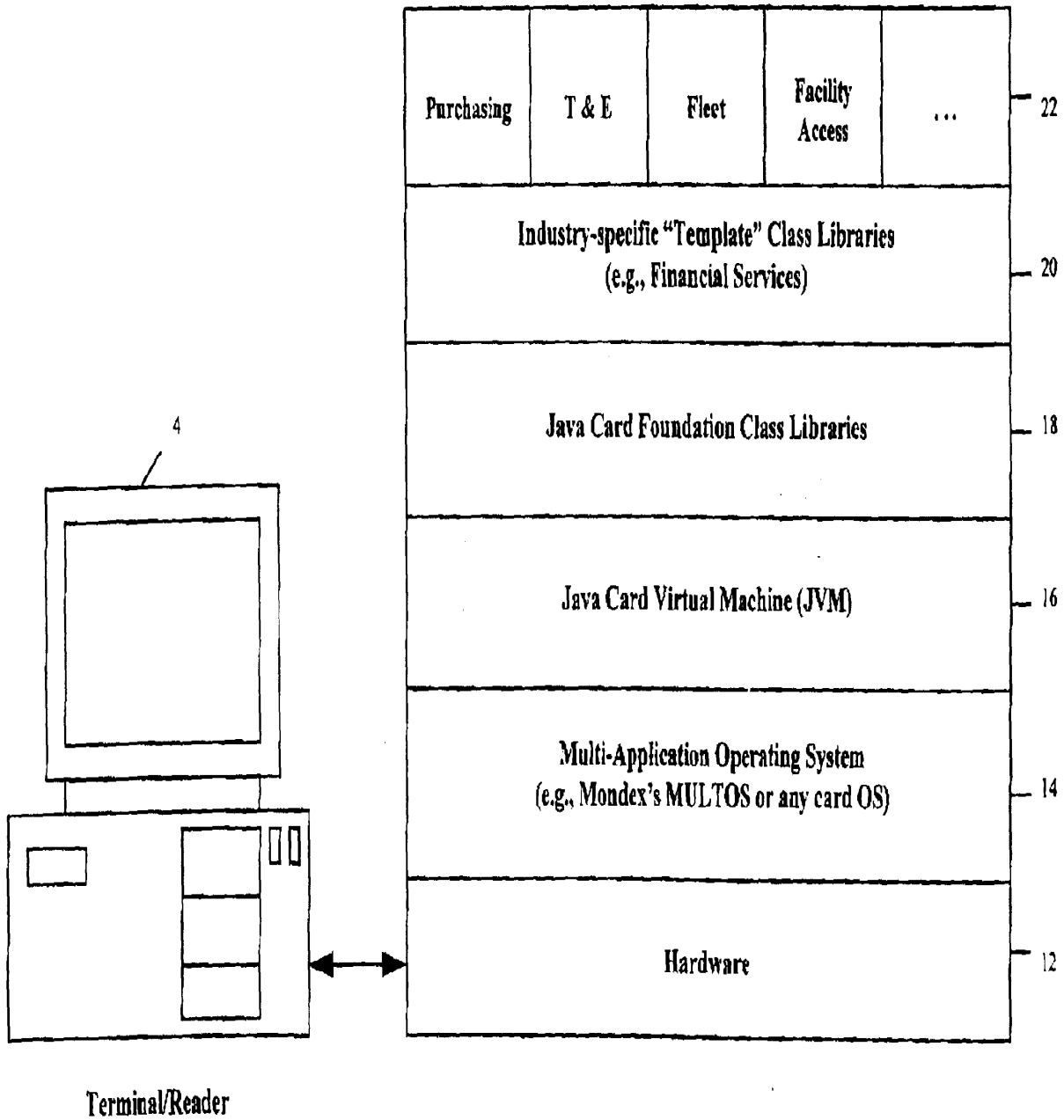


FIG. 2

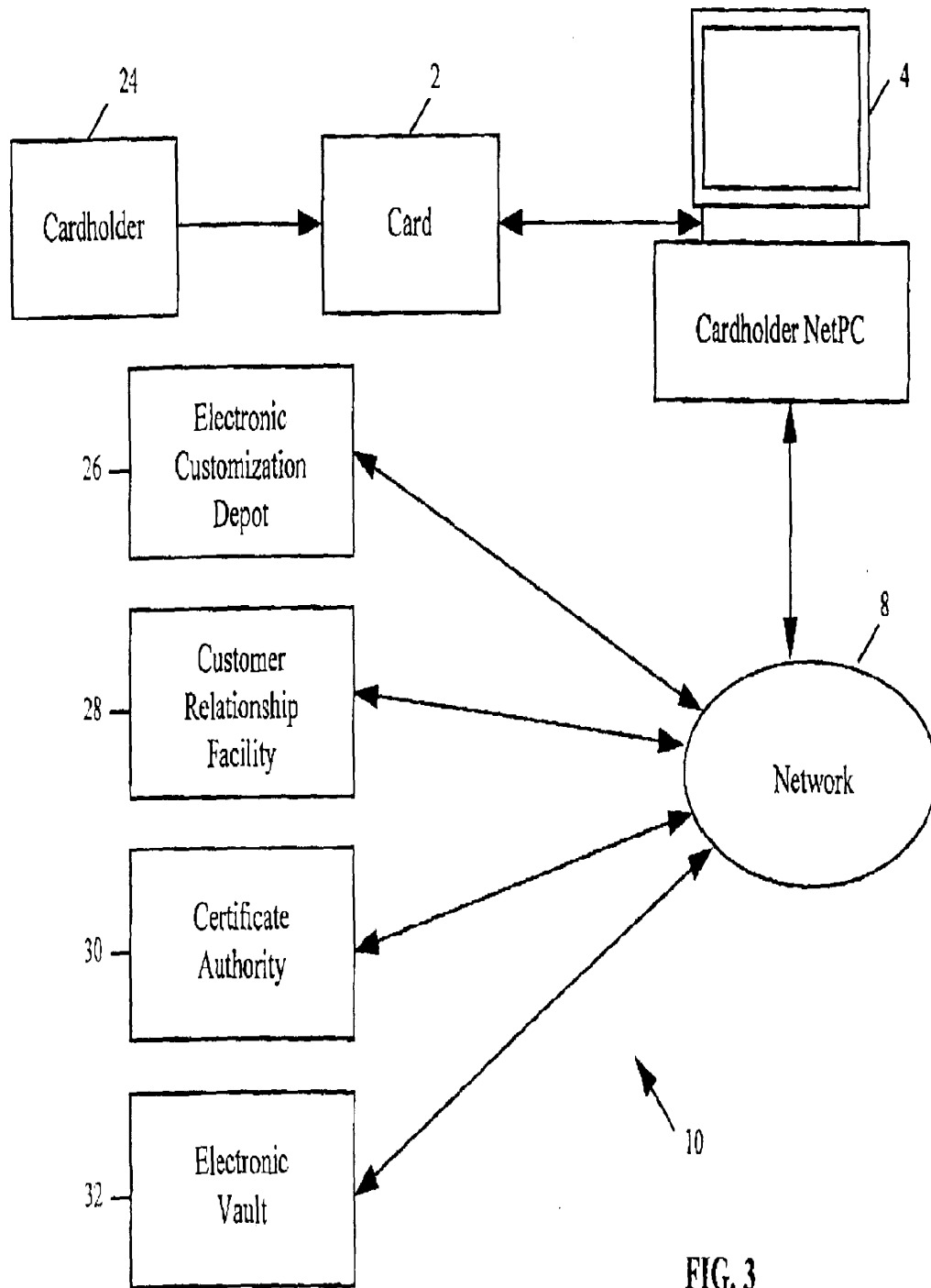


FIG. 3

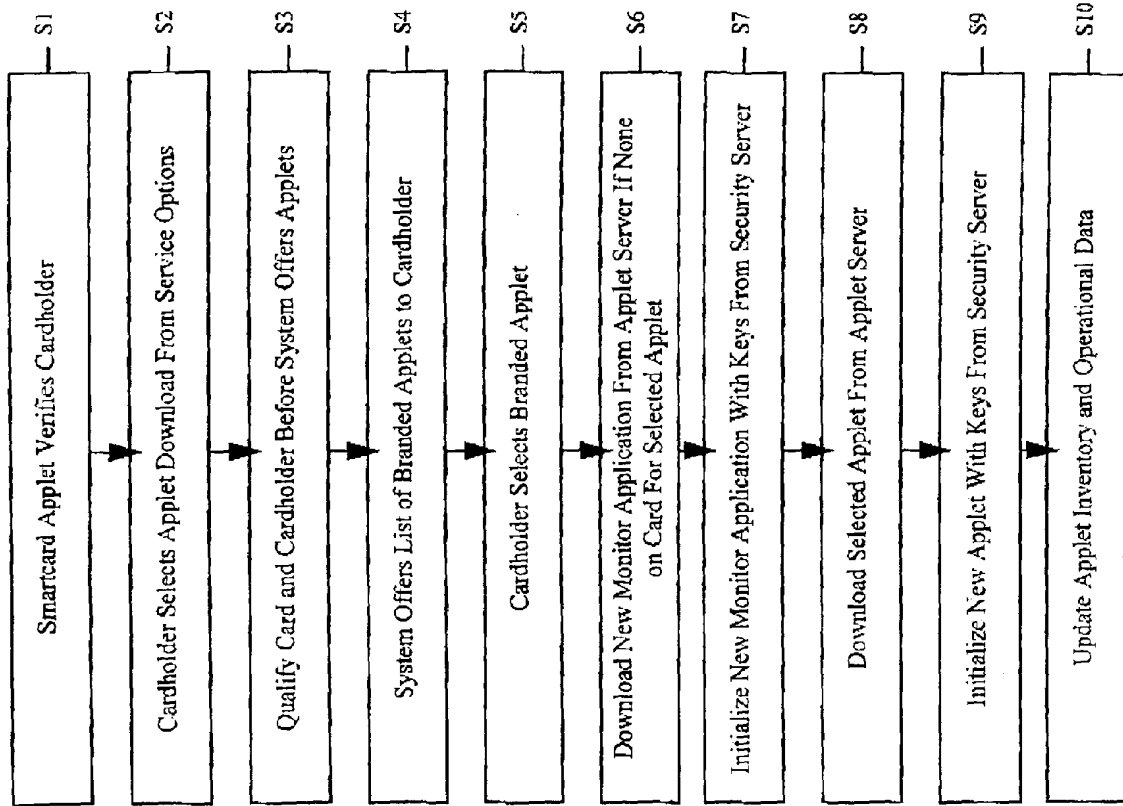
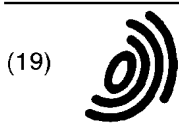


FIG. 4

STATEMENT OF RELEVANCY - EP 1003135

EP 1003135 relates to electronic payment terminals.



(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:  
 24.05.2000 Bulletin 2000/21

(51) Int Cl.7: G07F 7/10

(21) Numéro de dépôt: 99402893.4

(22) Date de dépôt: 22.11.1999

(84) Etats contractants désignés:  
 AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
 MC NL PT SE  
 Etats d'extension désignés:  
 AL LT LV MK RO SI

(71) Demandeur: SAGEM SA  
 75116 Paris (FR)

(72) Inventeur: Sarradin, Jean-Louis  
 95190 Fontenay en Parisis (FR)

(30) Priorité: 20.11.1998 FR 9814625

(74) Mandataire: Bloch, Gérard  
 2, square de l'Avenue du Bois  
 75116 Paris (FR)

(54) Terminal de traitement d'informations et de paiement électronique

(57) Le terminal de traitement d'informations comporte des circuits (11, 16) de liaison avec un centre de

téléchargement de données d'initialisation et un bloc de mémorisation des données, qui comporte un lecteur (20) d'exploitation de mémoires amovibles (21).

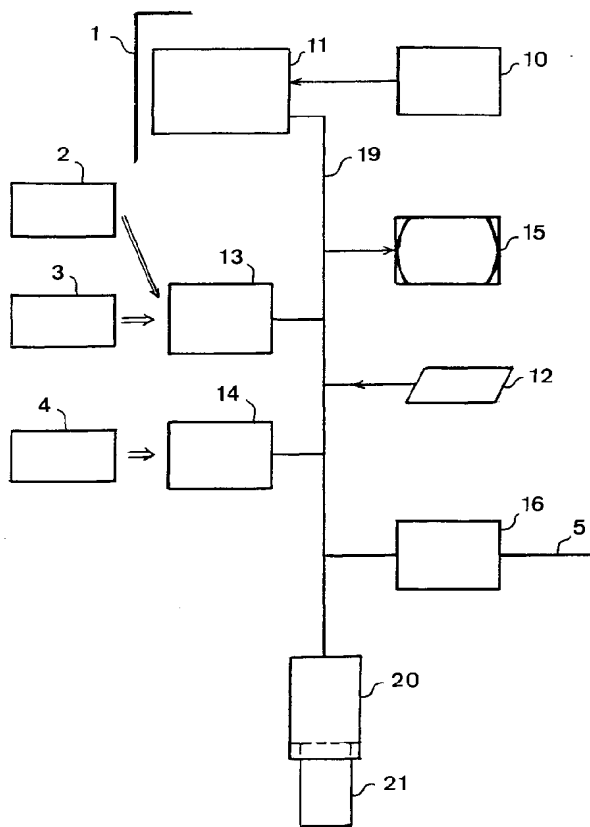


FIGURE UNIQUE



## Description

**[0001]** Un terminal de paiement électronique, installé chez un commerçant, permet au porteur d'une carte bancaire d'effectuer des achats par transfert électronique d'argent de son compte bancaire à celui du commerçant.

**[0002]** Des sécurités sont prévues pour éviter toute erreur ou fraude lors de telles opérations. Ainsi, le terminal n'accepte que les cartes bancaires validées par un code confidentiel que le porteur de la carte doit saisir par un clavier du terminal. De même, le commerçant est identifié par une carte spéciale.

**[0003]** Le terminal mémorise temporairement les transactions, c'est-à-dire les parties d'opération se déroulant jusqu'à l'édition des tickets, pour les transmettre périodiquement, par le réseau téléphonique, à un centre de télécollecte et de traitement qui en assure la mémorisation définitive et l'exécution.

**[0004]** Le terminal a aussi en mémoire un numéro d'appel d'un centre d'autorisation pour pouvoir éventuellement effectuer des transactions dépassant un plafond.

**[0005]** Depuis le centre de télécollecte, le terminal est initialement configuré par téléchargement de données d'initialisation relatives au commerçant, comme son identité bancaire, et aussi relatives aux échanges avec les centres ci-dessus, tels que numéros de téléphone, nombre maximal de tentatives d'appel, liste noire des cartes bancaires interdites et autres.

**[0006]** Cependant, en cas d'échange standard du terminal, suite à une panne, ou en cas de traitement de cartes bancaires autres que celles prévues, il faut rappeler le centre de télécollecte pour réinitialiser le terminal.

**[0007]** La présente invention vise à s'affranchir de la contrainte qu'imposent de telles réinitialisations.

**[0008]** Le problème des réinitialisations ne se posant pas qu'avec les terminaux de paiement électronique, la demanderesse entend d'ailleurs élargir la portée de sa demande à tout terminal de traitement d'informations.

**[0009]** A cet effet, l'invention concerne un terminal de traitement d'informations comportant des moyens de liaison avec un centre de téléchargement de données d'initialisation et des moyens de mémorisation des données, terminal caractérisé par le fait que les moyens de mémorisation de données comportent des moyens d'exploitation de moyens mémoires amovibles.

**[0010]** Naturellement, l'invention s'applique parfaitement à des terminaux de paiement électronique.

**[0011]** Ainsi, les données d'initialisation fournies par le centre de téléchargement, qui particularisent le terminal, peuvent être initialement mémorisées en mémoire amovible et être ensuite localement fournies au terminal, en y implantant la mémoire amovible voulue, éventuellement transplantée depuis un autre terminal.

**[0012]** Le terminal est donc construit en associant une partie banalisée, formée du matériel et de logiciels stan-

dards résidents éventuels, et une partie spécifique amovible à mémoire, qui peut être associée avec toute partie banalisée de tels terminaux.

**[0013]** Avantagusement, les moyens d'exploitation comportent un lecteur de carte à puce qui, de préférence, est agencé pour recevoir une carte SIM (module d'identification d'abonné). La carte SIM constitue ainsi une mémoire facilement transportable.

**[0014]** L'invention sera mieux comprise à l'aide de la description suivante d'une forme de réalisation préférée du terminal de traitement d'informations de l'invention, en référence à la figure unique en annexe.

**[0015]** Le terminal de traitement d'informations, référencé 1 sur la figure, est ici un terminal de paiement électronique agencé pour recevoir, de façon classique, une carte bancaire 2 à puce et/ou piste d'un client, ou carte porteur, une carte spéciale commerçant 3 et une carte sécuritaire commerçant 4. Il est relié, de façon fixe ou amovible, à une ligne 5 du réseau téléphonique commuté pour dialoguer avec un centre de télécollecte et téléchargement, non représenté.

**[0016]** Le terminal 1 comporte une base de temps 10 rythmant le fonctionnement d'un microprocesseur 11 avec mémoire qui règle le fonctionnement des divers circuits du terminal 1, reliés au microprocesseur 11 par un bus 19.

**[0017]** Un lecteur de carte 13 permet d'exploiter les cartes 2 et 3 et d'inscrire le montant des transactions et un lecteur 14 est réservé à la carte 4, selon les flèches de la figure. Un clavier 12, relié au microprocesseur 11 par le bus 19, permet de saisir les commandes voulues pour effectuer les séquences d'opérations pour une transaction, et en particulier un code confidentiel client associé à la carte 2. Le microprocesseur 11 commande un écran 15 visualisant les diverses étapes et guidant les opérateurs, client et commerçant. Un modem 16 relie le microprocesseur 11 à la ligne 5.

**[0018]** Le microprocesseur 11 est aussi relié à un circuit d'interface 20 agencé pour exploiter une mémoire amovible 21 qu'il reçoit, c'est-à-dire la lire et éventuellement y écrire des données. Dans cet exemple le circuit d'interface 20 est un lecteur de carte à puce exploitant une carte 21 de type SIM ou micro SIM.

**[0019]** Pour initialiser le terminal 1, le commerçant commande, par le clavier 12 et le microprocesseur 11, un appel du centre de télécollecte et téléchargement par la ligne 5. Ce dernier fournit en réponse des données d'initialisation du terminal 1, permettant son exploitation, telles que numéro d'un centre d'autorisation de transactions, fréquence des appels de télécollecte, heure d'appel, liste noire des cartes 2 et autres. Pour plus de précisions, on se reportera au "Manuel du paiement électronique" et au "Protocole de Transmission avec les Centres de Traitement et d'Autorisation" édités par le Groupement des Canes Bancaires "CB", incorporés ici par référence.

**[0020]** Les données d'initialisation reçues par le terminal 1 sont mémorisées dans une mémoire, associée

à un microprocesseur, de la carte SIM 21. En variante, il aurait pu être prévu un connecteur ou support de circuit intégré (tel que douilles de réception et de connexion des broches du circuit intégré) recevant un bloc mémoire pouvant être écrit dans le terminal 1 et conservant les données même après mise hors tension, donc à fonction de mémoire morte inscriptible en fonctionnement. C'est par exemple une mémoire du genre Flash, capable, sous tension, de modifier le potentiel d'entrées de "caissons" de stockage de charges électriques, définissant chacune l'état d'un bit, pour remplir ou vider ces caissons en écriture. En l'absence d'alimentation, les caissons restent fermés et peuvent donc être lus, sans perte de données, lorsqu'ils sont à nouveau alimentés, dans le terminal 1 ou dans un autre, semblable, qui le remplace. Une mémoire vive amovible à alimentation sauvegardée est de même envisageable. On peut par exemple penser à une mémoire CMOS associée à une pile.

5

10

15

20

### Revendications

1. Terminal de traitement d'informations comportant des moyens (11, 16) de liaison avec un centre de téléchargement de données d'initialisation et des moyens de mémorisation des données, terminal caractérisé par le fait que les moyens de mémorisation de données comportent des moyens (20) d'exploitation de moyens mémoires amovibles (21).
2. Terminal selon la revendication 1, dans lequel les moyens d'exploitation comportent un lecteur (20) de carte à puce (21).
3. Terminal selon la revendication 2, dans lequel le lecteur (20) est agencé pour recevoir une carte SIM (21).
4. Terminal selon l'une des revendications 1 à 3, qui est un terminal de paiement électronique.

25

30

35

40

45

50

55

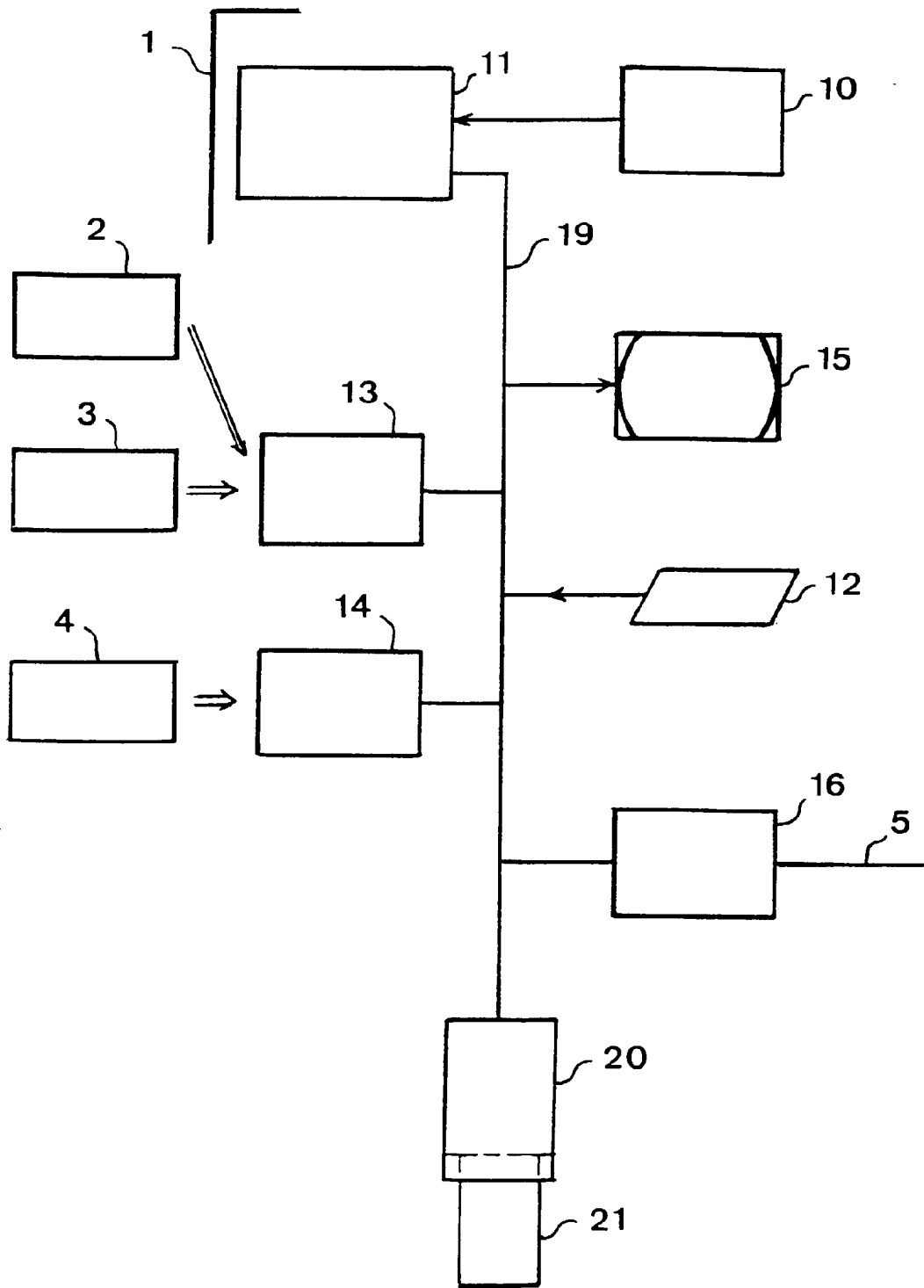


FIGURE UNIQUE



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication: **31.05.2000 Bulletin 2000/22** (51) Int Cl.7: **G07F 7/10, G06K 19/073**

(21) Application number: **00200559.3**

(22) Date of filing: **24.03.1998**

(84) Designated Contracting States:  
**AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE**  
 Designated Extension States:  
**AL LT LV MK RO SI**

- **Weise, Joel M.**  
**Burlingame, CA 94010 (US)**
- **Kekicheff, Marc B.**  
**Palo Alto, CA 94303 (US)**
- **Wentker, David C.**  
**San Francisco, CA 94117 (US)**

(30) Priority: **24.03.1997 US 41468**  
**14.10.1997 US 61763**

(74) Representative: **Finnie, Peter John**  
**Elkington and Fife,**  
**Prospect House,**  
**8 Pembroke Road**  
**Sevenoaks, Kent TN13 1XR (GB)**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:  
**98911952.4**

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION**  
**Foster City, CA 94404 (US)**

Remarks:  
 This application was filed on 18 - 02 - 2000 as a divisional application to the application mentioned under INID code 62.

(72) Inventors:  
 • **Chan, Alfred**  
**Daly City, CA 94015 (US)**

(54) **A system and method for a multi-application smart card which can facilitate a post-issuance download of an application onto the smart card**

(57) A smart card includes a card domain application that manages the card. Any number of security domain applications on the card provide security for loaded applications by managing keys; each application is associated with a security domain. Each of the card domain and security domains has a command interface for off-card communication, and an API for internal card use. The card life cycle includes the states of masked, initialized, load secured and blocked. An application life cycle includes the states of not available, loaded, installed, registered, personalized, activated and blocked. An application can block the card.

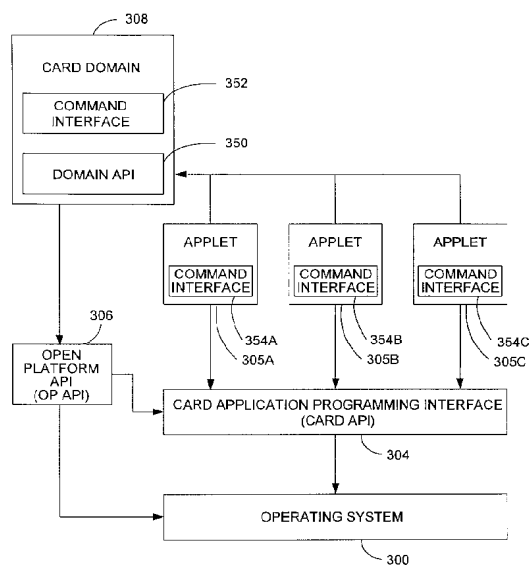


FIG. 3A

## Description

### Field of the Invention

[0001] The present invention relates to smart cards. In particular, the present invention relates to a system and method for providing a multi-application smart card which can facilitate a post-issuance download of an application onto the smart card.

### Background to the Invention

[0002] A smart card is typically a credit card-sized plastic card that includes a semiconductor chip capable of holding data supporting multiple applications.

[0003] Physically, a smart card often resembles a traditional "credit" card having one or more semiconductor devices attached to a module embedded in the card, providing contacts to the outside world. The card can interface with a point-of-sale terminal, an ATM, or a card reader integrated into a telephone, a computer, a vending machine, or any other appliance.

[0004] A micro-controller semiconductor device embedded in a "processor" smart card allows the card to undertake a range of computational operations, protected storage, encryption and decision making. Such a micro-controller typically includes a microprocessor, memory, and other functional hardware elements. Various types of cards are described in "The Advanced Card Report: Smart Card Primer", Kenneth R. Ayer and Joseph F. Schuler, The Schuler Consultancy, 1993.

[0005] One example of a smart card implemented as a processor card is illustrated in FIG. 1. Of course, a smart card may be implemented in many ways, and need not necessarily include a microprocessor or other features. The smart card may be programmed with various types of functionality, including applications such as stored-value; credit/debit; loyalty programs, etc.

[0006] In some embodiments, smart card 5 has an embedded micro-controller 10 that includes a microprocessor 12, random access memory (RAM) 14, read-only memory (ROM) 16, non-volatile memory 18, a cryptographic module 22, and a card reader interface 24. Other features of the micro-controller may be present but are not shown, such as a clock, a random number generator, interrupt control, control logic, a charge pump, power connections, and interface contacts that allow the card to communicate with the outside world.

[0007] Microprocessor 12 is any suitable central processing unit for executing commands and controlling the device. RAM 14 serves as storage for calculated results and as stack memory. ROM 16 stores the operating system, fixed data, standard routines, and look up tables. Non-volatile memory 18 (such as EPROM or EEPROM) serves to store information that must not be lost when the card is disconnected from a power source but that must also be alterable to accommodate data specific to individual cards or any changes possible over the

card lifetime. This information might include a card identification number, a personal identification number, authorization levels, cash balances, credit limits, etc. Cryptographic module 22 is an optional hardware module used for performing a variety of cryptographic algorithms. Card reader interface 24 includes the software and hardware necessary for communication with the outside world. A wide variety of interfaces are possible. By way of example, interface 24 may provide a contact interface, a close-coupled interface, a remote-coupled interface, or a variety of other interfaces. With a contact interface, signals from the micro-controller are routed to a number of metal contacts on the outside of the card which come in physical contact with similar contacts of a card reader device.

[0008] Various mechanical and electrical characteristics of smart card 5 and aspects of its interaction with a card reading device are defined by the following specifications, all of which are herein incorporated by reference.

[0009] Visa Integrated Circuit Card Specification, (Visa International Service Association 1996).

[0010] EMV Integrated Circuit Card Specification for Payment Systems, (Visa International Service Association 1996).

[0011] EMV Integrated Circuit Card Terminal Specification for Payment Systems, (Visa International Service Association 1996).

[0012] EMV Integrated Circuit Card Application Specification for Payment Systems, (Visa International Service Association 1996).

[0013] International Standard: Identification Cards - Integrated Circuit(s) Cards with Contacts, Parts 1-6 (International Standards Organization 1987-1995).

[0014] Prior to issuance of a smart card to a card user, the smart card is initialized such that some data is placed in the card. Initialization refers to the population of non-volatile memory with data that is common to a large number of cards while also including a minimal amount of card unique terms (e.g. card serial number and personalization keys). For example, during initialization, the smart card may be loaded with at least one application, such as credit or stored cash value, a file structure initialized with default values, and some initial cryptographic keys for transport security. Once a card is initialized, it is typically personalized. During personalization, the smart card is loaded with data which uniquely identifies the card. For example, the personalization data can include a maximum value of the card, a personal identification number (PIN), the currency in which the card is valid, the expiration date of the card, and cryptographic keys for the card.

[0015] A limitation of conventional smart cards is that new applications typically can not be added to an issued smart card. Smart cards are traditionally issued with one or more applications predefined and installed during the manufacturing process of the card. As a result, with traditional smart card implementation, once a card has

been issued to a card user, the smart card becomes a fixed application card. If a new application is desired, the smart card is typically discarded and a new smart card, which includes the new application, is issued.

[0016] It would be desirable to provide a smart card which would allow applications to be loaded after the card is issued. Further, it is desirable to provide a mechanism to manage the loading of an application as well as general management of the applications on the smart card. Additionally, it is desirable to allow an application provider to keep cryptographic keys confidential from the issuer of the smart card and to securely allow applications from different entities to coexist on a card.

### Summary of the Invention

[0017] The present invention provides a system and method which allow card issuers to add applications during the lifetime of the card after the card has already been issued (referred to herein as post issuance loading). Downloading an application after the card has been issued to the card holder will be referred to herein as a "secure install" process.

[0018] The system and method of the present invention allow the post issuance loading of an application and/or objects from an application server via a card acceptance device and its supporting system infrastructure delivery mechanism onto a card in a secure and confidential manner.

[0019] The present invention also provides a system and method for controlling at least one function associated with an issued smart card. In a multi-application smart card, a privileged application, herein referred to as a card domain, manages multiple functions related to the smart card. Examples of these functions include card initialization, global card data, card life cycle, and secure installation of smart card applications.

### Brief Description of the Drawings

[0020] Examples of the present invention will now be described in detail with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of a smart card system suitable for implementing the present invention;

Figure 2 is an example of a block diagram of software layers which can be utilized in a smart card;

Figures 3A - 3B are block diagrams of examples of software layers according to embodiments of the present invention;

Figure 4 is a flow diagram of an example of a method according to an embodiment of the present invention for installing an application onto an issued smart card utilizing a card domain;

Figure 5 is a flow diagram of a method according to an embodiment of the present invention for providing confidential information to an application in a

smart card using security domains;

Figure 6 is a flow diagram of an example of a method according to an embodiment of the present invention for installing an application onto an issued smart card utilizing a card domain;

Figure 7A is a flow diagram illustrating a sequence of card life states;

Figure 7B is a flow diagram illustrating a sequence of card life states;

Figure 8 is an illustration of an example of a card life cycle;

Figure 9 is a flow diagram of an example of a method according to an embodiment of the present invention for blocking a card utilizing a card domain;

Figure 10 is a block diagram illustrating interactions between a card domain and a security domain on a smart card according to an embodiment of the present invention;

Figures 11A and 11B are flow diagrams of an example of a method according to an embodiment of the present invention for loading an application by using a security domain after the smart card has issued;

Figures 12A-12B are flow diagrams of an example of a method according to an alternate embodiment of the present invention for loading an application using a security domain after the smart card has issued; and,

Figure 13 is a block diagram illustrating an example of key management and key dependencies for post issuance download of applications onto the smart card.

### Detailed Description

[0021] Figure 2 is a block diagram of an example of software layers which can be utilized in a smart card. The smart card shown in Figure 2 includes an operating system 200, a card application programming interface (API) 204, and applications 206A-206B. Operating system 200 can include functionality to control the cards, memory management, input/output (I/O), and cryptographic features. Card API 204 utilizes the instructions from operating system 200 and writes these instructions into blocks which can be reused for common routines in multiple applications. Applications 206A and 206B can run on the smart card via instructions from API 204. These applications can include any application which can run on a smart card, such as stored value, credit, debit, transit, and loyalty.

[0022] One embodiment of the present invention is based upon the Java Card standard. In this case applications are referred to as 'Applets' and they are written to link to a Java Card API which is the application programming interface present on smart cards built to the Java Card standard.

[0023] Although the conventional software system shown in Figure 2 allows for multiple applications, it does not solve the problem of how to securely load an

application after issuance of the smart card to a user. If an application is to be loaded post issuance, a mechanism is needed to manage the loading of an application as well as the general management of the applications on the smart card. Additionally, an application provider may wish to keep cryptographic keys confidential from the issuer of the smart card. Accordingly, a mechanism is needed to provide for the separation of confidential information between an application provider and an issuer of a smart card. Embodiments of the present invention address such a need.

**[0024]** Figures 3A - 3B are block diagrams showing software components of a smart card according to embodiments of the present invention. The arrows indicate dependencies between components. Figure 3A shows an embodiment of a smart card utilizing a card domain, while Figure 3B shows an embodiment of a smart card utilizing a security domain, as well as a card domain.

**[0025]** The example shown in Figure 3A includes an operating system 300, a card API 304, applications 305A-305C, a card domain 308, and open platform (OP) API 306. The system shown in Figure 3 allows for a secure and managed post issuance download of an application onto a smart card. A card domain is a card issuer's on-card control mechanism for a smart card according to the present invention.

**[0026]** Open platform API 306 classifies instructions into card domain 308 and security domains 310A-310B (shown in Figure 3B). Accordingly, OP API 306 facilitates the formation of instructions into sets which can be identified as being included as part of card domain 308 and security domains 310A-310B.

**[0027]** Applications 305A-305C can include any application which can be supported by a smart card. Examples of these applications include credit, debit, stored value, transit, and loyalty. Applications 305A-305C are shown to include command interfaces, such as APDU interfaces 354A-354C which facilitate communication with the external environment.

**[0028]** Applications 305A-305C can run on the smart card via instructions from card API 304. Card API 304 is implemented using the instructions from the card operating system and writes these instructions into blocks which can be reused for common routines for multiple applications. Those skilled in the art will recognize that a translation layer or interpreter may reside between API 304 and operating system 300. An interpreter interprets the diverse hardware chip instructions from vendor specific operating system 300 into a form which can be readily utilized by card API 304.

**[0029]** Card domain 308 can be a "privileged" application which represents the interests of the smart card issuer. As a "privileged" application, card domain 308 may be configured to perform multiple functions to manage various aspects of the smart card. For instance, card domain 308 can perform functions such as installing an application on the smart card, installing security domains 310A-310B (shown on Figure 3B), personali-

zation and reading of card global data, managing card life cycle states (including card blocking), performing auditing of a blocked card, maintaining a mapping of card applications 305A-305C to security domains 310A-310B, and performing security domain functions for applications 305A-305C which are not associated with a security domain 310.

**[0030]** Card domain 308 is shown to include an API 350 and a command interface, such as Application Protocol Data Unit (APDU) interface 352. APDU interface 352 facilitates interfacing with the external environment in compliance with, e.g., International Standards Organization (ISO) Standard 7816-4, entitled "Identification Cards - Integrated circuit(s) cards with contacts - Part 4, Inter-industry commands for interchange," which is herein incorporated by reference.

**[0031]** For example, APDU interface 352 can be used during post issuance installation of an application or during loading of card global data. An application load and install option is performed via a set of appropriate APDU commands received by card domain 308. API 350 facilitates interfacing with the internal smart card environment. For example, API 350 can be used if card domain 308 is being utilized as a default in place of a security domain 310, or if an application requires information such as card global data, key derivation data, or information regarding card life cycle.

**[0032]** Memory allocations have been performed by the time an application is in an install state. An application is also personalized after loading and installing. A personalized application includes card holder specific data and other required data which allows the application to run. In addition to managing the installation and personalization of the application, card domain 308 can also manage global card information. Global card information includes information that several applications may need to perform their functions, such as card holder name and card unique data utilized in cryptographic key derivations. Card domain 308 can be a repository for the global card information to avoid storing the same data multiple times.

**[0033]** Card domain 308 can also manage card life cycle states including card blocking. The smart card will typically move through several states during its life cycle. Card domain 308 keeps track of what state the card is in during its life cycle. Card domain 308 may also manage a block request to block virtually all functions of the card. Further details of card domain 308 management of a block request will be discussed in conjunction with Figure 6. Card domain 308 may also keep track of the state of an application during an application's life cycle. This kind of information regarding an application can be utilized during an auditing of a card. Auditing can be performed at any time during a card's lifetime. For instance, auditing may be performed after a card has been blocked or prior to installing a new application to validate the card contents. Although virtually all card functions are no longer functioning when a card is blocked, an is-

suer may be able to query card domain 308 for information regarding a state of an application or the life cycle state of the card. In this manner, the issuer of a card may still access a profile of the blocked card and its applications.

**[0034]** Figure 3B shows an embodiment of the present invention utilizing a security domain 310, as well as card domain 308'. The example shown in Figure 3B includes an operating system 300', a card API 304', applications 305A'-305C', security domains 310A-310B, a card domain 308', and open platform (OP) API 306'. The system shown in Figure 3B also allows for a secure and managed post issuance download of an application onto a smart card.

**[0035]** Card domain 308' can work in conjunction with a security domain 310. Security domain 310 is a logical construct that can be implemented as an application to provide security related functions to card domain 308' and to applications associated with security domain 310. Security domains 310A-310B can assist in secure post issuance loading of an application onto the smart card. Security domains 310A-310B provide for a mechanism which keeps the application provider's confidential information, such as cryptographic keys, from being disclosed to the issuer of the smart card.

**[0036]** There may be multiple security domains 310 on a smart card, each represented by a unique cryptographic relationship. A security domain 310 is responsible for the management and sharing of cryptographic keys and the associated cryptographic methods which make up the security domain's cryptographic relationship. An application which is loaded to the smart card post issuance can be associated with a security domain, preferably with only one security domain. However, multiple applications may be associated with the same security domain 310. Applications installed on a smart card during the pre-issuance phase may optionally be associated with a security domain 310 on the smart card for purposes of loading confidential personalization data to those applications using security domain 310 keys.

**[0037]** The software for security domain 310 may be installed by the card manufacturer at the time of card manufacturing (e.g., when the ROM is masked), or may be added during initialization or personalization stages. Security domains 310 can be implemented as selectable applications which are isolated from one another and the rest of the system. If security domain 310 is implemented in a Java card as an application, standard Java card security can be relied upon to ensure isolation of security domain 310. In addition, or alternatively, other security mechanisms such as hardware security can be utilized through OP API 306 implementation. OP API 306 may utilize special security features to enforce isolation of security domain 310. An example of such a security feature is the utilization of chip hardware security routines which may be employed by OP API 306.

**[0038]** Each security domain 310A-310B provides a command interface, such as an Application Protocol Da-

ta Unit (APDU) interface 320A-320B, for communication off card, and on card APIs 322A-322B.

**[0039]** The APDU interface 320A or 320B consists of personalization commands and is intended to allow the initial loading of security domain keys and to support key rotation if desired during the life of the security domain. APIs 322A-322B may include a signature verification method and decryption method which are shared with card domain 308' for post issuance loading of applications. Additionally, applications may utilize API interfaces 322A-322B for decrypting application confidential data. Note that card domain 308' may always function as a security domain and does so as the default.

**[0040]** Security domain 310 manages signing and decrypting keys and provides cryptographic services using those keys. Security domain 310 processes APDU's for numerous functions. These functions can include key management functions, e.g., functions to load or update keys. During a secure installation of an application, security domain 310 can provide services to card domain 308' to decrypt an application install file and check the signature of an application file. For an application associated with a security domain 310, that application's security domain 310 provides decrypt and signature functions, such as MACing on an update key APDU command during the personalization phase of a newly installed application. Thereafter, the application can use the updated key to decrypt and check signatures on subsequent key updates.

**[0041]** The smart card issuer may decide whether security domain 310 utilizes a static key or a session key for transactions. A static key is a cryptographic key which exists prior to processing APDUs and which exists during and after the processing of APDUs. A session key is a cryptographic key which can be generated for a particular transaction and is typically no longer used for APDU processing after the transaction. If a session key is utilized, security domain 310 preferably derives its own session key for processing APDUs.

**[0042]** Figure 4 is a flow diagram of a method according to an embodiment of the present invention for providing an application to a smart card. The example illustrated in Figure 4 also applies to installing a security domain 310 onto a smart card. Note that all of the flow diagrams in this application are merely examples. Accordingly, the illustrated steps of this and any other flow diagram, can occur in various orders and in varying manners in order to accomplish virtually the same goal.

**[0043]** A smart card is issued (step 400), and an application is forwarded to the issued smart card (step 402). The forwarding of the application can occur through any electronic media which can interface with a smart card and connect to an appropriate network. For example, devices such as an automatic teller machine (ATM), a display phone, or a home computer, can be used to forward an application to the issued smart card. The forwarded application is then loaded onto the smart card, and the loading of the application is managed by



card domain 308 (step 404).

**[0044]** Figure 5 is another flow diagram of a method according to an embodiment of the present invention for providing an application onto an issued smart card. A smart card is created and provided with a first application, the first application including a cryptographic service (step 1002). A second application is loaded onto the smart card (step 1004). Thereafter, the second application is installed, and the cryptographic service of the first application is utilized to install the second application (step 1006).

**[0045]** Figure 6 is another flow diagram of an example of a method according to an embodiment of the present invention for providing an application onto an issued smart card. This method for providing an application also applies to providing a security domain 310 onto the smart card. In the example shown in Figure 6, a card issuer deploys smart cards to customers (step 500). A decision is made to install a vendor's application onto the issued smart card (step 502). When a dialogue between the issuer and the smart card is initiated, a pre-signed copy of the application is forwarded to the smart card (step 504). As previously stated, the dialogue between the issuer and the smart card can occur via any electronic device which can interface with a smart card and connect to an appropriate network. The application can be pre-signed with a key equivalent to that which already exists on the card so that each application has a unique signature that can be verified by the card.

**[0046]** Card domain 308 can then take the steps to load the application. Card domain 308 decrypts the forwarded application and checks the signature of the application (step 508). Card domain 308 can decrypt the application with the issuer's secret key. An appropriate cryptography method, such as Data Encryption Standard (DES) or 3DES, can be utilized to decrypt at least a portion of the application. Those skilled in the art will recognize that a number of cryptographic techniques may be used to implement embodiments of the present invention. For the purpose of illustration, symmetric key techniques are addressed herein, although asymmetric techniques are also contemplated. A good general cryptography reference is Schneier, Applied Cryptography, 2d Ed. (John Wiley, 1996), the contents of which are incorporated herein by reference.

**[0047]** It is then determined whether the signature on the application is valid (step 510). If the signature associated with the application is not valid, then the application is not loaded onto the card and the process ends (step 520). If, however, the signature associated with the application is valid the application is then installed and available for personalization. During personalization the application receives personalization data (step 512). Personalization data includes data which is unique to the smart card user. For instance, in a airline loyalty application, personalization data can include the smart card user's seating preference, meal preference, and eligibility for various possible perquisites. This personali-

zation data can also be signed and encrypted.

**[0048]** The application then invokes card domain's 308 decryption service for the received personalization data (step 513). Card domain 308 can then performs a signature check for the received personalization data (step 514). Methods of decrypting personalization data and performing signature checks are well known in the art. Finally, the application can then be activated (step 518).

**[0049]** A new application which as been downloaded onto a smart card post-issuance can be stored in a variety of ways. One example is to store the application into a file. Another example is to maintain a pointer to the application object.

**[0050]** Figure 7A is a flow diagram illustrating an example of card life cycle. The sequence is preferably considered irreversible. The first card state is when the smart card is Masked (700). During the Masked state (700), the smart card obtains its operating system, card identification, and preferably at least one application. The Masked state (700) is achieved as soon as all of the necessary components for card initialization are made available. An example of when necessary components are made available is when card domain 308 and OP API 306 are enabled, as well as the Java card environment being enabled, such as a Java card virtual machine and a Java card API.

**[0051]** After the Masked state, the next state is the Initialized ( 702) state. The Initialized state is achieved once all card activity requiring an initialization key is complete. As part of card initialization, if not already available, the card domain 308 application must be installed and registered. In addition , one or more security domains may also be installed and registered. These installed domains must then be selected and personalized. An initialization key is a secret key which is typically used by a smart card manufacturer during loading of data onto the smart card prior to issuance.

**[0052]** The next state is Load Secured ( 704). The Load Secured state is achieved after a secure install (post-issuance download) mechanism for loading of applications through the remainder of the card lifetime has been established.

**[0053]** The final card state is when the card is either expired or blocked ( 706). The blocked state is achieved as soon as an authorized smart card application has received a command to block the card.

**[0054]** The card life cycle is preferably an irreversible sequence of states with increasing security. Initialized and all subsequent card life cycle states and their transitions are preferably under the control of card domain 308. Card domain 308 executes and responds to commands that result in a transition in the card life cycle from one state to the next. These commands are preferably Application Protocol Data Unit (APDU) commands. Card domain 308 is also responsible for the installation of applications on the card, but preferably has no control over the applications' life cycle states. Each application

is preferably responsible for its own application life cycle state management but it preferably allows card domain 308 to have access to its life cycle states for auditing purposes.

**[0055]** The card life cycle is designed in such a way to increase the level of security enforced by the card at each successive state. As stated above, the cycle is also established as a process which can only ratchet forward to ensure that once the card begins a life cycle state with associated security policies, the only option is to cycle forward to the next state in the life cycle with a higher level of security. The card domain as the system security manager of the card maintains the current life cycle state, enforces the associated security policies, and controls the state transitions in the card life cycle.

**[0056]** Figure 7B is a flow diagram illustrating an example of an application life cycle. The application is initially unavailable (750). This state is achieved as soon as an applet is deleted and/or blocked from access. The next state is a loaded state (752). The application reaches the loaded state once the application has been physically loaded onto the smart card. The application is then installed (754), and registered (756). The installed state is achieved as soon as an applet has allocated all of the necessary space and data structures for operation. The registered state is achieved as soon as an applet has been included in the registry of applets. Once the application is registered, it can be deleted at any time thereafter. The next state is the personalized state, wherein personalized information is included in the application (758). The personalized state is achieved as soon as an applet has been updated with card holder specific data. Finally, the application may expire or be blocked (760).

**[0057]** Figure 8 is an illustration of an example of multi-application card life time line. The illustration does not include any off-card activities that occur prior to masking, initialization, personalization, Secure Install, nor activities that may be related to card management procedures. The illustration shows a card that contains six applications (A through F) over its lifetime.

**[0058]** In this example, application A can be installed in ROM and used during the complete life of the card from Masked ROM stage 800 to card blocked/expired stage 802. Application B is also in ROM and utilized during a first portion of the life of the smart card. The life of application B ends at stage 804. Application C is located in non-volatile memory, such as EEPROM, which is loaded during initialization. Application C is shown to expire at stage 806. Application D is also located in EEPROM and is used for the complete life of the card until card blocked/expired stage 802. Application E is installed at stage 808, sometime after issuance of the smart card. Application E is located in EEPROM and used until the end of the card life at card blocked/expired stage 802. Application F is also installed post issuance at stage 810, and expires sometime before the end of the card life at stage 812.

**[0059]** Figure 9 is a flow diagram of a method accord-

ing to an embodiment of the present invention for blocking a card. A card can be blocked if a breach of security is detected by an application. According to an embodiment of the present invention, a smart card can be blocked while an application is in use. A blocked card will no longer operate so that a suspect user cannot utilize any of the applications on the smart card. Blocking is merely one example of the many functions card domain 308 can perform in managing the other applications on the smart card. Examples of other functions include installing an application on the smart card, installing security domains 310A-310B, personalization and reading of card global data, managing card life cycle states including card blocking, performing auditing of a blocked card, maintaining a mapping of card applications to security domains, and performing security domain functions for applications which are not associated with a security domain.

**[0060]** In the example shown in Figure 9, an application is currently in use (step 600). The application detects a problem which triggers a card block request from the application (step 602). The application then sends a card block request to card domain 308 (step 604). Card domain 308 determines whether the card block request is valid (step 606). A card block request can be valid if the request originates from a predetermined application. If the card block request is not valid, the card domain 308 does not block the smart card (step 608). However, if the card block request is valid, then card domain 308 authorizes the card blocking (step 610), and card domain 308 blocks the smart card (step 612) such that the smart card will reject any attempted transactions for any of the applications on the card.

**[0061]** Figure 10 is a block diagram illustrating the use of security domain 310 by the card domain 308. The method and system according to an embodiment of the present invention allows for multiple application providers to be represented on a smart card in a secure and confidential manner. This security and confidentiality can be achieved through the use of security domains 310A-310B shown in Figure 3.

**[0062]** Figure 10 illustrates an example of a smart card which contains two security domains 310A-310B. In this example, it is assumed that a masked application 305A from the smart card is associated with a security domain, such as security domain 310A, and an additional application 305B will be added post issuance and be associated with a second security domain, such as security domain 310B. The arrows indicate key relationships between the various smart card entities as will now be described. Masked application 305A uses key services from security domain 310A for decrypting confidential data and optionally for full personalization. Card domain 308 uses key services from security domain 310B for decrypting and checking the signature of an application loaded post issuance, such as post issuance loaded application 305B. Post issuance loaded application 305B uses key services from security domain 310B for

decrypting confidential data and optionally for full personalization.

**[0063]** Figures 11A and 11B are further flow diagrams of an example for a method according to an embodiment of the present invention for providing an application onto an issued smart card. The card issuer decides to include a security domain 310 onto a smart card (step 1100). The issuer assigns security domain 310 to vendor A (step 1102). Vendor A, or an application developer on behalf of vendor A, generates cryptographic keys such as those used in symmetric or asymmetric cryptography operations (step 1104). Examples of these cryptography operations include encryption, decryption, MACing, hashing, and digital signatures. Examples of cryptographic methods which utilize such keys and are suitable for implementation for the embodiment of the method and system of the present invention include Data Encryption Standard (DES) and 3DES. The card personalization agent receives the keys and loads security domain keys associated with a specific security domain 310 for each smart card (1106). The card personalization agent receives smart cards and collects other data, OS, code, and application and card holder specific data, and places the data on the smart card (step 1108).

**[0064]** The card issuer then deploys the smart card to customers (step 1110). A decision is then made to install vendor A's application on the smart card (step 1112). When a dialogue between the smart card issuer and the smart card is initiated, a signed copy of the application is forwarded to the smart card (step 1114). The application can be signed with a key equivalent to that which already exists on the smart card so that each application has a unique signature that can be verified by the smart card.

**[0065]** The smart card's card domain 308 then takes steps to load the application. Card domain 308 invokes an associated security domain's cryptographic service to decrypt the application and check the signature (step 1118). It is then determined if the signature is valid (step 1120). If the signature is not valid, the process ends (step 1122). If, however, the signature is found to be valid, then the application receives personalization data which can be signed and optionally encrypted (step 1124). The loaded application then invokes its associated security domain's decryption service and signature check for the received personalization data (step 1126). Secret keys required to run or operate the application on the smart card are used to activate the application by authentication (step 1130).

**[0066]** Figures 12A and 12B are flow diagrams of a method according to another embodiment of the present invention for providing confidential information to an application using a security domain 310. The issuer decides to include a security domain 310 on a smart card (step 1200). A trusted party generates secret cryptographic keys and sends the keys to a card personalization agent in a secure manner (step 1201). A trusted party is typically a third party who performs the function of

certifying the source of information, such as a signature. A card personalization agent (which may be the same as the trusted party) receives the key and loads a unique secure domain key associated with a specific security domain 310 for each smart card (step 1202).

**[0067]** The card personalization agent receives the smart card and collects other data, such as OS, code, and application and card holder specific data, and places the data on the smart card (step 1204). The issuer then deploys the smart card to its customers (step 1206). A decision is made to install vendor A's application on the issued smart card (step 1208). Vendor A obtains secret keys for security domain 310 from the trusted party (step 1210). Vendor A then sends the smart card issuer a signed copy of Vendor A's application (step 1212).

**[0068]** When a dialogue between the smart card issuer and the smart card is initiated, a signed copy of the application is forwarded to the smart card (step 1214). The application can be signed with a key equivalent to that which already exists on the smart card so that each application has a unique signature that can be verified by the smart card. Card domain 308 invokes security domain's cryptographic service to decrypt the associated application and check its signature (step 1218). It is then determined whether the signature is valid (step 1220). If the signature is not valid, then the process ends (step 1222).

**[0069]** If, however, the signature is valid, then the application receives personalization data, which can be signed and optionally encrypted (step 1224). The loaded application then invokes security domain's decryption service and signature check for the received personalization data (step 1226). The cryptographic secret data required to run or operate the application on the card are used to activate the application (step 1230).

**[0070]** Figure 13 is a block diagram illustrating the use of cryptographic keys for post issuance loading of an application onto a smart card. Applications that are not masked and not loaded during card initialization stage or personalization stage need their executables downloaded using a secure installation method, such as the post issuance download described in the previous figures. The applications can be loaded using the card domain cryptographic keys. The applications are then decrypted and can have their signature verified using the key services of the corresponding security domain 310. Therefore, the desired security domain(s) 310 preferably have encryption and signature keys installed prior to the post issuance download of the corresponding application.

**[0071]** In the example shown in Figure 13, only one security domain 310 is shown since security domains 310 for other applications are not relevant to illustrate the downloading of a single application. Note that the result of the secure installation is initially a loaded application, which must then be installed, registered and personalized. After loading, the application is installed,

preferably by issuing an install APDU command to card domain 308. An application can be installed when its install method has executed successfully. Memory allocations have been performed by the time an application is in an install state. A loaded application should also be registered. When an application is registered, it is selectable and it is ready to process and respond to APDU commands. Installation and registration may be performed simultaneously by the same APDU command. An application is also personalized after loading. A personalized application includes cardholder specific data and other required data which allows the application to run.

**[0072]** In the example shown in Figure 13, the cryptographic key and MAC/Signature key are shown to be included in the functions of card domain 308/security domain 310. If a security domain is associated with the application being loaded, then the security domain will be invoked. However, if no security domain 310 is associated with the application which is being loaded, then the cryptographic key and the signature key of card domain 308 will be utilized. In contrast to the install commands sent to the smart card during the initialization phase, the post issuance install command is not issued in a secured environment, therefore it is preferably protected with a cryptographic key, such as a MAC/Signature key. Card domain 308 manages the post-issuance loading of a new application, while security domain 310 ensures the validity and integrity of the new application once the new application has been loaded onto the smart card. If a security domain 310 is not associated with the newly loaded application, then card domain 308 performs security domain's 310 functions. Once the new application is post-issuance downloaded, various keys such as a cryptographic key and a signature key are preferably utilized for installation and personalization of the application.

**[0073]** A method and system for a smart card domain and a security domain has been disclosed. Software written according to the present invention may be stored in some form of computer-readable medium, such as memory or CD-ROM, or transmitted over a network, and executed by a processor.

## Claims

1. A smart card comprising:

a card life cycle having a plurality of states;  
a memory including an indication of which of said states said card life cycle is in; and  
a card domain application including

an issuer key associated with the issuer of said smart card,  
a function for managing said life cycle of said smart card, and

a function for tracking the status of said life cycle of said smart card, whereby said card domain application represents the interests of the issuer and manages said card life cycle.

2. A smart card according to claim 1, wherein said card domain application further includes:  
a function for blocking said smart card.

3. A smart card according to claim 1 or 2, wherein said states of said card life cycle include masked, initialized, load secured and blocked.

4. A smart card according to any preceding claim, wherein said states of said card life cycle are in an irreversible sequence.

5. A smart card according to any preceding claim, wherein the contents of said memory determines the state of said card life cycle.

6. A method of blocking a smart card comprising the steps of:

detecting a problem with said smart card by an application of said smart card; sending a card block request from said application to a card domain application of said smart card, said card domain application having the capability to block said smart card;  
determining by said card domain application whether said card block request is valid; and,  
blocking said smart card by said card domain application, whereby said smart card is not operational for a user.

7. A method according to claim 6, wherein said card domain application includes an issuer key associated with the issuer of said smart card, whereby said card domain application represents the interests of the issuer.

8. A method of moving a smart card through a sequence of card life cycle states, said method comprising the steps of:

receiving said smart card in a masked state, said masked state indicating that components necessary for initialization are available on said smart card;  
initializing said smart card using an initialization key;  
placing said smart card into an initialized state;  
loading an application onto said smart card post-issuance; and,  
placing said smart card into a load secured state, whereby said smart card passes through

- a number of said states of said card life cycle.
9. A method according to claim 8, further comprising the steps of:
- 5 receiving a card block request;  
blocking said smart card; and,  
placing said smart card into a blocked states, whereby said smart card is not operational for a user.
10. A method according to claim 8 or 9, wherein said states of said card life cycle are in an irreversible sequence.
11. A method according to any of claims 8 to 10, wherein said states of said card life cycle are in an irreversible sequence.
12. A method according to any of claims 8 to 11, wherein said states of said card life cycle place said smart card into an increasing level of security.
13. A smart card comprising:
- 25 a first application having a sequence of life cycle states; and  
a card domain application including
- 30 an issuer key associated with the issuer of said smart card,  
a function for loading said application onto said smart card, said installing causing said first application to be placed into an installed state; and,  
35 a function for registering said application on said smart card, said registering causing said first application to be placed into a registered state, whereby said card domain application represents the interests of  
40 the issuer and manages said first application.
14. A smart card according to claim 13, wherein said card domain application further includes:  
45 a cryptographic service for loading said first application onto said smart card post-issuance.
15. A smart card according to claim 13 or 14, wherein said first application further includes:  
50 a function for personalizing said first application, said personalizing causing said first application to be placed into a personalized state, whereby said personalizing is under the authority of said first application.
- 55 16. A smart card according to any of claims 13 to 15, wherein said first application further includes:
- a function for blocking said first application said blocking causing said first application to be placed into a blocked state, whereby said blocking is under the authority of said first application.
17. A method of moving an application of smart card through a sequence of application life cycle states, said method comprising the steps of:
- 10 receiving said application on said smart card, said receiving placing said application into a loaded state;  
installing said application on said smart card, said installing placing said application into an installed state;  
15 registering said application on said smart card, said registering placing said application into a registered state;  
personalizing said application on said smart card, said personalizing placing said application into a personalized state, whereby said application is available for use.
18. A method according to claim 17 further comprising the steps of:
- 25 receiving an application block request;  
blocking said application; and,  
placing said application into a blocked state, whereby said application is not available for use.
19. A method according to claim 17 or 18, further comprising the steps of:
- 30 receiving an application delete request;  
deleting said application from said smart card; and,  
35 indicating said application is in a not available state, whereby said application is not available for use.
20. A method according to any of claims 17 to 19, wherein said application is received by being loaded into a memory of said smart card during initialization of said smart card, whereby said application is present on said smart card before issuance.
21. A method according to any of claims 17 to 19, wherein said application is received by being loaded onto said smart card post-issuance, whereby said application appears on said smart card after issuance.
22. A method of moving an application of smart card through a sequence of application life cycle states after issuance of said smart card, said method comprising the steps of:

issuing said smart card;  
indicating within said smart card that said ap-  
plication is in a not available state;  
loading said application onto said smart card  
post-issuance, said loading placing said appli- 5  
cation into a loaded state; and,  
installing said application on said smart card,  
said installing placing said application into an  
installed state, whereby said application is  
available for use on said smart card. 10

**23.** A method according to claim 22 further comprising  
the step of:  
personalizing said application on said smart card,  
said personalizing placing said application into a 15  
personalized state.

20

25

30

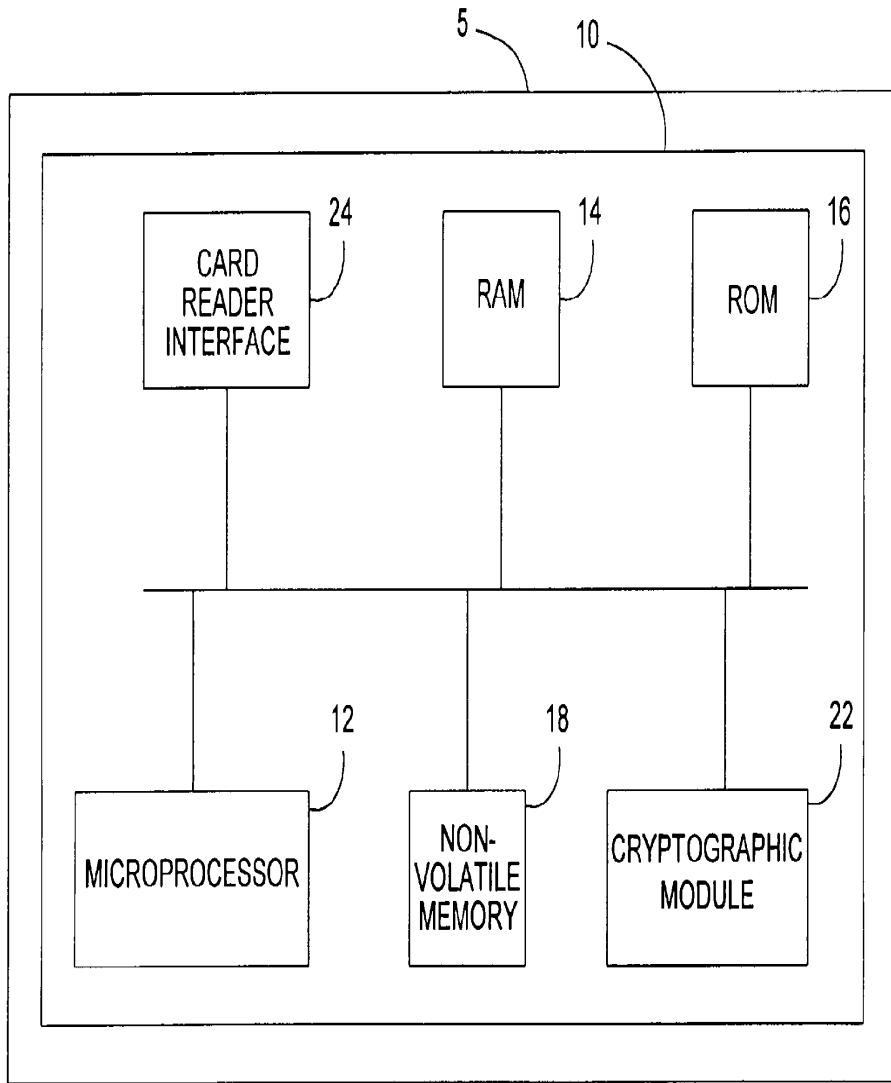
35

40

45

50

55



SMART CARD

FIG. 1  
(PRIOR ART)

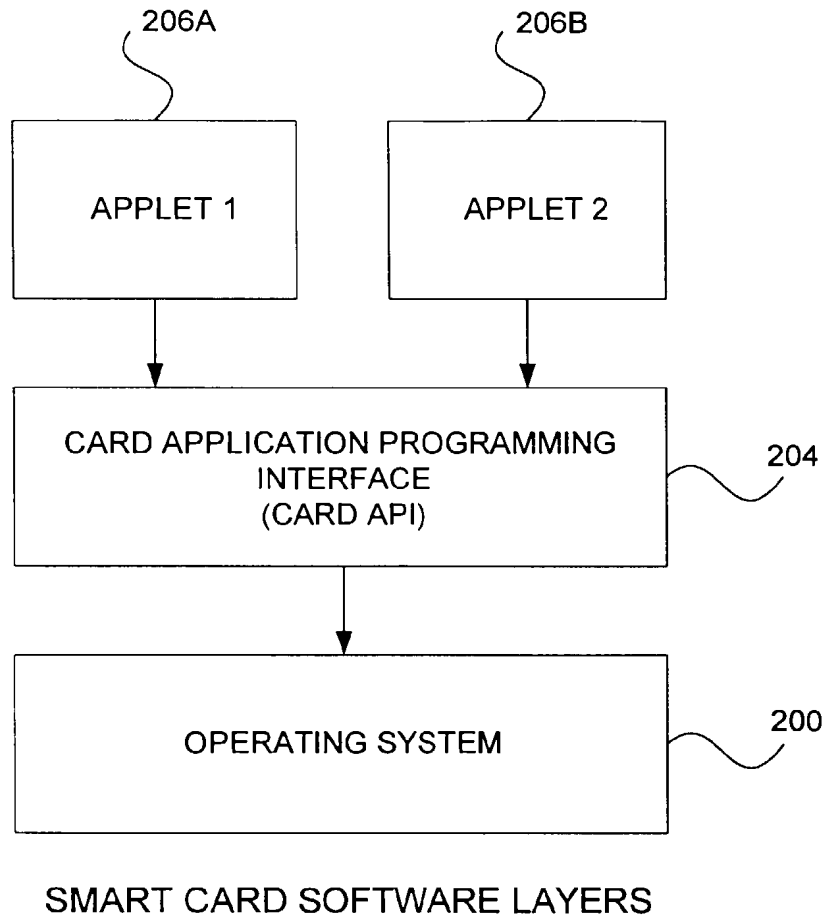


FIG. 2  
(PRIOR ART)



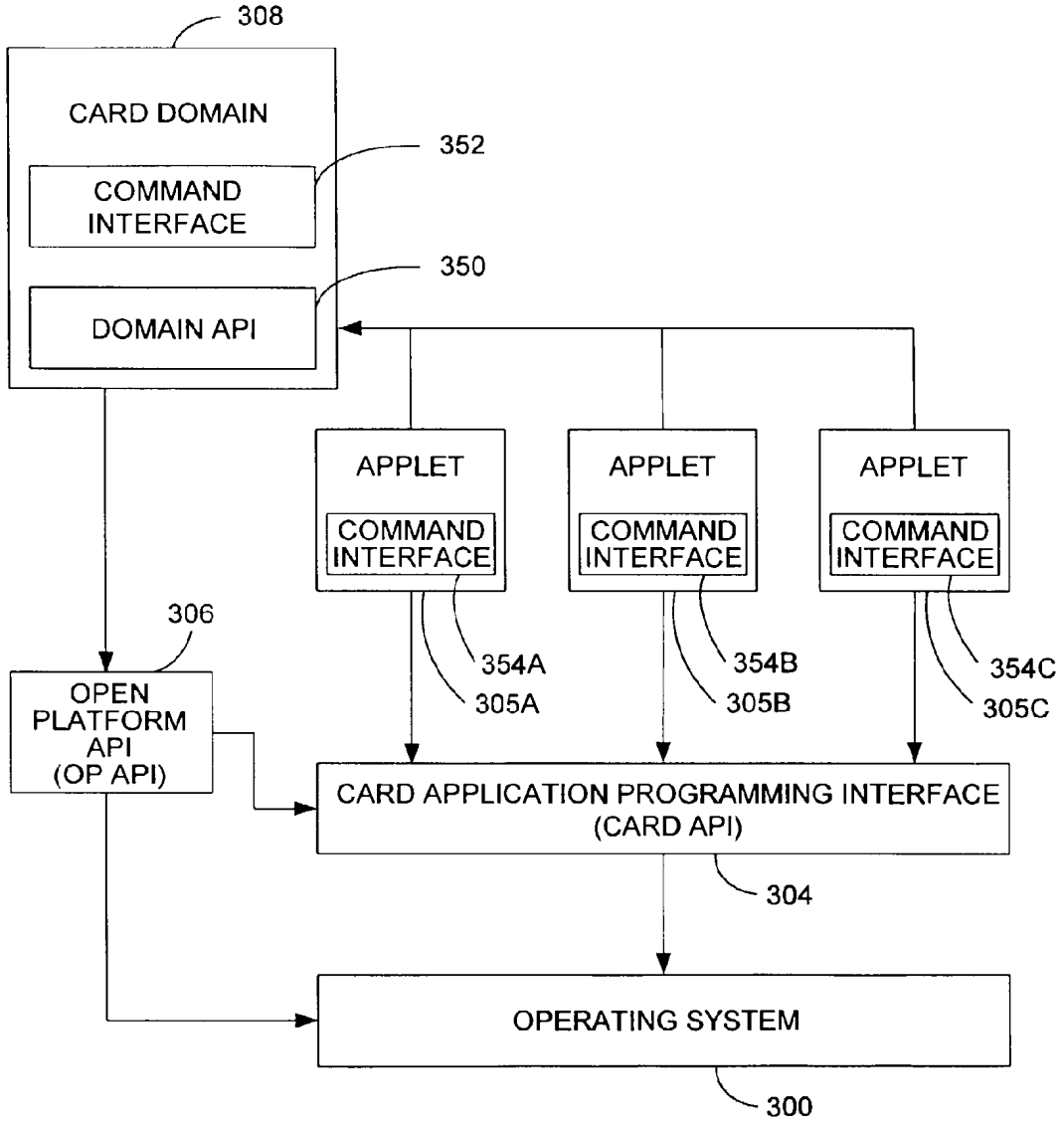


FIG. 3A

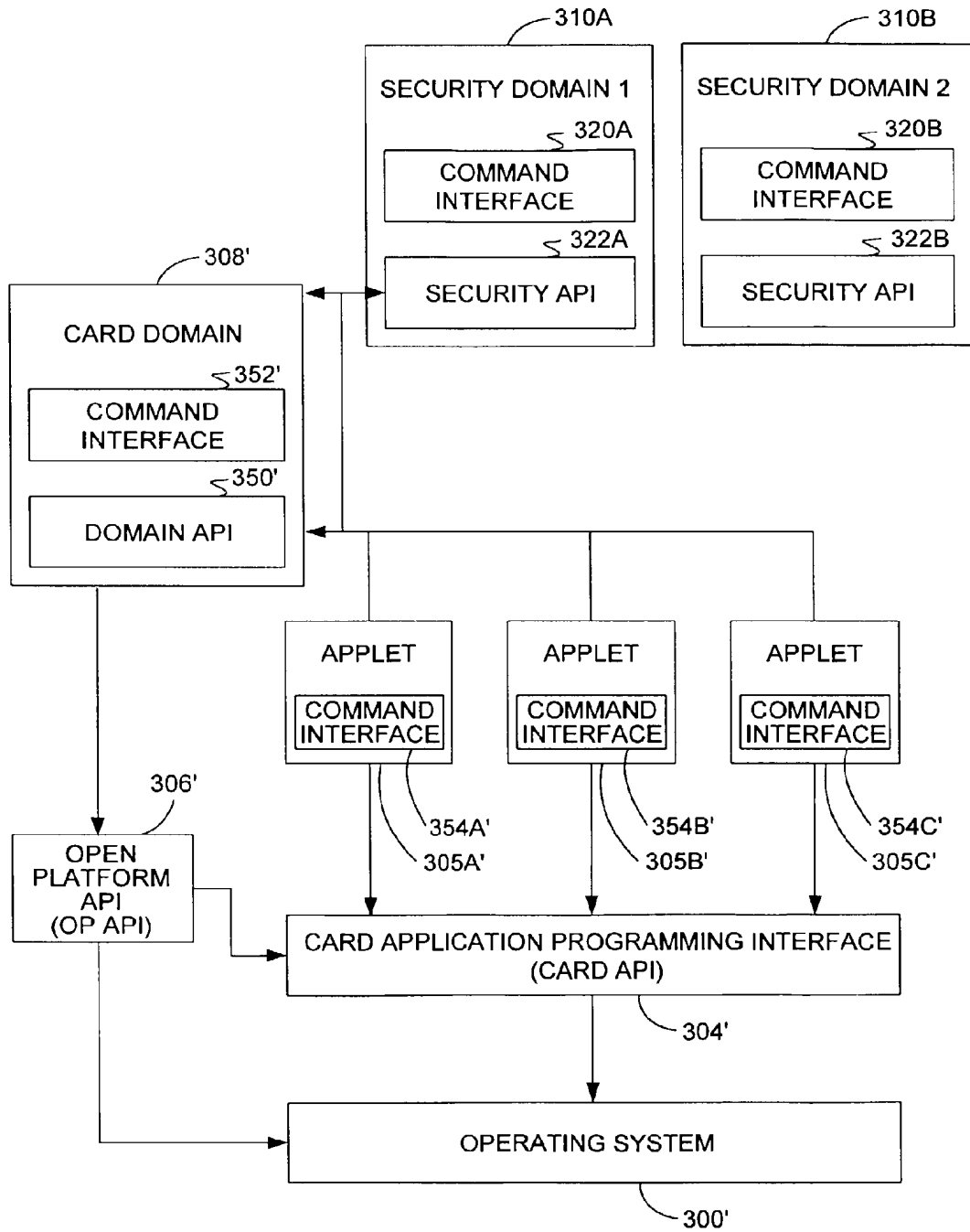


FIG. 3B

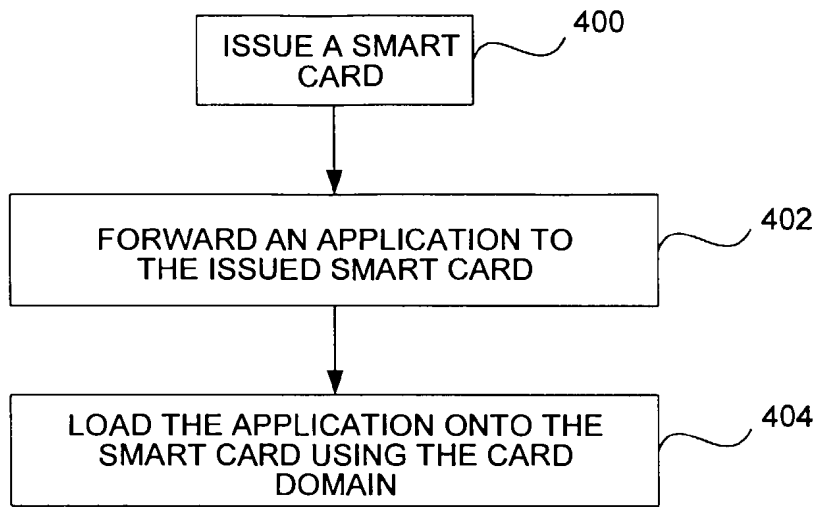


FIG. 4

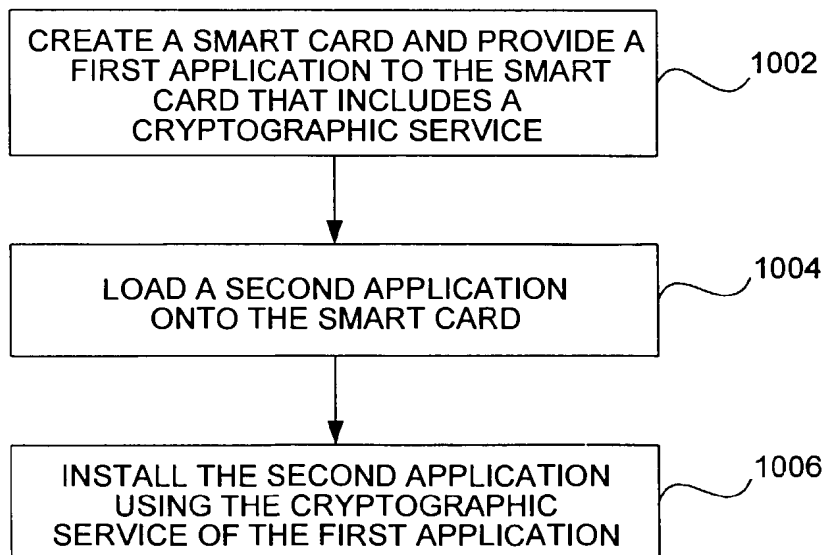


FIG. 5

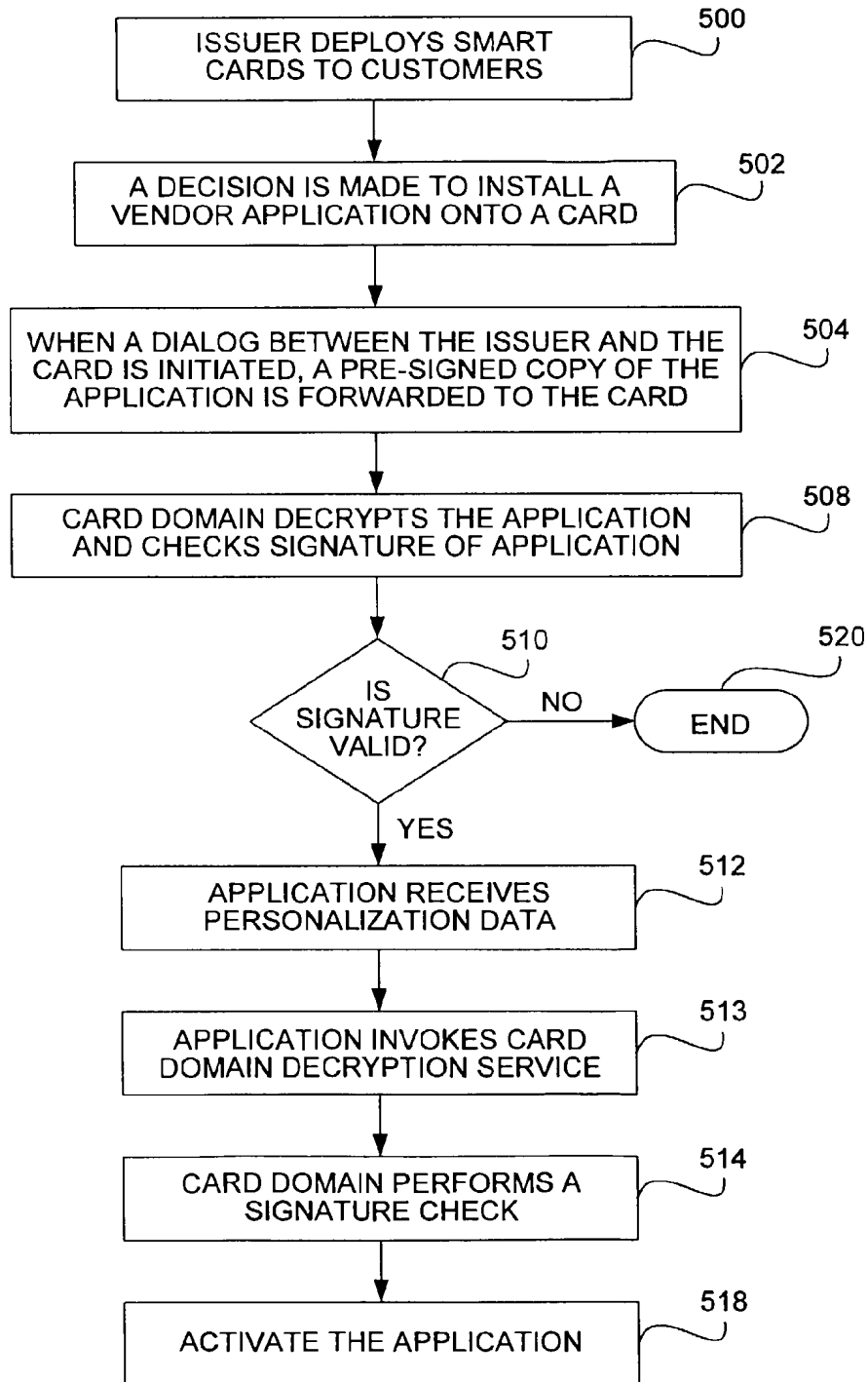


FIG. 6

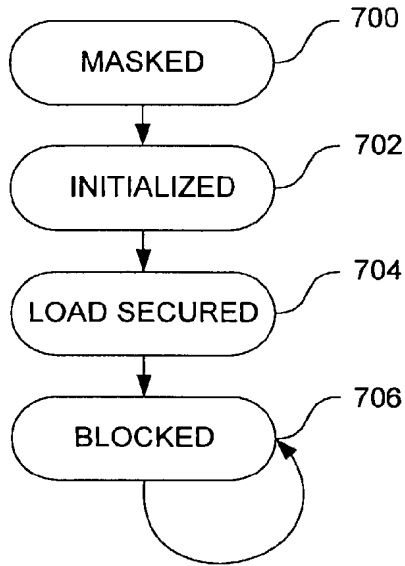
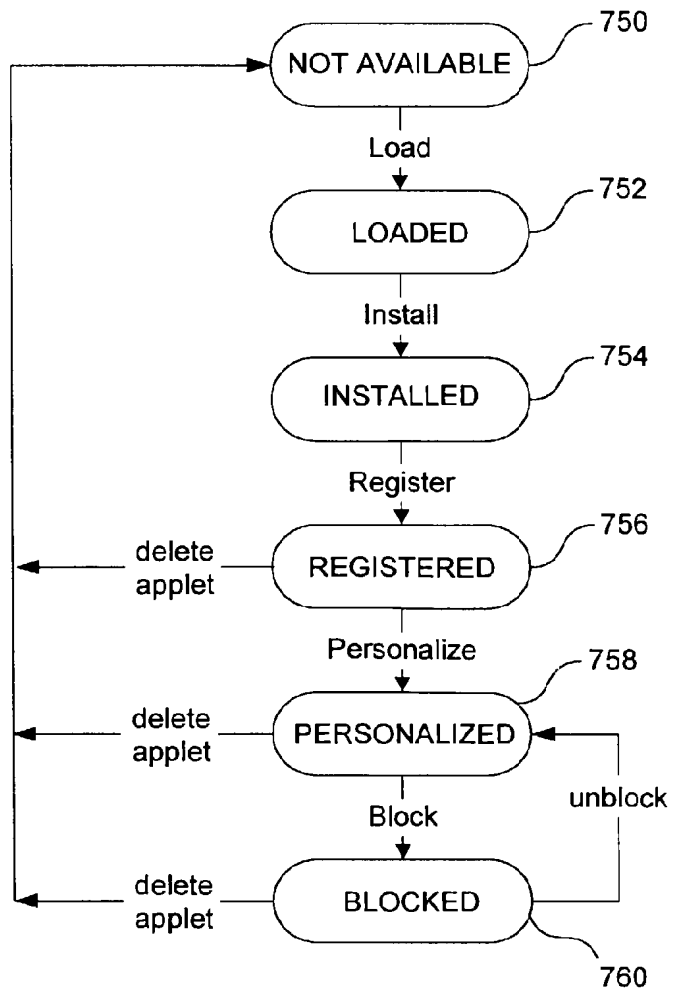


FIG. 7A

FIG. 7B



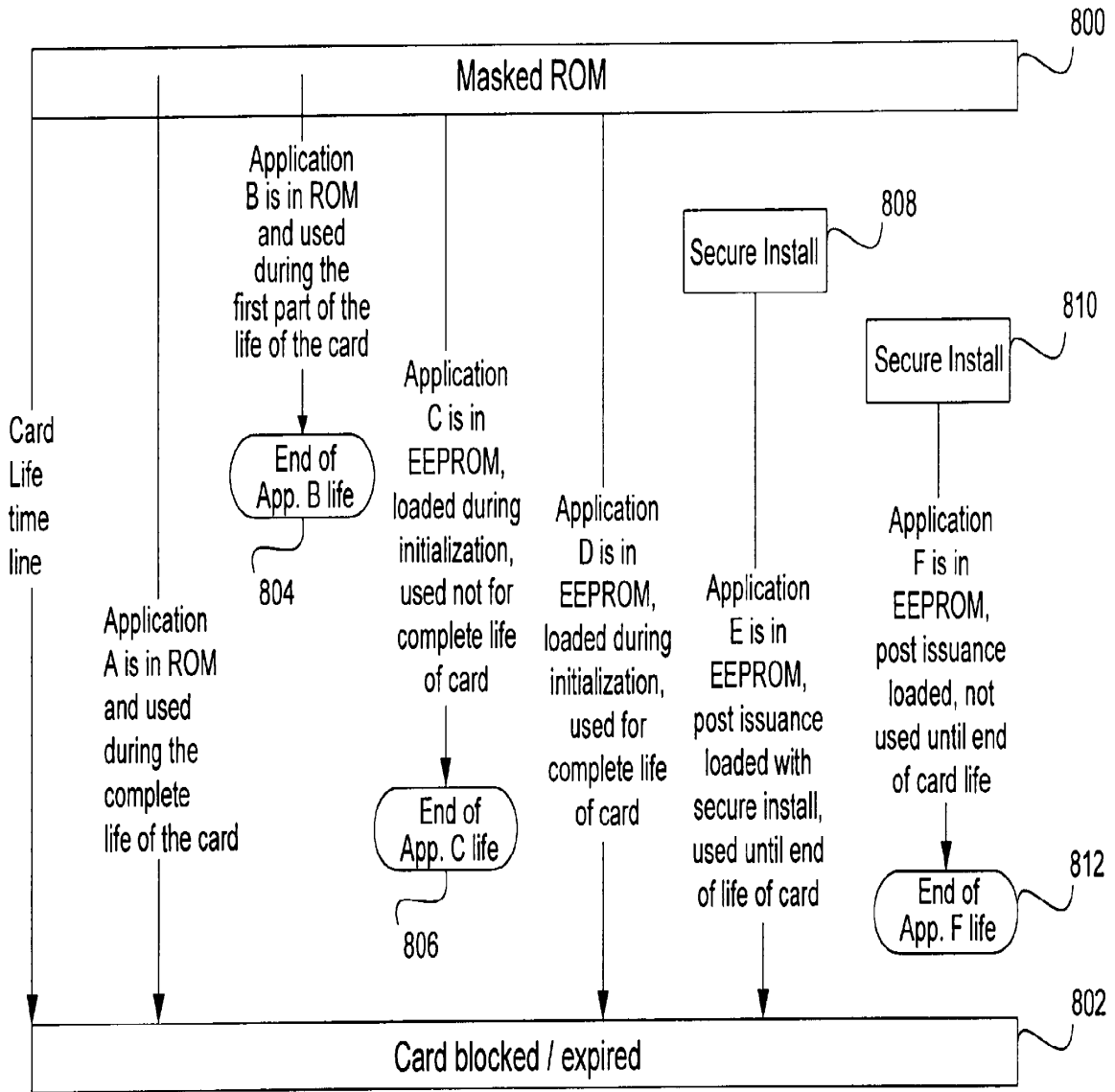


FIG. 8

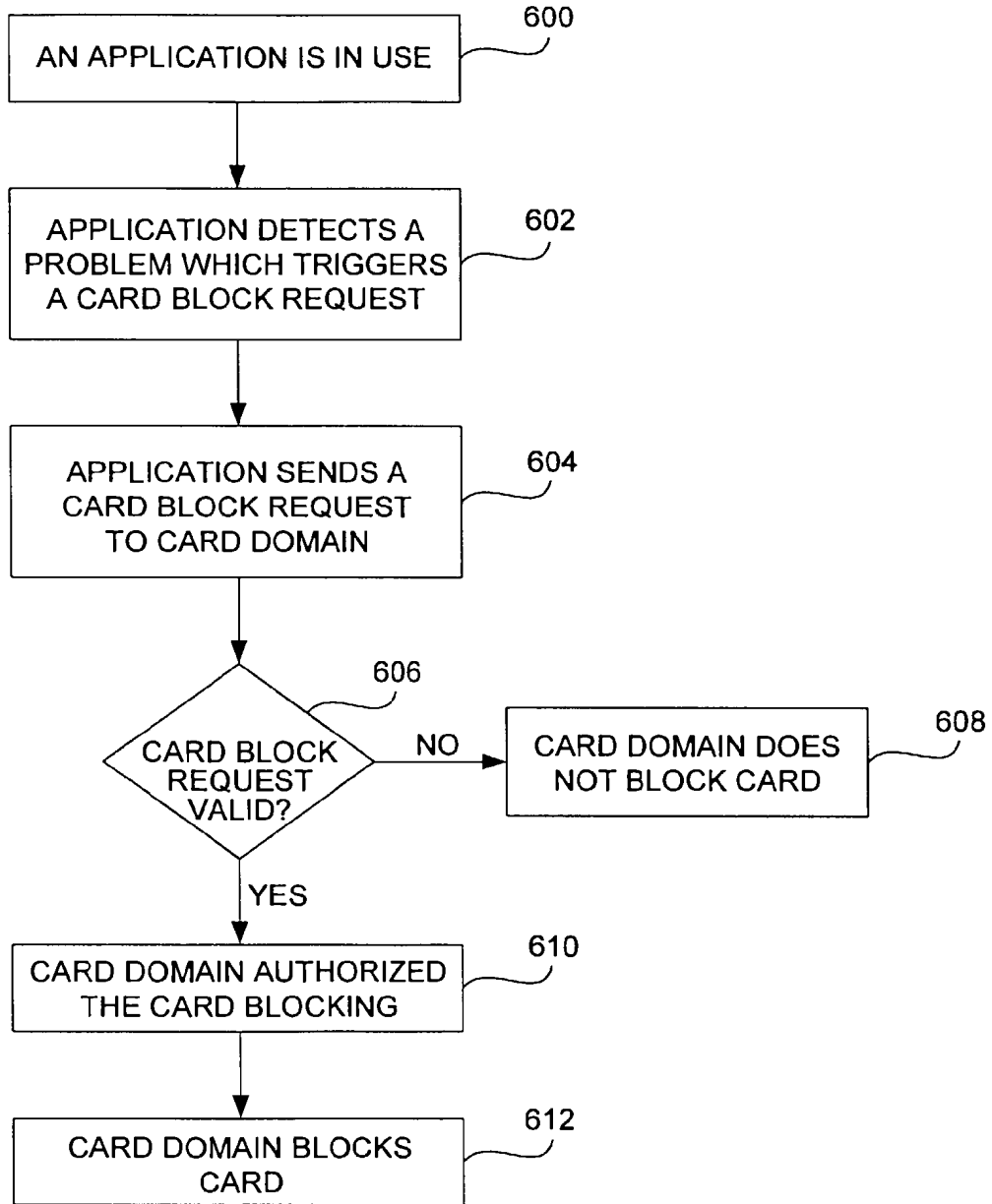


FIG. 9

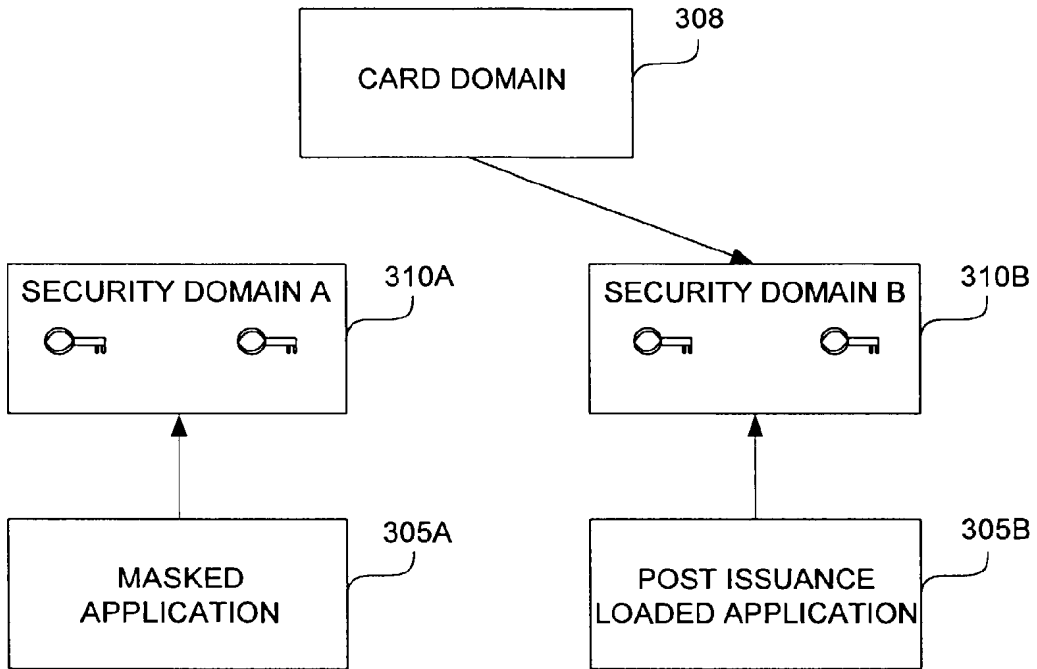


FIG. 10



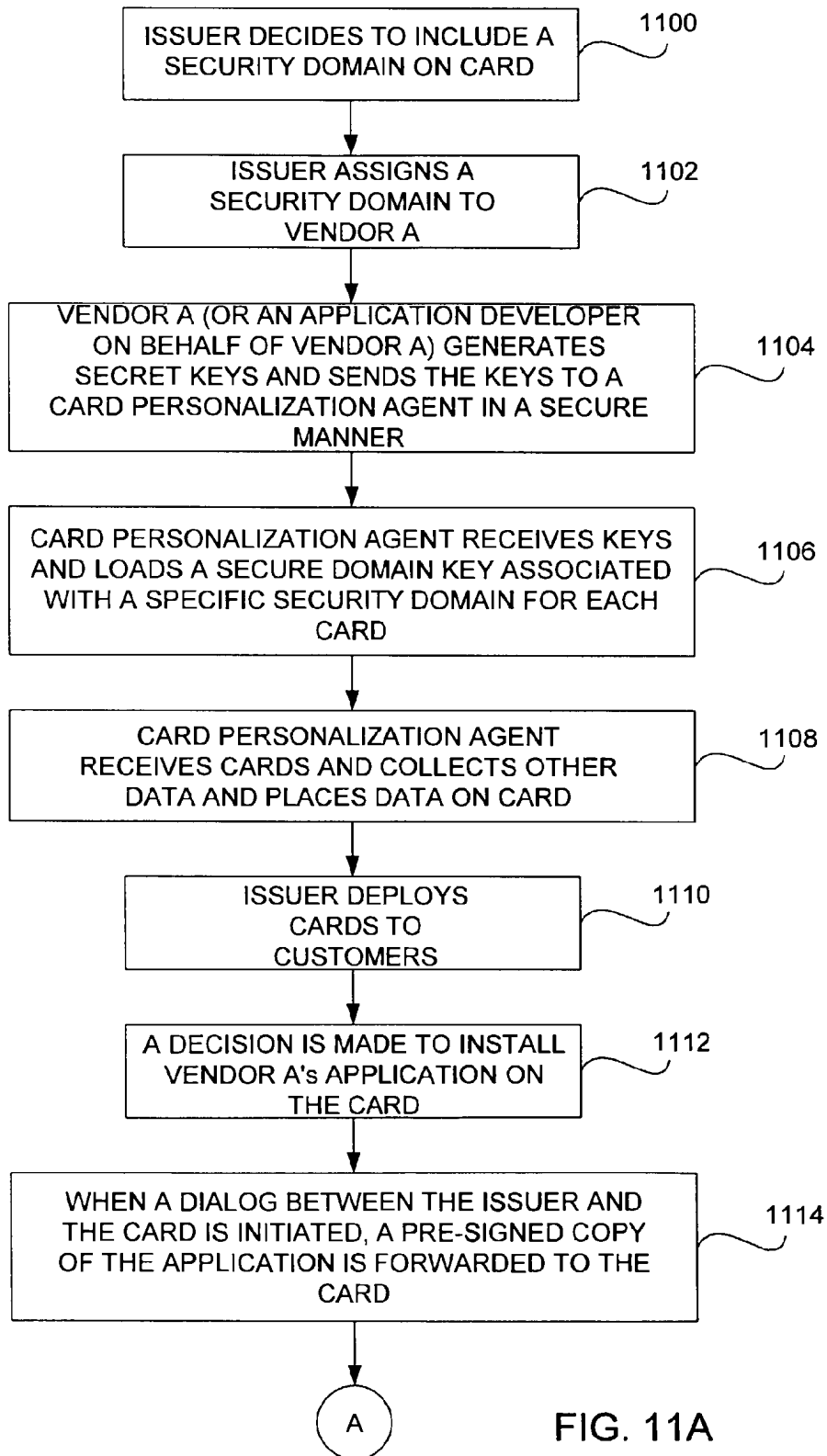


FIG. 11A

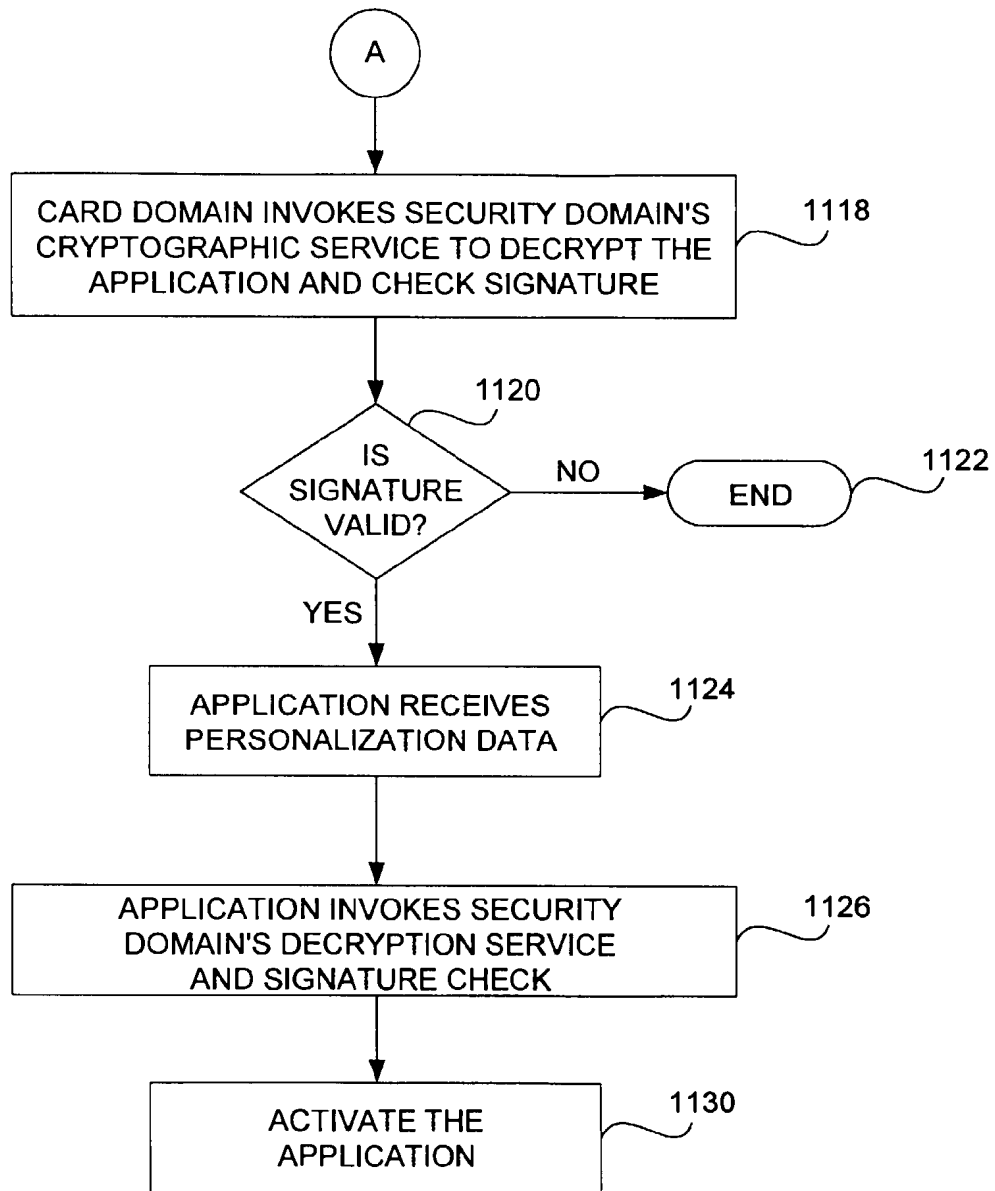


FIG. 11B

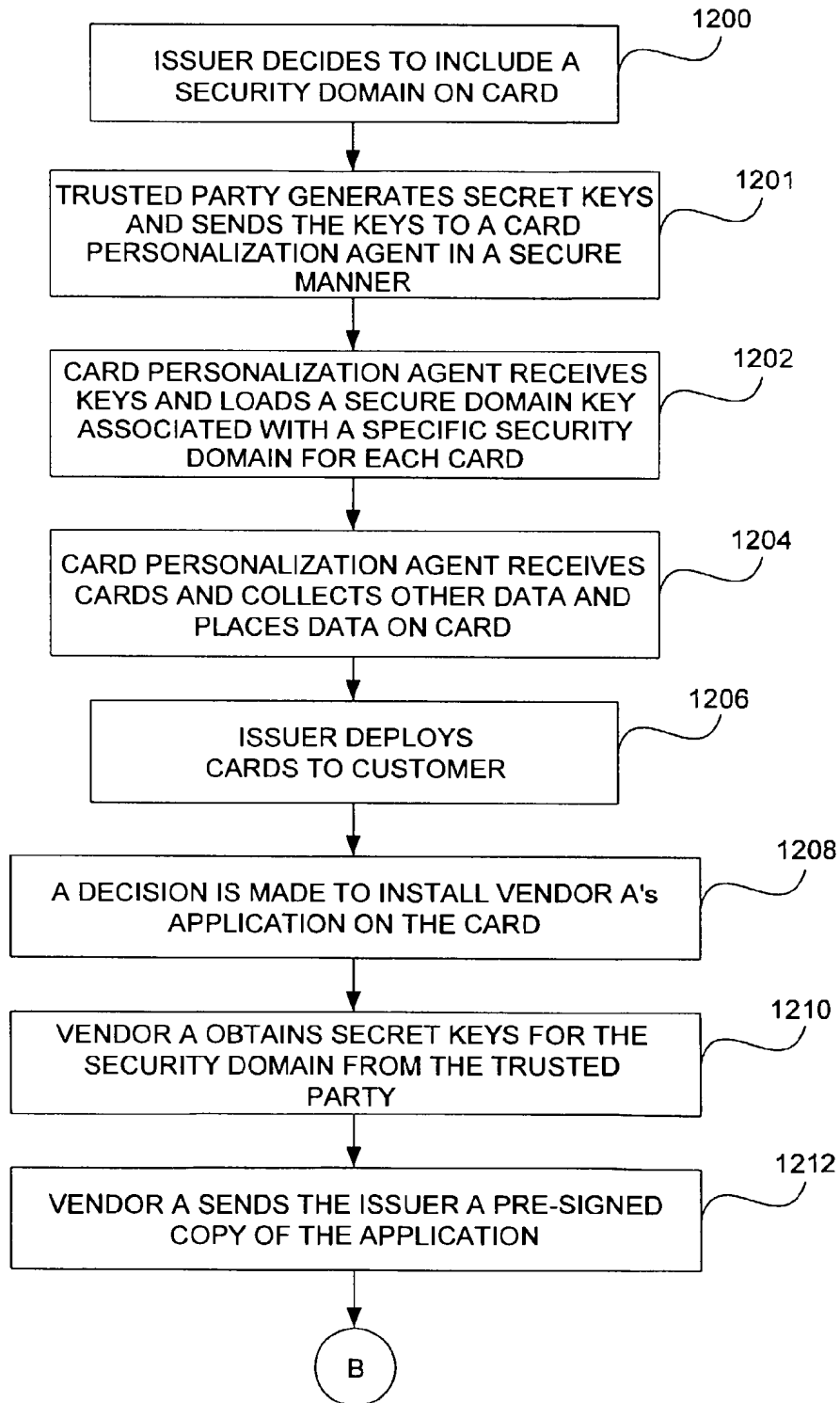


FIG. 12A

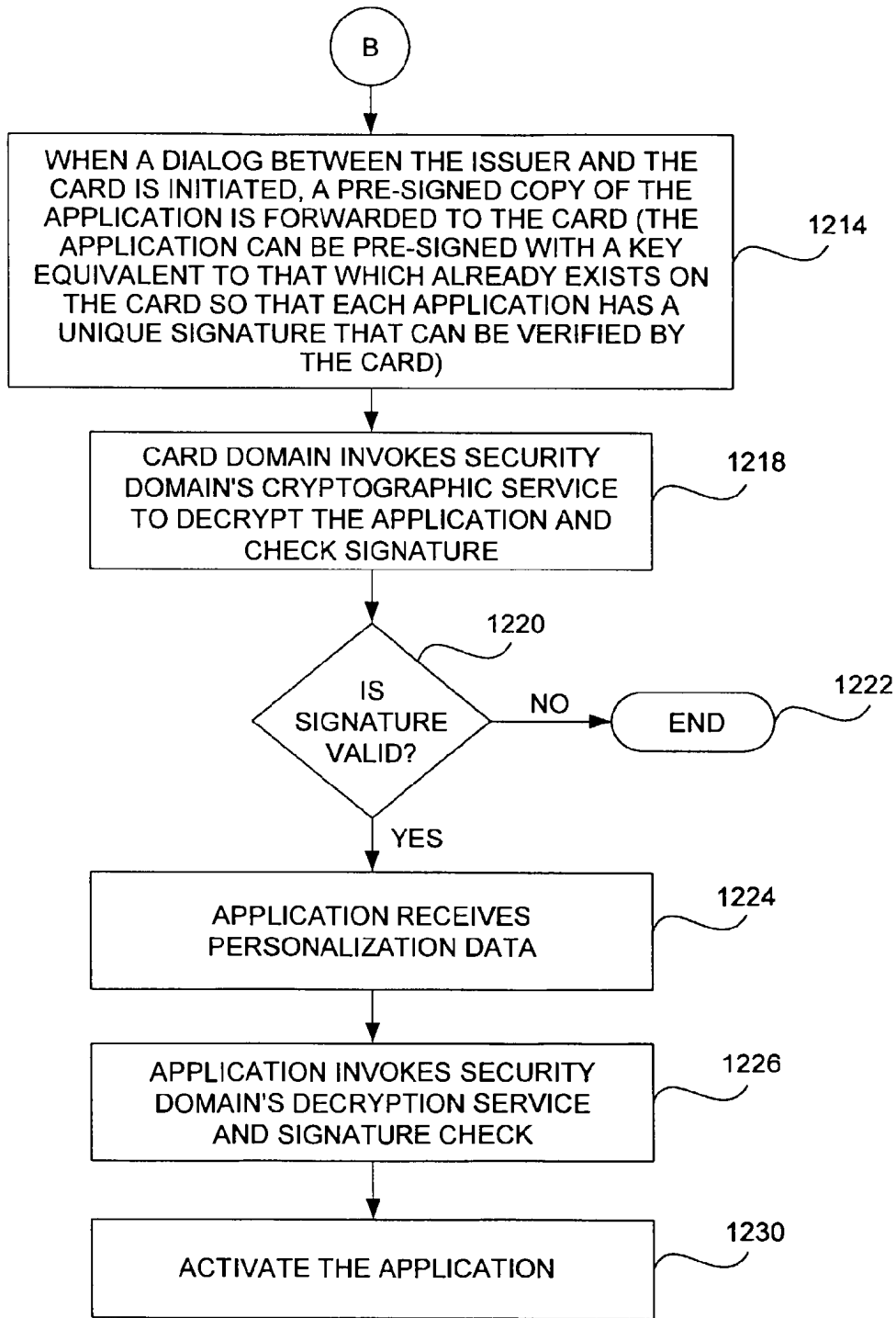


FIG. 12B

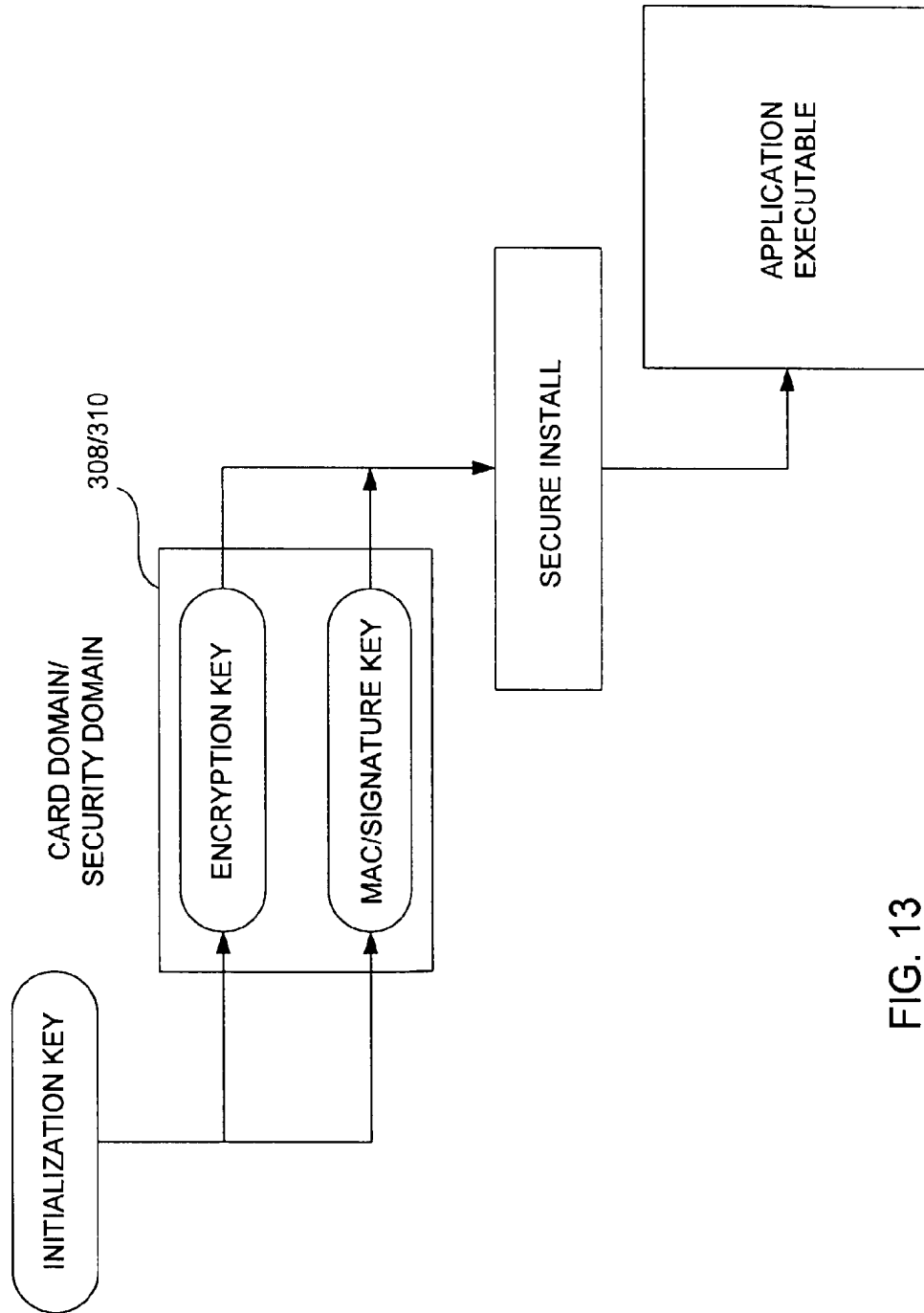


FIG. 13

---

(12) **UK Patent Application** (19) **GB** (11) **2 082 816 A**

---

(21) Application No **8010709**  
(22) Date of filing **31 Mar 1980**  
(30) Priority data  
(31) **7911393**  
(32) **2 Apr 1979**  
(33) **United Kingdom (GB)**  
(43) Application published  
**10 Mar 1982**  
(51) **INT CL<sup>3</sup>**  
**G06K 7/08**  
(52) Domestic classification  
**G4M A1 A2 B3 C1 D1 D4**  
**DX F2 F3 F4 K1 N6 RX**  
**G4A 17B 1C KB**  
(56) Documents cited  
**GB 11393/79**  
**GB 1504196**  
**GB 1314021**  
(58) Field of search  
**G4A**  
**G4M**  
(71) Applicants  
**J. W. Halpern,**  
**14 Belsize Park Gardens,**  
**London NW3,**  
**W. Ward,**  
**14 Belsize Park Gardens,**  
**London NW3**  
(72) Inventor  
**J. W. Halpern**

(54) **Solid state on-person data carrier and associable processing system**

(57) A personal identification data carrier contains solid state logic and memory elements and is associable with a data processing system comprising a computer and program control unit, data being transferable by a magnetic link between the data carrier and the computer. The data

carrier memory is a large scale I.C. chip in which the data may be erased and repeatedly altered. An amount of credit may be entered into this memory which may be added to or subtracted from when the data carrier is used for various transactions e.g. making a payment to a vending machine. The memory also has a part, which cannot be read out, into which a security check number is to be entered.

**GB 2 082 816 A**

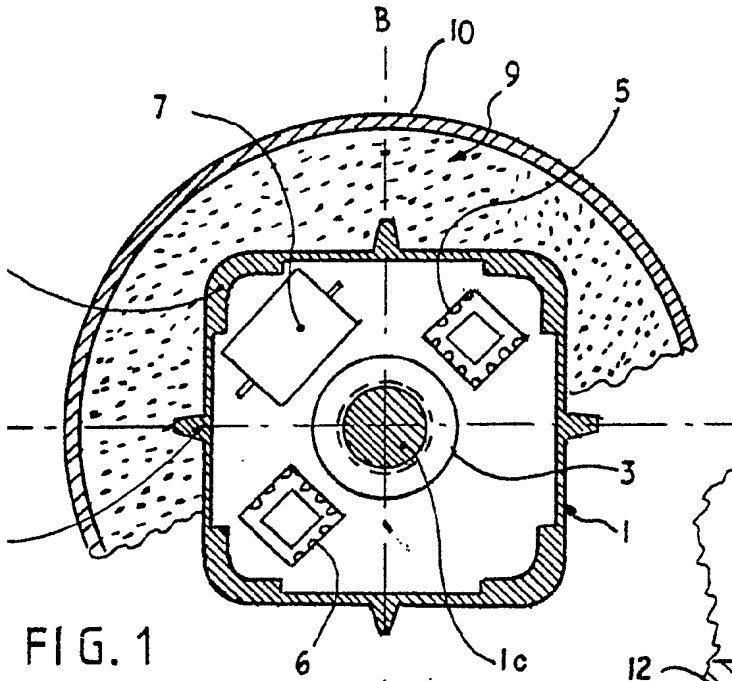


FIG. 1

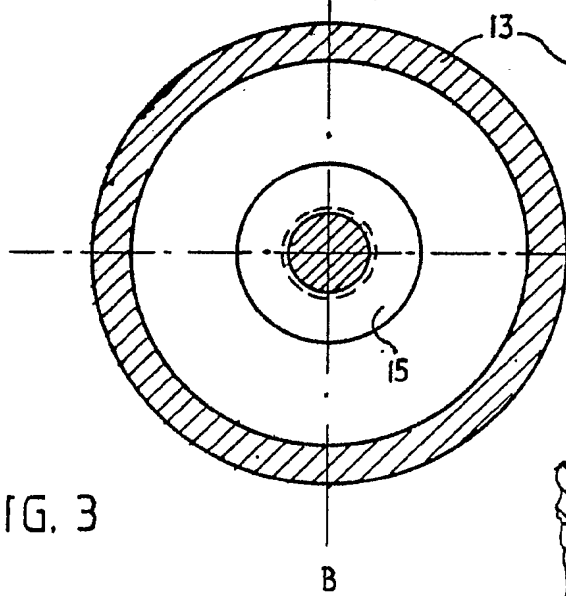


FIG. 3

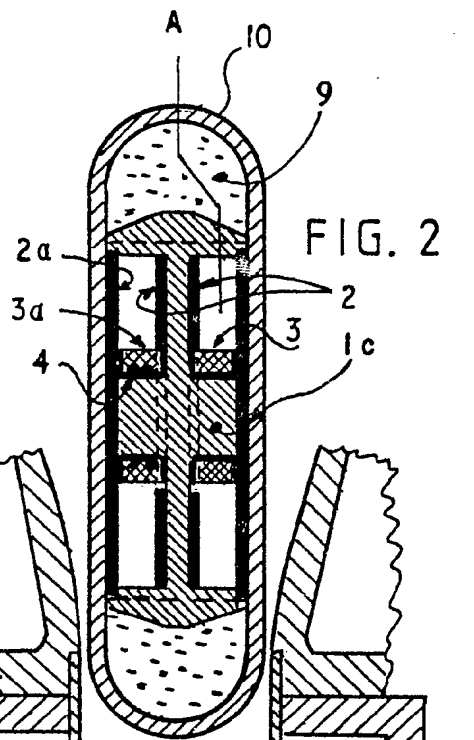


FIG. 2

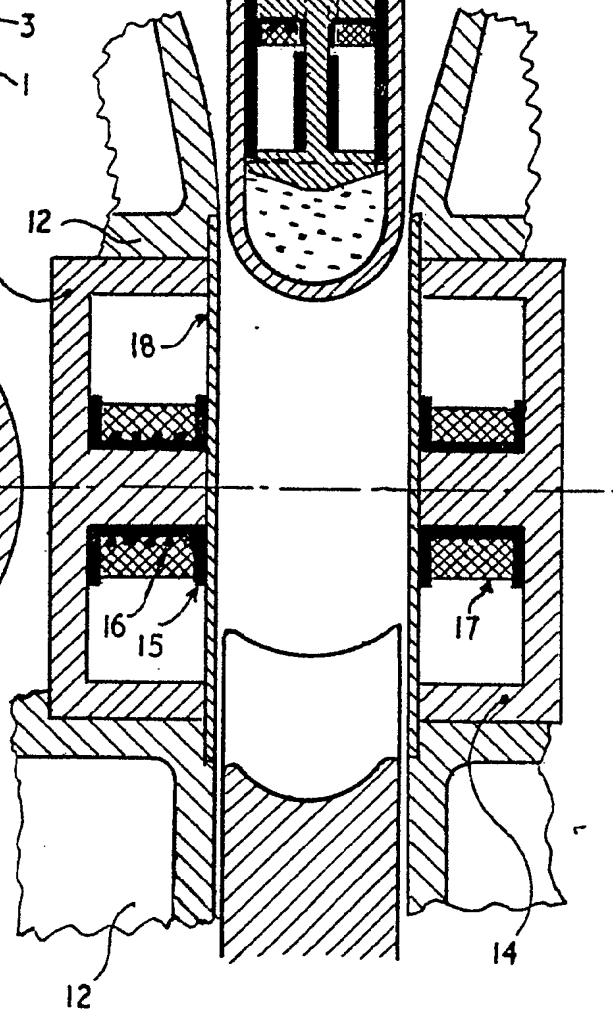


FIG. 4

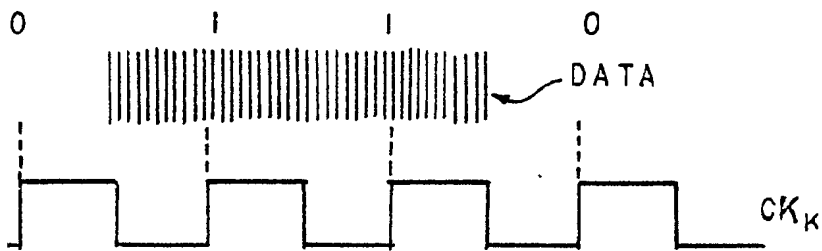


FIG. 5

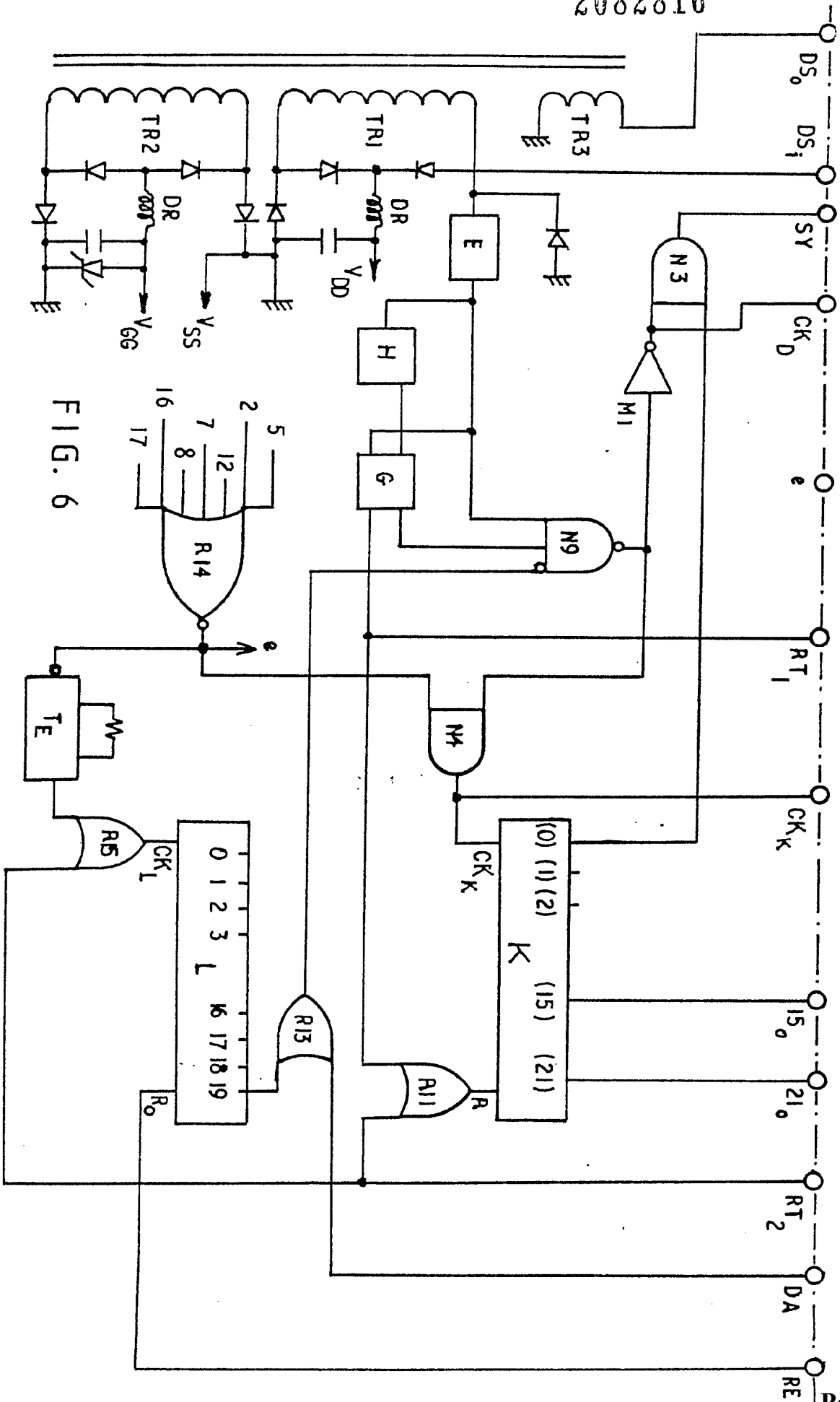


FIG. 6



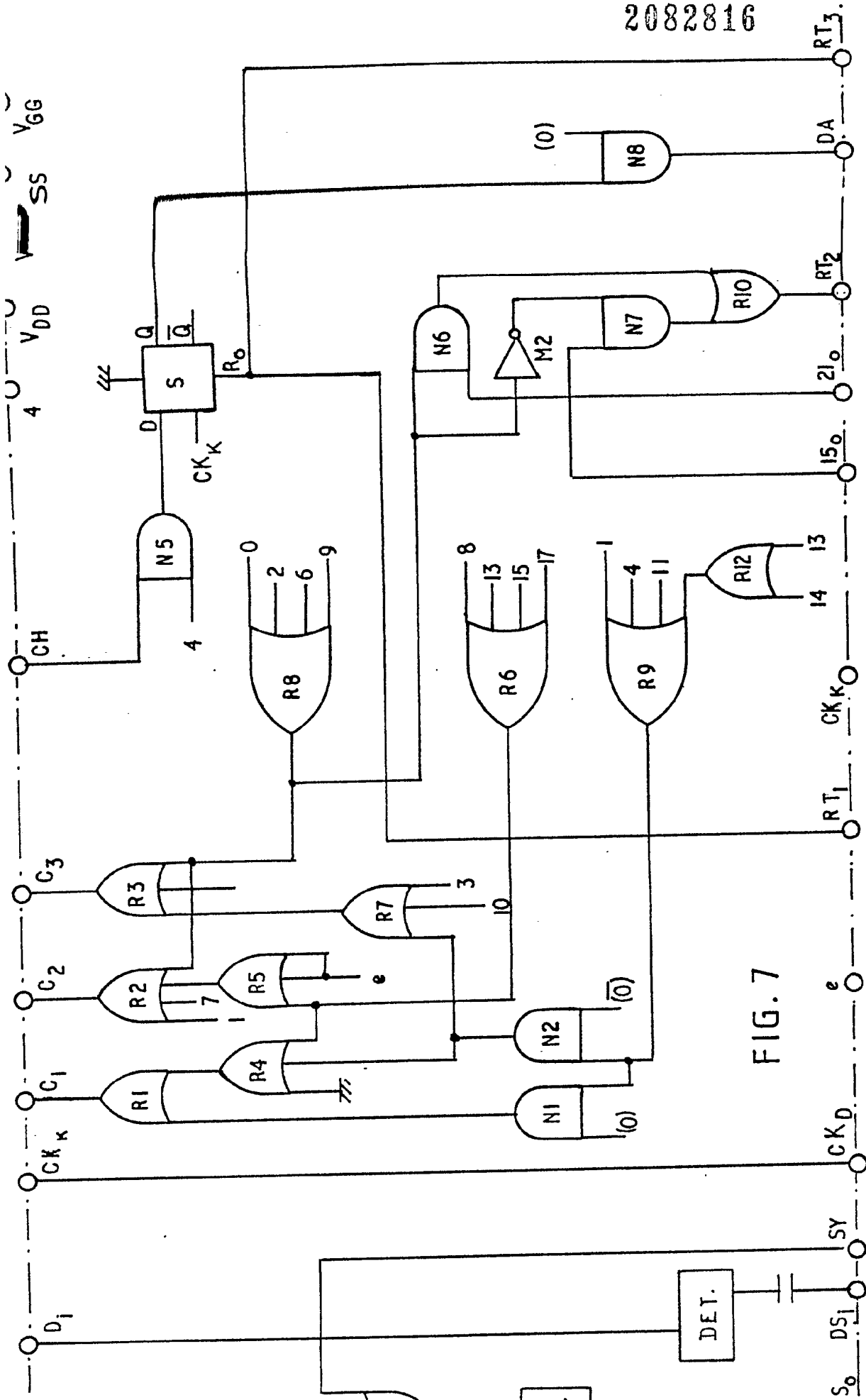


FIG. 7

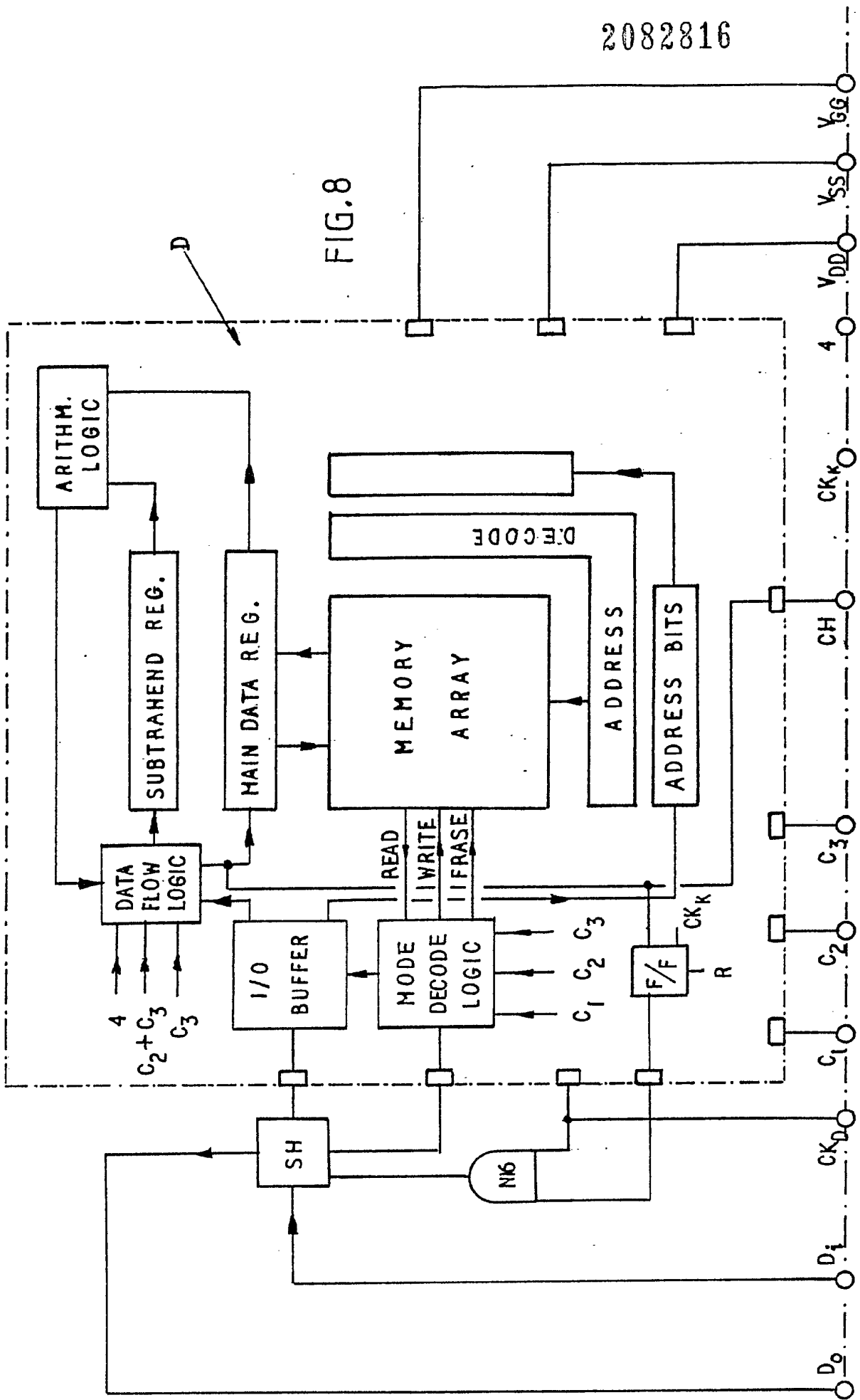


FIG. 8

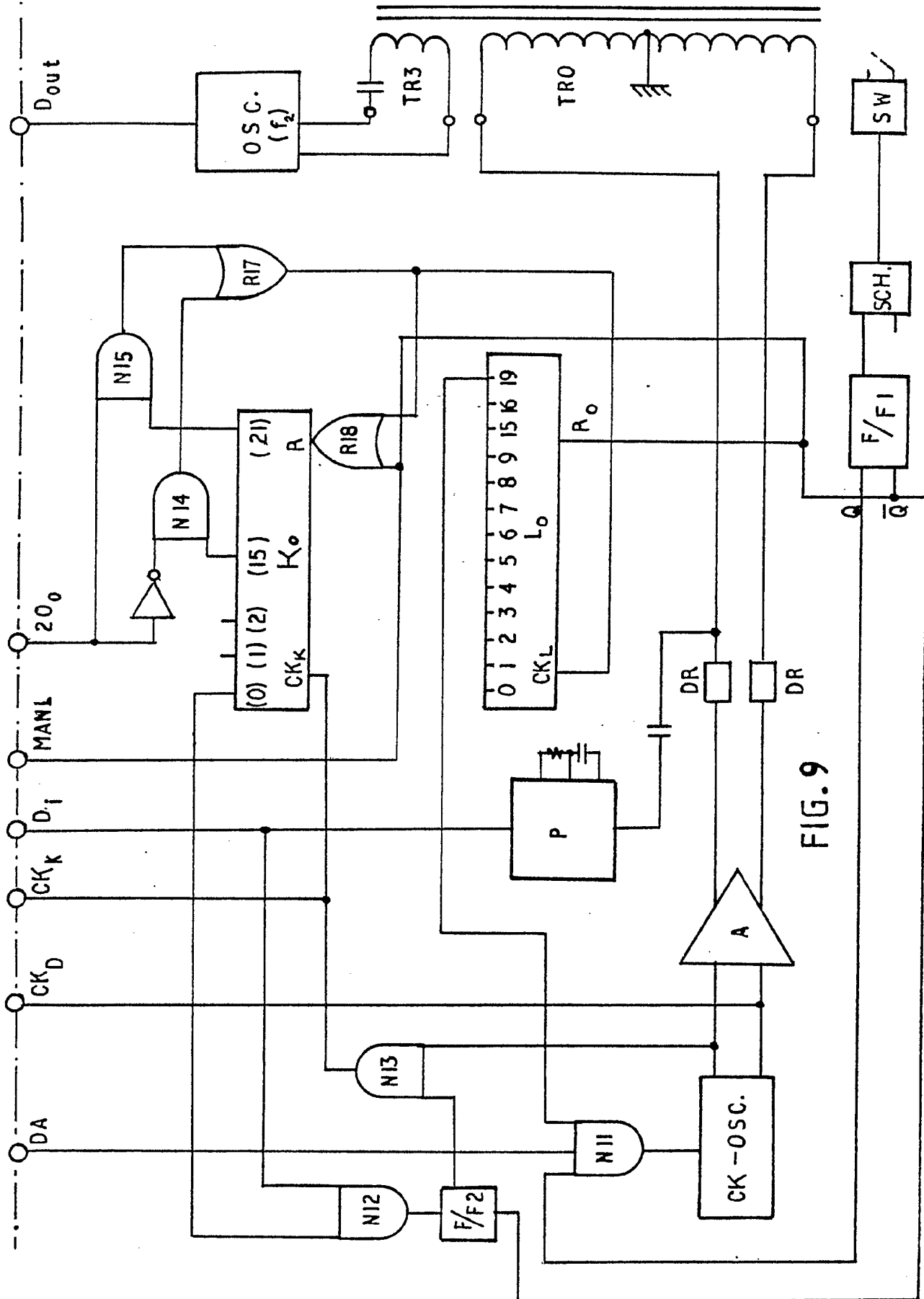


FIG. 9

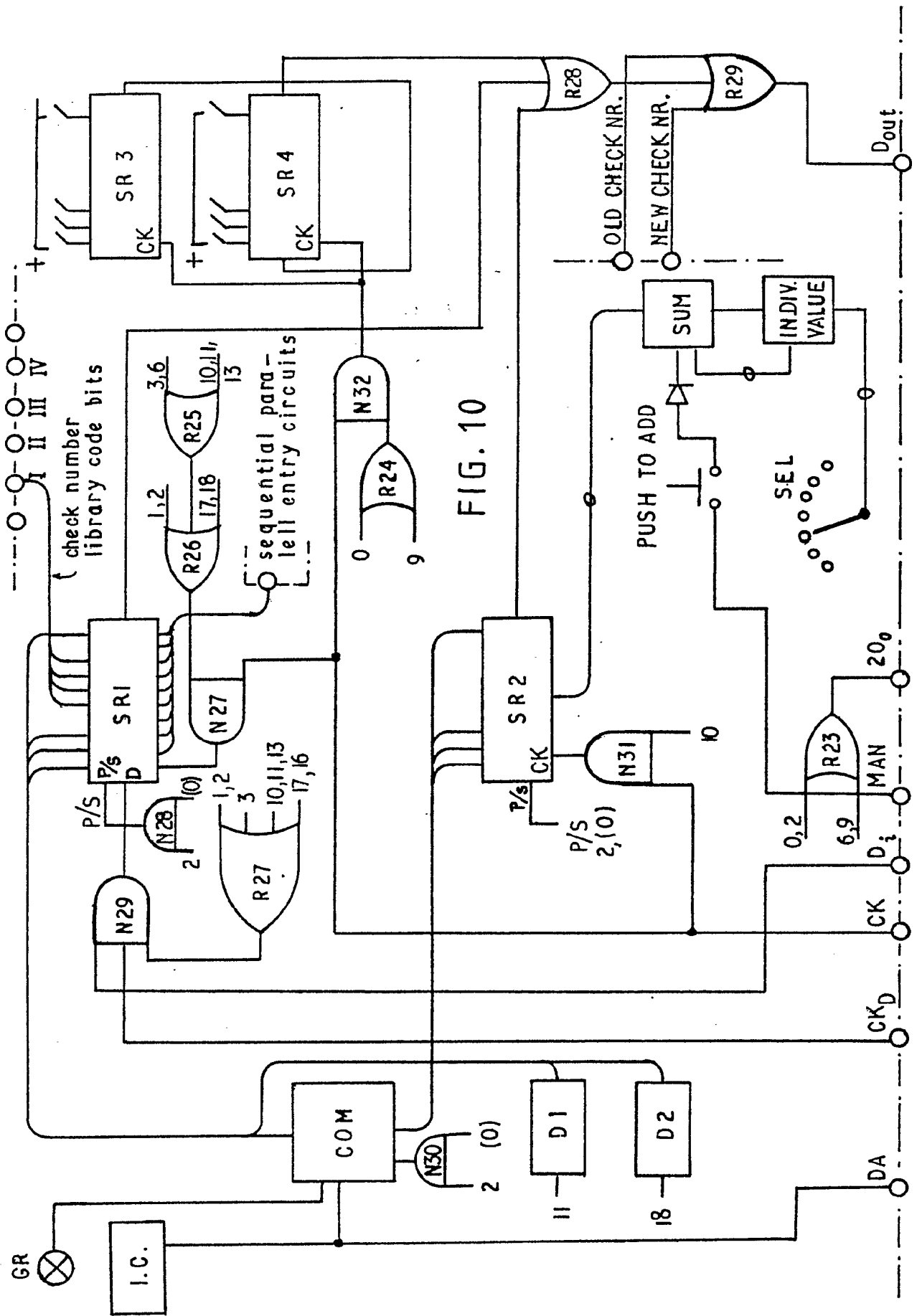


FIG. 10

## SPECIFICATION

**Solid state on-person data carrier and associable processing system**

## INTRODUCTION

The principle of a solid state pocket-size carrier of electronically stored digital data and the manner  
 5 of reactively transferring data bidirectionally between said carrier and a stationary computer has already 5  
 been described by the applicants in their US patent applications Ser. No. and their British Patent  
 1,314,021 (Digital Data Carrying Component and Associable Data Transfer Device). The degree of  
 security against fraudulent alteration of the data contents according to this patent was not very high but  
 this drawback was overcome by the introduction of a barrier in the form of a check number comparison  
 10 and a shut-down procedure after a number of fraudulent attempts as described in US patent No. 10  
 3,906,460.

Already British Patent 1,314,021 gives detailed description of a data carrier containing an inert,  
 programmable, memory device (magnetic core shift register, also solid state bistable register with  
 retentive magnetic loads), thus avoiding the need for a data maintaining voltage source (battery).  
 15 Recent technological progress has led to a fully solid-state electrically alterable Read Only Memory 15  
 (EAROM) and this may with advantage replace a magnetic core memory because of its smaller size. It  
 has also been proposed to use a so-called programmable memory in an on-person portable data carrier  
 (Br. Patent No. 1,504,196), in which the configuration of a fixed memory is pre-set by means of current  
 20 pulses which burn out unwanted inputs to tiny bistables. Such a memory may be usable in some 20  
 applications requiring only a fixed data word. Equally, so-called re-programmable memories were  
 suggested in which erasure of data must be done by means of Ultra Violet light. Such devices have poor  
 security and would have by far too slow operating speed for normal use.

It is thus one of the purposes of this improvement to show how an integrated circuit of the EAROM  
 type may be constructed, and used within an on-person solid state data carrier.  
 25 Another purpose of the invention is to provide a data carrier that can be inexpensively mass 25  
 produced.

A further purpose is to elaborate on various electro-magnetic configurations of the data carrier to  
 ensure, on the one hand, a satisfactory energy flow from the Sensor Unit to the data carrier circuit, on  
 the other hand contribute to both simplicity and reliability of the transfer of data from and to the data  
 30 carrier. 30

As described in the author's US and British patents, the data transfer is proposed to be carried out  
 by reactive coupling means which are hidden within the smooth surface of the data carrier. It is believed  
 that this is the best method for attaining a long-term reliable system, and the same method is used also  
 in the present invention. There exists another proposal (British Patent 1,504,196) in which the coupling  
 35 means are accessible at the exterior of the data carrying device in the form of light-emitting diodes and 35  
 photo transistors. The authors believe, however, that this method cannot offer long-term security  
 because of the unavoidable deterioration of the surface condition in the process of handling the card.

## DESCRIPTION

To summarize, this paper describes three innovative improvements. One is a method for  
 40 batteryless operation. Another is a simplified and more robust mechanical construction of the data 40  
 carrier. A third is the exact circuit for synchronizing the processing steps in the controlling computer and  
 the data component and to produce a start signal in dependence of the energy level injected into said  
 component. In the drawings which illustrate these improvements.

Figure 1 is a partial cross section A—A through a portable data carrier. 45

Figure 2 is a section B—B of the same. 45

Figure 3 is a sectional view of the data sensor unit.

Figure 4 is a section B—B through said data sensor showing clock drive and data coils.

Figure 5 is an auxiliary sketch showing by way of example the nature of the currents flowing in the  
 drive and data coils.

50 Figures 6, 7, 8 comprise the logic circuitry and the power supply circuit in the interior of the 50  
 portable data carrier of fig. 1 & 2.

Figures 9 and 10 showing the essential portions of the circuitry of the data transfer control unit  
 which is connected to the coils of the Data Sensor Unit, figs. 3 & 4.

*Description of the on-person data carrier, Figs. 1 and 2*

The same consists of a moulded or otherwise formed object 1 of a ceramic or semi-flexible ferrite 55  
 material having a central core 1c and finlike extensions 1b. The corners 1a of the essentially square-like  
 object are re-inforced in thickness. Coils 3 and 3a are fitted on the core. A further coil with fewer  
 number of turns is the coil 4. A printed circuit board 2 is attached to both sides of the central disk and  
 carries various electrical and IC components such as for example flat packages 5 and 6 or capacitor 7,  
 60 etc. The whole assembly may be closed by side plates 2a and potted in suitable resin or silicon 60  
 compound. The finished component may then be placed into two halves of a flat disk 10 the hollow  
 spaces of which filled with a softer grade of elastic material 9. Afterwards the two half spheres are

moulded and fused together, for example by microwave heat.

*Description of the Sensor Unit, Figs. 3 and 4*

The same consists in this example of two halves fitted into a supportive frame 12. This frame also serves as a receptacle for the data carrier component 10 which, as the drawing indicates, may be  
 5 dropped into the sensor unit after which it would come to rest on the piston 20. The latter may be so  
 connected to mechanical actuators that on completion of the data transfer transaction it is either  
 sideways withdrawn permitting the data component to drop into a receptacle, or the piston 20 is lifted  
 upwards to return the component 10 to the user. 13 and 14 are the above mentioned two parts. The  
 outer diameter of the potlike insert is about equal to the diagonal dimension of part '1' of the On-person  
 10 data carrier. Drive coils are 15 and 17; 16 has again fewer turns and mediates the data signal which, in  
 this example, has a higher frequency than the clock pulses injected into the coils 15 and 17.

*Description of the circuitry of the on-person data carrier*

Figures 6, 7 and 8 should be laid together, with Fig. 6 at the bottom and Figure 8 uppermost, to  
 form one single circuit. The same provides an example for realizing an on-person data component by  
 15 using a non-volatile ROM with repeatable data alteration capability. It is clear that the adaptation of the  
 idea depends on the specific type of memory. The present description is oriented to a GI (General  
 Instruments) chip known as ER 1400 for which a data sheet may be supplied. This circuit depends on  
 the use of separate erase pulses having a negative voltage for erasing a memory location. More recent  
 devices may not require this operation step but, on the other hand, may require others. What is  
 20 described hereunder should therefore be taken only as an illustration of a principle. — In the here  
 proposed EAROM IC chip, one alteration has been made. Whereas the General Instruments device  
 employs all-but one of the 'mode control inputs'  $C_1$ ,  $C_2$ ,  $C_3$ , the unused one being , this latter  
 combination is used for the command 'Enter data stream into the Subtrahent Register'. The GI device  
 has no subtrahent register.

The transformer coil TR1 in Fig. 6 is identical with coil 3a in Fig. 2. The coil TR2 in Fig. 6  
 25 corresponds to coil 3, Fig. 2, and TR3 corresponds to coil 4, Fig. 2. TR1 carries clock pulses as indicated  
 in Fig. 5 and produces a dc output at  $V_{DD}$ . TR2 carries the same clock pulses and produces a negative  
 voltage  $V_{GG}$ . TR3 carries only data pulses phase shifted against clock pulses as indicated in Fig. 5; they  
 consist of pulses of a much higher frequency which are detected by tuned circuits or by a phase-locked  
 30 loop circuit such as shown (integr. circuit 'P') in Fig. 9, or 'DET' in Figure 7.

*Method for causing the minimum voltage dc level being built up in the data carrier after insertion into the Sensor Unit to produce a synchronising pulse*

It must first be explained that the exchanging of data depends on the correct, synchronous  
 operation of counters in the Control Unit circuit (figs. 9 and 10) and in the on-person component (figs. 6,  
 35 7, 8). In the former, these counters are word bit counter  $K_0$  and process counter  $L_0$ , in the latter bit  
 counter K and process counter L. The synchronizing pulse is generated in circuit fig. 6 and is passed via  
 the sensor/data component transformer configuration to circuit fig. 9 causing there bystable F/F—2 to  
 set. The following is a detail explanation:

The clock pulses are shaped in 'E', fig. 6 and passed on to Nandgate N9 as also to a voltage sensor  
 40 'H'. As  $V_{DD}$  voltage is being built up beyond a required minimum level 'H' produces a dc output which is  
 applied to 'G'. 'G' is a bistable clocked by output from 'E', i.e. by rising pulse fronts. When 'G' goes high,  
 output from Nandgate N9 goes low,  $CK_k$  at word bit counter K goes also low but this produces no count  
 pulse as yet. The output SY from Nandgate N3 goes high to pass on an enabling pulse to OSC via OR  
 gate 16. A high frequency pulse burst is generated in TR3 and detected by 'P' in fig. 9 producing a  
 45 corresponding high-level dc output into Nandgate N12 thereby setting F/F—2. When next a clock pulse  
 from CK—OSC. goes high, N13 passes on a count pulse to counter  $K_0$  for the first time. The same also  
 happens in the coupled data component with counter K. From that moment onwards all the events in  
 the coupled circuit groups proceed in synchronous steps. The counters  $L_0$  and L are stepped on either by  
 the reset pulse for counter K or by a single pulse generator  $T_E$  (fig. 6). The K counters count up the word  
 50 bits to be handled during each program step, in this case 14 and 20 bits and 1 bit. Where one bit applies  
 which happens whenever OR Gate R14 has an input from the process counter L, the counter K is  
 impeded. The single pulse length process steps are needed for read and erase instructions. If a program  
 step contains 14 bits a data word is transferred; if it contains 20 bits an address instruction is  
 transferred from circuits 9, 10.

The decoded single outputs from the process counters  $L_0$  and L are applied to various gates and  
 55 functional subcircuits as during the consecutive program steps must play a part, all in accordance with  
 the operating mode of the ROM ER 1400 as modified for our purposes. The following events are carried  
 out in the individual program steps:

K-Counters	L-Counters	Mode Control	Operation
(0)	0	—	synchronising pulse, one clock pulse wide as described
(1) — (20)	0	$C_2$ & $C_3$	address data generated in Computer are serially transferred to Fig. 8 via $D_1$ terminal and applied to ADDRESS BITS registers to select memory location. Output O from counter L is applied to OR gate R 8 in Figure 7 enabling mode control lines $C_2$ and $C_3$ . Figure 7 contains most of the mode control logic.
(0)	1	$C_1$	Instruction: Read data of the selected location and enter them into the on-chip data register.
(1) — (14)	1	$C_1$ & $C_3$	data register contents are serially shifted out and transferred to computer circuits figs. 9, 10 and entered into shift register SR1 (fig. 10).
(0)	2	—	In the computer or process controlled, apply the parallel readout bits of the SR1 register and of the SR2 register (containing the intended debit) to the comparator circuit COMP (fig. 10). Lamp GR lights if value in portable data component is larger than value to be debited. If smaller, comparator output is applied to disable line DA and held, clock pulses stop. A display IC (insufficient credit) is lit. As the contents of the shift register SR1 contains also the reference or library bits by which the portable data component reveals which of the currently valid genuity check numbers it holds, the said bits are decoded selecting a register in the computer which holds the corresponding check number in readiness for the genuity check. This procedure is dealt with in more detail in a concurrent patent application.
(1) — (20)	2	$C_2$ & $C_3$	address data are transferred from computer to address register in portable component, for use in step 4.
(1) — (14)	3	$C_1$ & $C_2$ & $C_3$	Transfer the check number selected as described in the computer, to the data register in the PC (portable component) marked 'Subtrahent Register'.
(0)	4	$C_1$	Readout into main data register.
(1) — (14)	4	$C_3$	Recirculate the contents of both the data register and the subtrahent register through the 'Arithmetic Logic' circuit for serial comparison. If these numbers are identical, there will be no bitoutput from the said circuit. If not identical, any bit output sets the bistable F/F (Fig. 8) as well as the bistable 'S' in figure 7. This causes clock pulses to stop in both the computer and the portable component, as applied to the counters. In the computer, after F/F sets, only ones appear at the data. Input $D_1$ , fig. 9. This causes a display (not shown) "Not Acceptable" to be lit.

K-Counters	L-Counters	Mode Control	Operation
(0)	5	$C_2$	Produces short pulse 'e' to obtain erase pulse at the present memory address. Pulse 'e' derives from the OR gate R 14 Fig. 6 which, via TE circuit passes a pulse to the clock input of counter L; The length of the pulse might be controlled by counter K but this is not shown in the present circuit.
(1) - (20)	6	$C_2$ & $C_3$	ENTER new address for new check word.
(0) - (14)	7	$C_2$	ERASE any data at new address location.
(1) - (14)	8	$C_1$ & $C_2$ & $C_3$	ACCEPT new check word data register.
(0)	9	$C_1$ & $C_2$	WRITE word in data register into address location.
(1) - (20)	9	$C_2$ & $C_3$	ENTER address for value word. In computer, after the check reference or library bits in such a manner that after passing through the arithmetic unit will represent the bit combination corresponding to the new check word to be entered. Not shown in Fig. 10. This aspect is dealt with in greater detail in a concurrent application paper.
(1) - (14)	10	$C_3$	Accept debit word from computer and enter into the 'Subtrahent Register'.
(0)	11	$C_1$	READ OUT value number from the selected memory address and enter into Main Data Register.
(1) - (14)	11	$C_1$ & $C_3$	Circulate the contents of both the Subtrahent Register and the Main Data Register through the Arithmetic Logic unit and place the result in Data Register (equals the residual value).
(1) - (14)	12	$C_2$	ERASE memory at the present address.
(1) - (14)	13	$C_1$ & $C_2$	WRITE residual value in data register into the addressed memory location.
(0)	14	$C_1$	READ OUT from said memory location into data register.
(1) - (14)	14	$C_1$ & $C_3$	transfer the said residual value in data register to computer, for verification of correct entry into memory array.
-----			
the following steps do not occur in a vending operation but are required to be added to the afore-listed steps in order to carry out a value increment.			
(1) - (14)	15	$C_1$ & $C_2$ & $C_3$	ACCEPT value word into Main Data Register
(1) - (20)	16	$C_2$	ERASE existing value in the present address.



K-Counters	L-Counters	Mode Control	Operation
(1) - (14)	17	C <sub>1</sub> & C <sub>2</sub>	ENTER the new value into the addressed location from the data register.
(0)	18	C <sub>1</sub>	Read out the newly entered value word and enter into the data register.
(1) - (14)	18	C <sub>1</sub> & C <sub>3</sub>	Shift out serially and transfer to computer for verification of correct entry.

In a value debiting (vending) unit there would be no equipment for carrying out the last five program steps; it would be included in equipment installed at Banks and other authorized places where credit can be increased. The chief obstacle to any fraudulent attempt at inserting a new value (i.e. a higher value) into the data carrier would be the difficulty in deriving the correct check number from the library bits of the data carrier and the correct address for same. This might be possible if the entire update unit were stolen and analysed in a laboratory. It could be arranged, however, that any removal of a unit from its installed place would cause the destruction of the check bit codes. In addition, the check numbers may alter over a period of time as described in a co-pending application.

There are thus set up formidable obstacles to reaching program count 14 in an unauthorized manner; the last five program steps cannot be reached without having first gone through the preceding 14 stages.

The circuit diagrams for the portable data carrier as shown in Fig. 6, 7, 8 provide a fairly complete basis for following through the above listed sequential performance of the data transfer system, with due regard to data sheet for EAROM 1400 chop though in its here modified form.

The following is a description of how the circuits figures 9 and 10 are used:

Prior to the insertion of the PC (portable data component) into the point of sale or control equipment, that is, into the Sensor Unit as exemplified in figures 3 and 4, a control preselection may be performed manually with the aid of value selector switch SEL whereby a number is encoded and put into a register marked "Individual Value". If a series of such individual values are to be added up this may consecutively be done by suitable means, either automatically or manually by pushing an "ADD" button which activates a unit marked "SUM"; as can be seen, this push button receives its voltage over MANL (manual) line from the output of the bistable FF—1 (Figure 9). This ensures that no further debit can be added to the SUM register after the PC is inserted into the Sensor Unit where it actuates a Switch SW (fig. 9). The latter, via Schmitt trigger SCH, sets the bistable FF1 whereby gate N11 is enabled and CK-Oscillator commences to produce clock pulses. These are amplified in 'A', passed through chokes DR which keep out the high frequency component of data signals, and through windings TR<sub>0</sub>. As already explained, these pulses built up a dc voltage in the PC. When the minimum safe operating voltage is reached, the synchronising start pulse is emitted from the PC to the computer unit where it is sensed by phase lock loop circuit P, triggering bistable FF—2, as already described in detail.

It should be noted that the connection line between the register 'SUM' and the shift register SR2 represents parallel data bit connections, equally the output lines from register SR2 to the comparator COMP. P/S is the control input governing serial/parallel modes of the registers SR1 and SR2. The circuit group marked 'SEQUENTIAL PARALELL ENTRY CIRCUITS' indicates the fact that the shift register in the course of the total program is consecutively used for various types of data which have to be sent to the PC and therefore has a parallel entry facility. The bit output lines from the register SR1 comprise those numbered I, II, III, and IV which in this example contain the library code received from the PC for automatic selection of the requisite check number. This is described in greater detail in a co-pending application.

#### 40 CLAIMS

1. A solid state on-person data carrier and associable processing system comprising  
 (a) at least one on-person data carrier containing solid-state logic and memory elements  
 (b) a computer and program control unit  
 (c) a sensor unit conveying data between (a) and (b) wherein both the said data carrier and the sensor unit are furnished with means for being reactively (non-galvanically) coupled when placed in proximity to each other,

the improvement being characterized by the presence within the data carrier of a large scale integrated circuit chip including an electrically eraseable and repeatedly alterable memory circuit capable of responding many times to Erase- and Re-write commands additional to its ROM readout function, and means in the computer portion for applying said command signals via said sensor unit.

2. A data transfer system as in Claim 1, the combination within the data carrier of said EAROM memory circuit with an arithmetic register and subtrahent circuit, and a mode control channel for linking them with the memory input/output system.

3. A data transfer system as in Claim 1, the combination within the data carrier of said EAROM memory circuit with one or more program counters and requisite logic circuitry to follow through a certain sequence of process steps after the computer unit and the data carrier are physically brought into a working relationship via the Sensor Unit.
- 5 4. A data transfer system as in Claim 3 having program counters in both the on-person data carrier 5 and in the computer control unit, with means for synchronising these counters.
5. A data transfer system as in Claim 4, means in the data carrier for producing a synchronising trigger signal in dependence of achieving a built up within the data carrier circuitry of the minimum safe operating voltage.
- 10 6. A solid state on-person data carrier and associable processing system as in claim 1 wherein 10 both the data carrier and the sensor unit contain mutually complementary means for establishing a close electro-magnetic linkage with each other, the improvement characterized by the presence of a solid state IC EAROM chip within the said data carrier and means for loading a portion of said EAROM memory with a first number, furthermore means for accepting and temporarily storing in the chip a 15 second number transferred from the computer unit, means for comparing said first number with said 15 second number, and finally means in the data carrier for sending out to the said computer unit a distinguishing signal by which said unit distinguishes a genuine from a defect or fraudulent data carrier.
7. A data transfer system as in Claim 6 in which the fraud-or defect indicating signal has unchangable, uniform characteristics independent from the structure of said second number, thus not 20 permitting any analytical study for deriving the true check number in the portable data carrier. 20
8. A data transfer system comprising a data carrier, a computer unit and a Sensor unit, mutually complementary reactive coupling means in both, at least one EAROM integrated memory circuit in the data carrier, the system characterized by the provision of means for recognizing the identity of a second 25 data check word when received from the computer unit in the data carrier by reference to a first data 25 word held in the data carrier for producing a logical output level change, and by the presence of Inhibit Gates in the data token circuit which normally inhibit the Erase and Write Mode Control Circuits of the EAROM memory.
9. A data transfer system comprising at least one portable on-person data carrier containing logic memory elements, a computer and program control unit, and a sensor unit, wherein both the said data 30 carrier and the said sensor unit have means for being reactively coupled when placed in proximity to 30 each other, the improvement characterized by the presence in the data carrier and in the sensor unit respectively of *two reactive coupling channels* both of which are employed for the transmission of electrical energy whereas the conveyance of data and control signals is represented by a modulation of one or more characteristics of the energy flow in one, or the other, or in both of said coupling channels.
- 35 10. A data transfer system as in Claim 9 in which the said modulation includes the addition or 35 omission of one or more signal components having a frequency substantially different from that of the energy (clock beat) flow.
11. A data transfer system as in Claim 9 in which said modulation includes frequency shift modulation.
- 40 12. A data transfer system as in Claim 9 in which said modulation includes phase shift 40 modulation.
13. A data transfer system as in Claim 9 in which said modulation includes pulse width modulation.
- 45 14. A data transfer system as in Claim 9 in which said modulation includes delta modulation. 45
15. A data transfer system comprising at least one portable on-person data carrier containing solid 45 state logic and memory elements, a computer and program control unit, and a sensor unit for interfacing the former, wherein both the said data carrier and the said sensor unit are furnished with means for being reactively (non-galvanically) coupled when placed in proximity to each other, the improvement being characterized by a data carrier consisting of a twin back to back shallow disk with flanged rim 50 made of magnetically permeable material the bottom plate of which is common to both, each having a 50 centrally disposed stud of similar material wherein the said rims of the dishes or a part thereof, and the said studs serve as magnetically conductive yokes to, produce reactive coupling means on both sides of the disk.
16. A data transfer system as in claim 15 wherein the hollow spaces in said twin disk are used for 55 placing electronic circuitry and for potting it in an air-tight manner. 55
17. A data transfer system comprising a portable on-person data carrier, a computer, and a sensor unit, the linkage between them being performed by reactive coupling means, wherein the general frame of the data carrier consists of an elongated shallow tray-like disk and wherein the bottom of the trays contains deposited inter-chip circuit connections.
- 60 18. A data transfer system as in claim 15 to 17 wherein the data carrier is enshrouded by a shell 60 made of resilient, formstable material to procure maximum protection against physical and temperature shocks.



---

(12) **UK Patent** (19) **GB** (11) **2 092 353 B**

---

(54) Title of invention

**Adaptable value-token**

(51) INT CL<sup>3</sup>; G07F 7/02

---

(21) Application No  
**8102894**

(22) Date of filing  
**30 Jan 1981**

(43) Application published  
**11 Aug 1982**

(45) Patent published  
**31 May 1984**

---

(52) Domestic classification  
**G4V AL**

(56) Documents cited  
**GBA 2015221**  
**GBA 2011671**  
**GB 1422217**

(58) Field of search  
**G4A**  
**G4H**  
**G4T**  
**G4V**

(73) Proprietors  
**John Wolfgang Halpern,**  
**14 Belsize Park Gardens**  
**London NW3**  
**William Ward,**  
**14 Belsize Park Gardens**  
**London NW3**  
**David Arthur Chalmers,**  
**75 Gordon Road**  
**London N3 1ER**

(72) Inventor  
**David Arthur Chalmers**

(74) Agent and/or  
Address for Service  
**D. Chalmers,**  
**75 Gordon Road**  
**London N3 1ER**

## SPECIFICATION

**Adaptable value-token**

5 Various types of cards or tokens to be used in the place of cash have been described in the technical literature. The most advanced types, for example as described in the patent application 8028824 (UK) or corresponding US Ser. No 184377 can have their effective value periodically increased by the issuing Bank. To avoid fraudulent transactions several security features are designed into such pay token and the associated cash flow system.

10 A major drawback from the user's point of view is that such a pay token can be used only in conjunction with one bank account, or with one specific credit card organisation. Often, pay tokens are only for specific uses such as for making a journey with a bus; or for paying for a phone call.

15 This invention describes a value-token which can be changed to work in several modes and may therefore be applied to manifold uses. Mode control would be either by push touch buttons or similar means provided on the token itself, and/or by encoded instructions signalled to the value-token from an external read/write terminal into which the token is plugged during transactions.

20 *Figure 1* shows an example for the general appearance and features of a typical implementation of the token. (1) is a keyboard which is used to change the mode of operation of the token and also to input data to the token. By way of illustration this are some of the ways the keyboard may be used : pressing B and T selects a program which causes the data corresponding to the cash balance of the owner to be displayed on the liquid crystal display (4). Or, pressing C and N followed by 123 enters the number 123 into one of the internal stores of the token. This means that the owner wishes to withdraw from his bank account £123 and load this amount into the token; this transaction is then rapidly executed at the bank's outdoor terminal. (24) is the edge of the token which is inserted into the terminal.

25 *Figure 2* shows in schematic form one way in which a typical token may be implemented.

30 (1) is a keyboard rather similar in execution as in some hand calculators; Eight signal lines are scanned under control of (2) so that this circuit can electronically recognize which button or combination of buttons has been pressed. (3) is an oscillator which is the basic means for manipulating data through a sequence of instructions. (4) are control circuits which themselves are controlled by the Instruction Register (9); they are constituted by logic circuitry provided to ensure the correct execution of the instructions. (5) is a set of registers containing fixed data, for example the account number of the token owner. Once the data have been entered into these registers during manufacture they can never be changed. (6) is a number of registers containing data that can be changed via the data bus (21) from sources internal and external to the token. (7), (8), (9), (10) and (11) are registers in which data may be memorized. (7) is a store consisting of a number of registers in which fixed programmes are permanent-

ly stored during manufacture of the integrated circuit. (8) is a store consisting of a number of registers in which externally changable programmes are stored. (9) is a register which receives the keyed-in instruction to set the token for a specific performance. (10) is a register which at any time contains the data scheduled for display or requested for display on the Liquid Crystal panel (14).

70 (11) is a register which contains information as to the exact state at any time of the internal condition of the token circuitry so that external equipment can be informed via the input/output port (15,16,17) of this state. (12) is a register which temporarily stores in coded form which programme is being carried out. (13) is a set of binary logic circuits which decodes the data in (10) so that it can be used to control the LCD panel (14). The block 15 signifies a set of logic circuits which, working under the control of the control circuits (4) and the oscillator (3) change data from binary parallel form into a sequence of pulses or vice versa. Block (16) represents a circuit which carrier out one of two alternative functions. In one form the pulses to be outputted are power amplified and used to drive the inductive transmitter/receiver (17); in the second form pulses picked up by the inductive receiver (17) are amplified and shaped so that they are suitable to operate with the rest of the circuitry. (2) is a second inductive component which is used to pick up from the terminal into which a token is plugged, radiated power which is used to charge the token's encapsulated battery (19). This power input may also be used to inhibit the keyboard (1) and to enable input data via the inductive component (17). (22) is a data Bus along which data are transferred between the various sections of the circuitry of the token. (23) is an address Bus which is used, by means of binary signals, to control the destination of the data on (22).

80 All the circuits enumerated are well known in the art and therefore it is only the particular combination and manner of use which is the claimed unique factor of the invention.

85 A program is a set of instructions; when these are carried out in sequence a program is being implemented. In addition to such programmes brought into action via the said token keyboard, instructions may be introduced, one by one, in an ordered sequence via the external token terminal which would be designed to bring into operation one or the other of the internally stored programmes. In this mode of operation, the external circuitry after inputting to the token an instruction, awaits a signal from the token indicating that the instruction has been carried out and then, and only then inputs the next instruction and so on until all the instructions have been implemented.

## CLAIMS

125 1. An adaptable value-token containing a large scale integrated circuit having a multiplicity of fixed and changable data- and program stores, input/output circuits, and means for transferring data bidirectionally from/to the token to/from an external data base, characterized by the provision of a

multi-function keyboard on the surface of the token for selecting one of at least two different operating modes of the token circuit.

2. An adaptable value-token containing a large  
5 scale integrated circuit having a multiplicity of fixed and changable data-and program stores as in Claim 1 wherein the token has further means for receiving from an external data base to which it may be coupled encoded instructions, means for decoding  
10 these instructions and for making them select one of at least two different operating modes of the token circuit so as to adapt the token to the general requirements of the data system to which it is coupled.
3. An adaptable value-token containing a large  
15 scale integrated circuit having a multiplicity of fixed and changable data-and program stores as in Claim 1, wherein the coupling means consist of coils loaded by ferric cores.
4. An adaptable value-token as in claims 1 to 3  
20 wherein the data token has a display window for displaying desired data in humanly readable digits.
5. An adaptable value-token exhibiting the features as described in the specification and illustrated  
25 in the drawings.

The text of the specification has been reproduced by photocopying. The original typescript may be inspected on the premises of the Patent Office

- (21) Application No **8228365**  
(22) Date of filing **5 Oct 1982**  
(30) Priority data  
(31) **8130276**  
**371140**  
(32) **7 Oct 1981**  
**23 Apr 1982**  
(33) **United Kingdom (GB)**  
**United States of America**  
**(US)**  
(43) Application published  
**27 Apr 1983**  
(51) **INT CL<sup>3</sup>**  
**G07F 7/10**  
(52) Domestic classification  
**G4V AL**  
(56) Documents cited  
**WO 8103562**  
**EP 0041261**  
**GB 1556328**  
**GB 1166085**  
(58) Field of search  
**G4V**  
**G4T**  
(71) Applicant  
**Hecon Corporation,**  
**(USA - New Jersey),**  
**31-45 Park Road,**  
**Tinton Falls,**  
**New Jersey 07724,**  
**United States of America**  
(72) Inventor  
**Marvin Bernstein**  
(74) Agents  
**Matthews Haddan and**  
**Co,**  
**Haddan House,**  
**33 Elmfield Rd.,**  
**Bromley,**  
**Kent BR1 1SU**

(54) **Programmed electronic  
keycoder unit**

(57) A miniaturized card unit, resembling a standard credit card, incorporates solid state counter, which may be incremented or decremented in accordance with a direction control signal. Control signals transfer the count stored in the card unit to a display for visually displaying the decimal count stored in the card. A logical circuit monitors selected segments of the display to enable operation of the device controlled by the card reader unit so long as a card is inserted and the card inserted contains a non-zero count. Signals representative of the device usage are applied to the card unit counter for decrementing the count.

A new count is introduced into the card unit by insertion into a card programmer unit having settable thumbwheel switches for setting a down counter. The presence of a card unit and the closure of a program switch causes simultaneous incrementing of the card unit counter and decrementing of the card program counter.

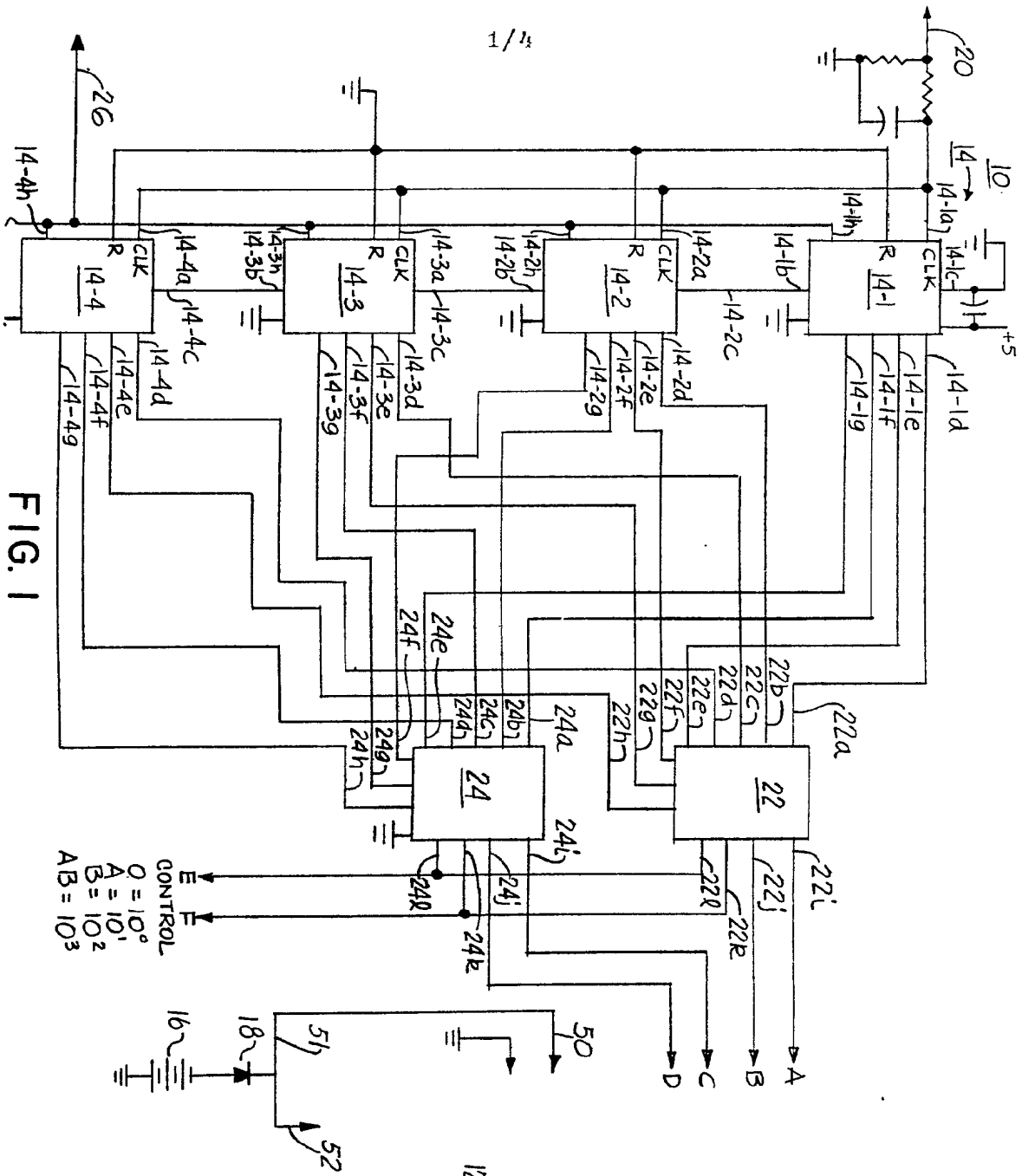


FIG. 1

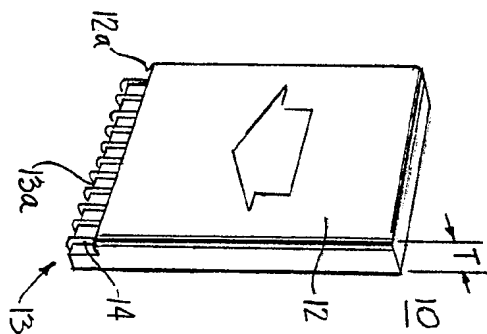


FIG. 1a

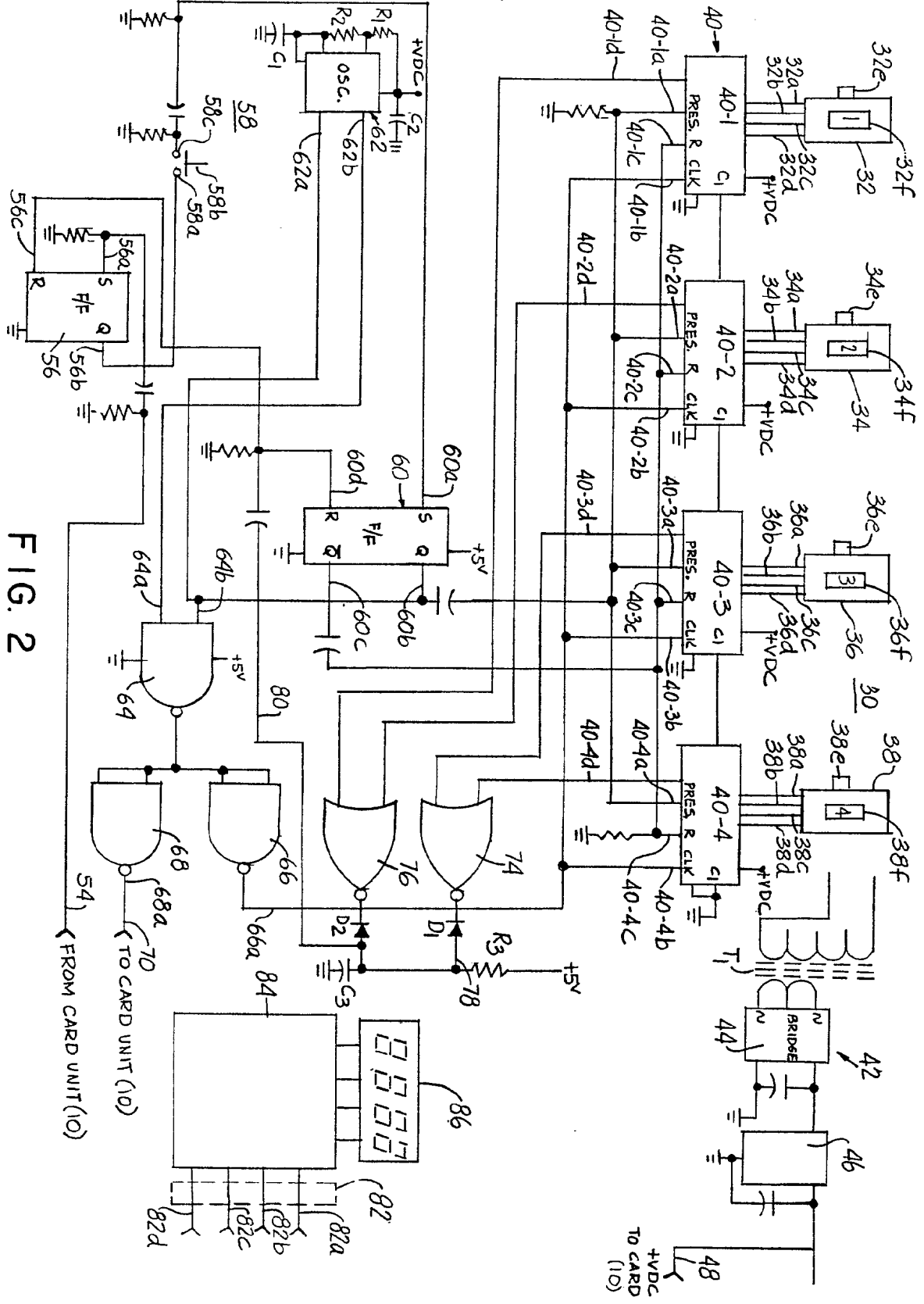


FIG. 2



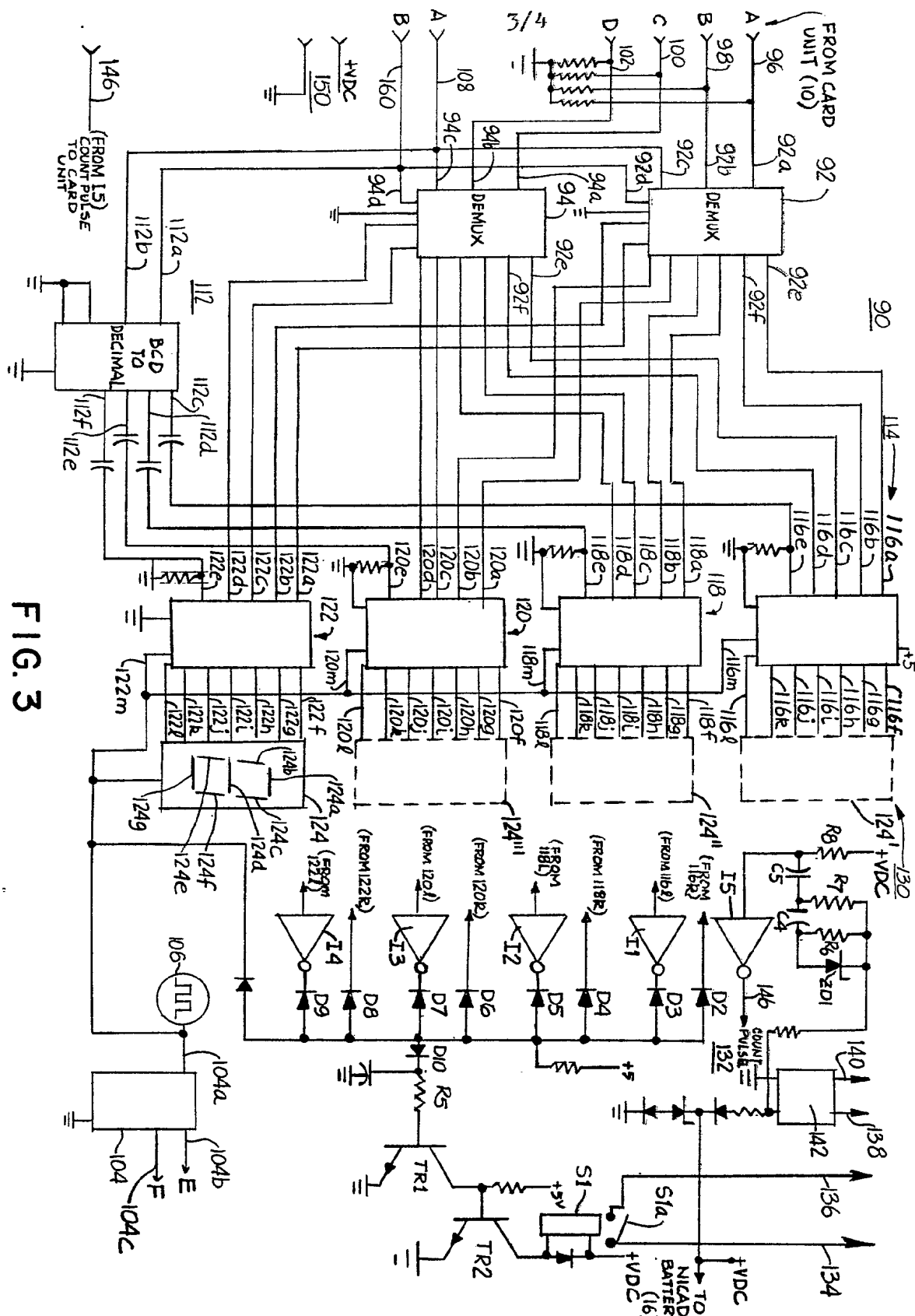


FIG. 3

1/4

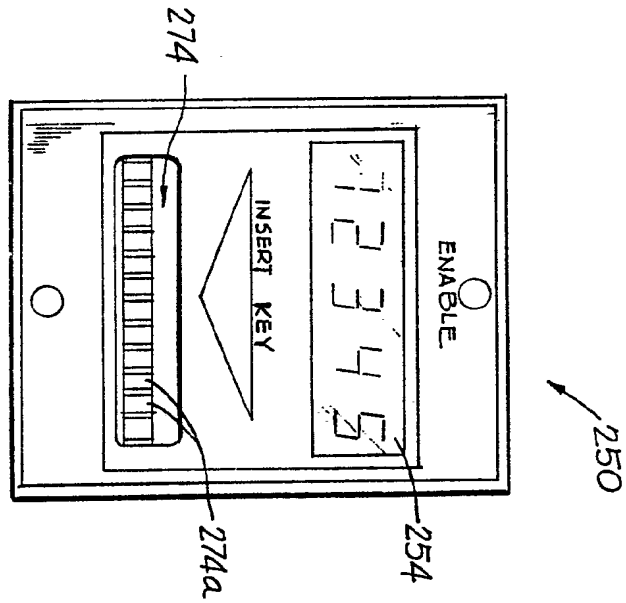


FIG. 4a

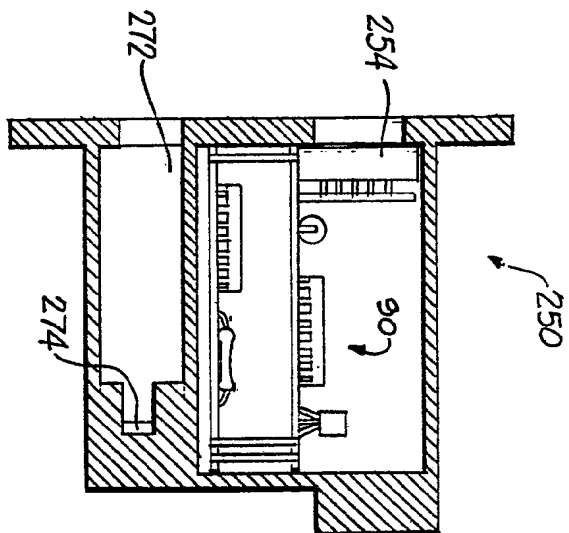


FIG. 4b

## SPECIFICATION

**Programmed electronic keycorder unit**

5 The present invention relates to control devices and, more particularly, to a control device for limiting access to a machine or other equipment or device to authorized personnel possessing a card unit which further contains stored data controlling the extent of access to the machine permitted to the holder of the card unit.

10 A number of applications exist wherein it is desirable to limit access to machines to only those persons having proper authorization and further to limit the extent of such access. As one example, it is sometimes desirable to limit the use of copier machines to selected personnel. The copier machine is often provided with a substantially tamper proof counter for maintaining a cumulative count of the number of copies which have been produced to date. One standard technique for authorizing use of the copier machine is to provide selected personnel with a conventional key arranged to release a cooperating mechanical lock which, when opened, may be arranged to provide for the completion of an electrical circuit to provide power to the machine. Since keys of this type may be simply, readily and inexpensively reproduced, one standard prior art approach to avoid simple reproduction of keys is described in U.S. Patent No. 3,436,530, issued April 1, 1969 and assigned to the assignee of the present application, and which discloses a control unit forming a part of the copier machine and arranged to releaseably receive a portable plug-in unit containing an electromechanical counter and an electrical or electronic circuit element or elements which, when the portable unit is plugged into the control unit, serve to operate a relay which couples the machine to a local power source. The control unit is also preferably provided with an electromechanical counter.

15 The machine or device whose access is being controlled generates pulses representative of machine usage. In the copier machine example, each pulse preferably represents the reproduction of a single copy. Each pulse is simultaneously applied to the electromagnetic counters of the portable, plug-in unit and the control unit. Ideally, the counter of the control unit should contain a count equal to the grand total of the individual counts in each of the portable plug-in units used in conjunction with that copier machine.

20 The above mentioned accountability system, although reasonably satisfactory for cost allocation purposes, fails to provide any means for limiting the extent of access which any authorized holder of a portable, plug-in unit.

25 This limitation led to the development of the system described in U.S. Patent No. 3,921,875, issued November 25, 1975 to the assignee of the present application. The apparatus described in the last mentioned patent also comprises a control unit forming part of the machine and a portable, plug-in unit. The portable unit contains an electromechanical counter which may be preset to any desired count

30 from 0 to a count of up to 99999, for example. The portable unit is also provided with an electrical circuit for operating a relay to couple the machine whose usage is being regulated to a local power source. Pulses generated by the machine and representative of machine usage are applied to the electromagnetic counter of the control unit and to the electromagnetic counter of the portable unit to respectively increment the control unit counter and decrement the portable unit counter. When the count in the portable unit counter has been decremented to a predetermined value (preferably 0) a switch is opened to deenergize the aforementioned relay and thereby decouple the machine from its source of power.

35 The count in the electromechanical counter of the plug-in unit may be reset by opening the plug-in unit through the use of a mechanical key. Alternatively, the count may be advanced through the use of a pulsing device which applies the number of pulses to the electromechanical counter equal to the desired count to be stored therein. This is a sluggish and tedious operation due to the electromechanical nature of the counter which is further subject to wearing over a period of continuous use. The portable plug-in units and control unit are also unnecessarily large and subject to wearing and breakdown due to the large number of mechanical moving parts utilized in these units.

40 In addition to the above disadvantages, the portable unit housing may be broken into rather easily and the electromagnetic counter mechanism may easily be tampered with to create a non-zero count condition, thereby destroying system security. The electromechanical nature of the device also lends itself readily to evaluation of the contents to further aid unauthorized personnel in their quest to defeat the security measures and thereby permit unauthorized use of the machine or device being protected against unauthorized use.

45 The present invention avoids all of the disadvantages of prior art systems and is characterized by comprising three basic subassemblies, each utilizing solid state circuits to totally avoid the disadvantages of large size and weight and wearing of components normally encountered in the prior art devices, such as those described, for example, in the above mentioned U.S. patents, and which present invention yields additional advantageous features as will be more fully described.

50 The three basic units employed in the solid state system of the present invention are a card unit, card reader unit and card programmer unit. The card unit is comprised of miniaturized solid state circuitry including an up/down counter, a multiplexer and a battery, all of which are arranged within a housing whose overall dimensions are of the order of a conventional credit card.

55 The card programming unit is substantially comprised of all solid state components including a display and driver circuit. When a card unit is inserted into the card programmer unit, a control circuit sequentially transfers the count in the card unit counter through the card unit multiplexer and the card programmer unit demultiplexer to a driver

circuit for displaying the contents of the card unit counter.

The count desired to be added to the card unit is set into manually settable switches.

- 5 Depression of a program start button in the presence of a card unit sets the count of the settable switches into the card programmer unit counter and enables a normally disabled clock in the card programmer unit counter. Pulses from the local oscillator increment the count of the card unit counter and simultaneously decrement the count of the card programmer counter. Logical gates, which continuously monitor the card programmer counter, deactivate the local oscillator and simultaneously
- 10 disable a previously enabled gate preventing spurious oscillator pulses from reaching the card unit counter. The card programmer display displays the count in the card unit counter to provide positive confirmation that the correct count has been added
- 15 to the card unit, as well as displaying the count in the card unit prior to and during insertion of the desired count.

A card reader unit, which is interconnected with the machine whose use and extent of use is to be controlled, is provided with solid state decoder drivers for driving a visual display.

A control unit controls the card unit multiplexer in synchronism with a card reader unit solid state demultiplexer for sequentially transferring the count in the card unit counter to the decoder driver circuit.

The card reader unit further incorporates a local oscillator which operates the control unit for operating the multiplexer and demultiplexer circuits in synchronism and provides time division pulses to the visual display.

The display driver circuits convert the data transferred thereto from the card unit counter into signals appropriate for illuminating the display device which is preferably of the seven segment LCD (liquid crystal display) type. Selected ones of the signals of each decimal digit position of the display are coupled with logical gating circuitry which operates to energize a relay for providing a machine enabling signal and for deenergizing a relay to disable the machine when the count in the card unit counter is decremented to zero by pulses derived from the machine, which zero count is also displayed by the card reader unit display.

Pulses representative of machine usage are applied to the card unit counter through the card reader unit to decrement the contents of the card reader unit counter upon the occurrence of each count pulse.

The simplified, miniaturized, solid state design eliminates the need for a card reader unit display and its attendant cost and weight, reducing the card reader unit, for example to a weight of no greater than one ounce, as compared with key counter units which, in addition to being relatively large and bulky, are more than five times the weight of the card unit.

The solid-state multiplexer and demultiplexer units significantly reduce the electrical connections required between the card programmer unit and the card unit and between the card reader unit and the card unit. The small battery employed in the card

unit is capable of a significantly long, useful operating life due to the elimination of a display in the card unit and the provision of single, visual display means in only the card reader and card programming units, yielding a significant reduction in cost and which is a direct function of the number of card units employed within a single system. As an alternative arrangement, the card unit may employ a rechargeable battery which is designed to be recharged either during the time that the card unit is being programmed to receive a new count or at the time the card unit is inserted into a card reader unit.

The system enhances centralized control or, alternatively, provides a prepayment capability.

The system employs extremely low power solid state integrated circuits as well as display devices which consume almost no power since they operate with low conductivity electro-statics and thereby consume significantly less power than prior art devices presently in use.

The circuit connections required to be made to the card reader unit serve as additional security means since specific knowledge of the machine construction would be required to have any reasonable chance of making the required connections.

It is therefore one object of the present invention to provide a novel, highly simplified solid state control system for controlling access to a machine and the extent of such access by means of a preprogrammed card unit having a solid state counter selectively engageable with a card reader unit for displaying the present count in the card reader unit, for decrementing the count responsive to machine usage and for locking the machine against further usage when the count in the card unit reaches a predetermined count.

Another object of the present invention is to provide a control system of the type described in which solid state programming means is provided for simply, rapidly and accurately entering a preprogrammed count into the solid state counter of a card unit and including display means for displaying the contents of the card unit counter to confirm entry of the preprogrammed count.

Still another object of the present invention is to provide a control system of the type described in which system security is obtained through the provision of a card identity code which is examined by a key acceptor unit for validity in order to enable the device being controlled.

The above, as well as other objects of the present invention, will become apparent when reading the accompanying description and drawing in which:

Fig. 1 is a schematic diagram of a card reader unit embodying the principals of the present invention.

Fig. 1a shows a perspective view of the card unit exterior.

Fig. 2 is a schematic diagram showing the solid state card programmer employed for introducing a preprogrammed count into a card unit of the type shown in Fig. 1.

Fig. 3 is a schematic diagram of a card reader unit arranged for selective insertion of a card unit of the type shown in Fig. 1 for controlling the access and extent of access of a machine coupled thereto.

Fig. 4a shows a front view of the card reader unit.  
Fig. 4b shows a sectional view of the card unit of Fig. 4a and an end view of the card unit of Fig. 1a.

One preferred embodiment of the card unit 10 of the present invention is shown in Figs. 1 and 1a, Fig. 1a showing the outward physical appearance thereof, wherein it can be seen that the card unit 10 comprises a thin, rectangular shaped body 12, preferably formed of plastic, and containing solid state circuits (to be more fully described) embedded therein. The body 12 generally resembles a conventional credit card but has a slightly greater thickness T. One end 12a, of a reduced thickness portion is provided with an edge connector assembly 13 for insertion into an edge connector socket to be more fully described, said socket 13 including individual end terminals 13a.

The card unit 10 comprises a solid state counter 14 of the binary coded decimal type which, in the preferred embodiment of Fig. 1 is further comprised of four CMOS type 4510 integrated circuits or stages 14-1 through 14-4 electrically connected to form an up/down counter 14, each stage capable of storing a decimal number. A battery 16 powers the counter 14. Battery 16 is shown schematically but may, for example, be comprised of a pair of 1.5 volt watch batteries of the type 393BP, and being connected in series. Diode 18 serves as a blocking circuit device to prevent charging of battery 16 by external connections.

Each counter stage 14-1 through 14-4 has its clock input 14-1a through 14-4a connected in common to a count input terminal 20. The carry outputs 14-1b through 14-3b of stages 14-1 through 14-3 are electrically connected to the carry inputs 14-2c through 14-4c of counter stages 14-2 through 14-4.

The binary coded decimal output terminals 14-1d through 14-1g and 14-4d through 14-4g are selectively connected to respective inputs 22a through 22h and 24a through 24h of solid state multiplex circuits 22 and 24 which are preferably type 4052 integrated circuits which multiplex (i.e. sequentially transfer) the digital data stored in counter 14 to the output terminals 22i and 22j of circuit 22 and 24i and 24j of circuit 24. The multiplexed data output terminals being labelled A, B, C and D respectively. Input lines labelled E and F are adapted to apply binary type control signals derived from an external source 30 or 90 to the control terminals 22k and 22l of circuit 22 and 24k and 24l of circuit 24 to control the multiplexing and demultiplexing operation as will be more fully described.

Control inputs 14-1h through 14-4h of the counter stages comprising counter 14 are connected in common to a terminal 26 arranged to be electrically connected with either the card reader unit or the card programmer unit and to receive a binary level signal from the card reader unit causing the counter to be decremented when count pulses are applied to terminal 20 and alternatively arranged to receive an opposite level binary signal causing counter 14 to be incremented when count pulses are applied to input 20 by the card programming unit 30, which operations will be more fully described hereinbelow.

The embodiment of the card unit 10 shown in Fig.

1 is thus capable of storing any count from 0000 through 9999. Obviously, the count capacity may be increased by adding one or more additional counter stages, if desired.

The card programmer unit 30, as shown in Fig. 2, functions to generate an exact number of pulses equal to the count desired to be added to a card unit 10 inserted into the card programmer unit 30.

This is accomplished by means of thumbwheel switches 32 through 38 each having their binary coded outputs electrically connected to associated inputs of a counter 40 (comprised of solid state counter stages 40-1 through 40-4) which are preferably type 4510 counter stages arranged to operate as a decrementing counter.

A local power supply 42 provided in card programmer unit 30 converts a 115 VAC source through transformer T1 and full-wave bridge 44 to a DC signal. A type 7805 circuit 46 provides a stabilized +5 VDC output which is coupled through terminal 48 forming part of a card programmer unit receptacle to terminal 50 forming part of the edge connector 12a of card unit 10 (shown in Fig. 1). Terminal 52 of card unit 10 is, in turn, coupled to terminal 54 of card programmer unit 30, shown in Fig. 2. Thus, when a card unit 10 is inserted into the connector forming part of the card programmer unit 30, an electrical circuit is completed from the +5V terminal 48 to terminal 50 of the card unit 10 and back to the card programmer unit 30 through lead 51 and terminal 54, which voltage is applied to the set input 56a of bistable flip-flop 56, causing its Q output 56b to go high. This voltage appears at terminal 58a of programming switch 58 and, when switch button 58b is pressed, completes an electrical circuit to stationary terminal 58c to apply a high signal to the set input 60a of bistable flip-flop 60 causing its Q output 60b to go high and causing its Q output 60c to go low.

The Q output of bistable flip-flop 60 is simultaneously applied to each preset input 40-1a through 40-4a of the counter stages of counter 40 causing the binary values, established by the settings of thumbwheel switches 32-38, to be preset into a respective one of the counter stages 40-1 through 40-4. Thumbwheel switches 32 through 38 are of a conventional type in which, by operation of a control knob such as control knob 32e, any number from decimal "zero" through decimal "nine" may be set within window 32f thereby providing a four bit binary output which is coupled to the input of the associated counter stage.

The Q output of bistable flip-flop 60 is further simultaneously applied to the reset terminal 62a of a type 555 timer which, by appropriate selection of the resistance values of resistors R1 and R2, and the capacitance values of capacitors C1 and C2, is operated as an oscillator which, in the present application, generates pulses at a rate of the order of 2kHz at its output terminal 62b. The output of oscillator 62 is coupled to input 64a of NAND gate 64 whose input 64b is also coupled to the Q output 60b of bistable flip-flop 60. The Q output of flip-flop 60 removes the reset level from inputs 40-1c through 40-4c of counter 40 enabling counter 40 to be preset.

The Q output of bistable flip-flop 60 also enables

NAND gate 64 to pass clock pulses from clock source 62. These pulses are simultaneously gated through NAND gates 66 and 68 which are wired to operate as inverters. Output 66a of NAND gate 66 is coupled in common to the clock inputs 40-1b through 40-4b of the counter stages of counter 40, which counter is operated as a decrementing counter whose count is reduced from the setting preset into the counter 40 by thumbwheel switches 32 through 38, toward a zero count.

Output 68a of NAND gate 68 is coupled through terminal 70 of card programmer unit 30 to terminal 20 of card unit 10 shown in Fig. 1 causing the count in counter 14 to be incremented simultaneously with the decrementing of the count in counter 40.

Assuming that the counter 40 of card programmer unit 30 has been preset to introduce a decimal count of 1000 into the card unit counter 14, after clock source 62 has applied 1000 pulses to card unit counter 14 and to card programmer unit counter 40, all four counter stages 40-1 through 40-4 will have been decremented to zero. A pair of eight-input NOR gates 74 and 76 have respective ones of their inputs electrically connected to respective ones of the binary coded outputs of counter stages 40-1 through 40-4. Gate 74 has its eight inputs respectively coupled to four outputs of stage 40-4 and stage 40-3, while gate 76 has its eight inputs respectively coupled to the four binary coded outputs of stages 40-2 and 40-1, respectively.

Diodes D1 and D2 electrically connect the outputs of gates 74 and 76 to common terminal 78 arranged between resistor R3 and capacitor C3.

When all sixteen outputs of counter stages 40-1 through 40-4 are low, representing the decimal number 0000, the outputs of both gates 74 and 76 go high raising common terminals 78 to the +5V level, which level is simultaneously applied through conductor 80 to reset inputs 56c and 60d of bistable flip-flops 56 and 60, respectively. The Q output of bistable flip-flop 60 simultaneously disables gate 60 and terminates the operation of clock source 62 preventing any noise from inadvertently pulsing the card unit counter 14 and thereby adding a false count to the card unit. The Q output of flip-flop 60 goes high preventing counter 40 from being accidentally preset. The resetting of bistable flip-flop 56 causes its Q output to go low preventing the programming operation from being repeated in the event that program button 58 is accidentally operated before the card unit 10 which has just had a preprogrammed count added to it, has been removed from the card unit receptacle forming part of card programmer unit 30.

The card programmer unit 30 is further provided with a solid state demultiplexer and control circuit 82, a display driver circuit 84 and a four digit display 86 which are substantially identical to like circuits provided within card reader unit 90 (to be more fully described hereinbelow). The inputs 82a through 82d of demultiplexer 82 receive the A through D outputs of multiplexers 22 and 24 provided in card unit 10. The demultiplexer and control circuitry 82 transfers the binary coded count stored in the stages of card unit counter 14 through multiplexer circuits 22 and

24 and demultiplexer 82 to the display driver circuitry 84 for illuminating display 86, which is preferably provided with four decimal display units, each being of the seven segment decimal type. A detailed description of the transfer of data from the card unit counter 14 to the card reader unit visual display 86 will be set forth in detail hereinbelow, it being understood that the operation of the same circuitry within the card programmer unit 30 is substantially identical to that provided in card reader unit 90.

Card programmer unit 30 thus makes it possible to enter an exact preprogrammed count into the card unit counter 14 in a simple, rapid manner, the entire operation taking, at most, a few seconds including set up, insertion and removal of the card unit 10. The display 86 provided within the card programmer unit 30 provides direct visual confirmation that the preprogrammed number has been correctly introduced into the card unit 10. The display 86 also serves as a means to ascertain the count within the card unit 10 before initiating a programming operation and further enables a preprogrammed count to be added to a card unit counter 14 which has other than a zero count when first introduced into the card programming unit 30.

The card reader unit 90, shown in detail in Fig. 3, performs the functions of: displaying the four digit decimal number contained within the memory of the card unit 10 inserted into the card reader unit receptacle and enabling the machine being controlled by the card reader unit 90 when the count in the card unit 10 is other than zero. However, when the count in the card unit 10 reaches zero, the card reader unit 90 causes the machine to be made inoperative.

Card reader unit 90 recovers the count in card reader unit 10 by demultiplexing the binary coded information on the four lines labelled A through D which are respectively coupled to solid state demultiplexer circuits 92 and 94 which are preferably type 4052 integrated circuits. Input terminals 96 and 98, receiving data bits A and B, are coupled to inputs 92a and 92b of demultiplexer circuit 92 while terminals 101, 102 couple data bits C and D to inputs 94a and 94b of demultiplexer circuit 94.

Control signals for controlling the transfer of the count from card unit 10 to the card reader unit 90 are derived from solid state circuit 104 which is preferably a type 4029 circuit having a clock input 104a coupled to the output of a 100Hz oscillator 106 for developing binary coded decimal control signals E and F at the outputs 104b and 104c, respectively.

The E and F signals are applied: through terminals 108 and 110 to the control inputs 22k, 22l and 24k, 24l of multiplexer circuits 22 and 24 in card unit 10 (shown in Fig. 1); and are simultaneously applied to the control inputs 92c, 92d and 94c, 94d of demultiplexer circuits 92 and 94; and to the inputs 112a and 112b of a binary coded decimal to decimal decoder circuit 112 which is preferably a type 4028 solid state circuit arranged to convert a two bit binary coded input into a radix four ("one of four") output.

Each of the multiplexers 22 and 24 of card unit 10 has four pairs of input terminals for a total of eight input terminals 22a through 22h and 24a through

24h. The binary coded multiplexer control signals E and F are simultaneously applied to the aforementioned control inputs of multiplexers 22 and 24 to cause only one pair of the four pair of input signals to appear at output terminals 22i, 22j and 24i, 24j of the multiplexer units 22 and 24, in accordance with the binary code applied to the control inputs 22k, 22l and 24k, 24l. For example, when control signals EF develop a binary code 0,0, the binary levels at outputs 22i and 22j are respectively coupled to inputs 22a and 22b, while the binary levels at outputs 24i and 24j are respectively coupled to inputs 24a and 24b causing the four binary bits representing the least significant decimal position, stored in counter stage 14-1, to appear at data output terminals A through D respectively.

Simultaneously therewith, control signals E and F control the demultiplexer circuits 92 and 94 so that the input signals appearing at 92a, 92b are transferred to outputs 92e and 92f and so that the inputs 94a and 94b are transferred to outputs 94e and 94f. These output pairs 92e-92f and 94e-94f are respectively coupled to inputs 116a through 116d of latched decoder driver circuit 116 forming part of the driver array 114 which further includes latched decoder driver circuits 118, 120 and 122. Solid state circuits 116 through 122 are preferably type 4056 circuits capable of converting a binary coded decimal input into a group of signals which selectively appear on output lines 116f through 116l for driving a seven-segment decimal display unit such as, for example, unit 124 coupled to the aforementioned seven output lines of the driver circuit, such as for example driver circuit 122, in order to selectively illuminate two or more of the display segments 124a through 124g which collectively cooperate to form the decimal digits "0" through "9".

The four binary signals representing the least significant decimal digits are loaded into driver circuit 116 by decoder 112 which decodes the two binary control signals E, F applied to inputs 112a, 112b to cause one of its four output lines 112c through 112f to develop a strobe signal, to the exclusion of the remaining three output lines. In the present instance, decoder 112 decodes the control signals E and F causing its output line 112 to develop a strobe pulse for latching the four binary bits representing the least significant decimal digit into latched decoder driver circuit 116. Circuit 116 decodes the four binary inputs and develops signal levels at the outputs 116f through 116l representative of the decimal digit to be displayed, which signals are applied to the display unit, such as unit 124 to display the appropriate decimal digit.

The outputs of control signal generating circuit 104 change at a rate controlled by oscillator 106 causing the next significant decimal digit to be transferred through multiplexer circuits 22 and 24 of card unit 10 to the demultiplexer circuits 92 and 94 of card reader unit 90 thereby causing the binary coded signals representing the next significant decimal digit to appear at outputs 92g and 92h of demultiplexer 92 and 94g and 94h of demultiplexer 94, which signals are applied to respective inputs 118 through 118d of driver circuit 118. The control

signals E and F are also applied to decoder 112 causing a strobe signal to be developed at output 112d to transfer and latch the next significant decimal digit into driver circuit 118 for display by its associated display unit (not shown for purposes of simplicity). This operation is continued until all four decimal digits are transferred to the associated driver circuits 116 through 122 and displayed by their associated display units, which are preferably of the liquid crystal display (LCD) type. The data transfer operation is also continuously repeated at the 100Hz rate.

Clock pulses from source 106 are further simultaneously applied to the control inputs 116m through 122m of driver circuits 116 through 122 and to the input 124a of the display unit 124 for generating the liquid crystal display square wave signal which causes the display unit 24 to operate in an intermittent fashion as is conventional with such units, the pulsing of the display units in array 130 by clock source 106 being at a rate sufficiently rapid to cause the eye of the observer to perceive a "steadily illuminated" decimal digit. The remaining display units function in an identical fashion.

The transfer of the count in card reader unit 10 to the driver circuit array 114 is continuously updated since the count in the card reader unit 10 is being decremented at a rate determined by machine usage. Assuming that the machine controlled by card reader unit 90 is a copier machine, the copier machine is enabled in the following fashion:

The card unit 10 is inserted into the receptacle of the card reader unit 90 which automatically initiates transfer of the count in card unit 10 to the driver circuit array 114. In addition to the count being displayed by the display array 130, logical gating circuitry 132 continuously monitors the driver array 114 to detect for the presence of a zero count condition. A unique condition exists for digit zero since the segment of the display whose illumination is controlled by output 116k will have a voltage on it and the segment whose illumination is controlled by output 116l will have no voltage on it. Outputs 116k, 118k, 120k and 122k are directly connected to diodes D2, D4, D6 and D8 whereas outputs 116l, 118l, 120l and 122l are connected to diodes D3, D5, D7 and D9 by inverter circuits I1 through I4 respectively. Thus, when all digits displayed are decimal zero, a forward base drive is applied to the base electrode of transistor TR1 causing its collector to go to ground and removing base drive from the base electrode of transistor TR2 thereby deenergizing relay S1. Relay contact S1a is then opened thereby developing an open electrical circuit between terminals 134 and 136 which may, for example, be utilized to decouple the machine from its local power source or to provide any other desired disabling function sufficient to prevent further use of the machine when the count in the card unit inserted into the card reader unit has been decremented to zero. The fact that the card reader unit contains a zero count is confirmed by the display array 130.

The copier machine, as is conventional, develops pulses which are applied to pulse inputs 138 and 140 coupled through a full-wave diode bridge 142 to a

signal stabilizing circuit 144 comprises of resistors R6 through R8, zener diode ZD1 and capacitors C4 and C5, the output of the signal stabilizing circuit being coupled to count pulse output terminal 146 through inverter 15. Terminal 146 is coupled to terminal 20 of card reader unit 10 when the card unit 10 is inserted into the receptacle of the card reader unit 90. Terminal 150 applies a ground level to the terminal 26 of card unit 10 causing counter 14 to operate as a down counter whereby pulses representative of machine use applied to card unit 10 to cause the count in counter 14 to be decremented.

Although the application set forth hereinabove describes the system of the present invention for use with a copier machine, it should be understood that the system is readily adaptable for use with other machines and/or devices. For example, the system of the present invention may be utilized for dispensing items and materials such as, for example, fuel oil, wherein a fuel tank dispenser is enabled and signals are developed representative of the amount of fluid dispensed to reduce the count in the card unit counter 14. The dispenser may also be a vending machine of the automatic type, wherein the vending machine is provided with processing means for comparing the cost of the selection with the present contents of the card unit wherein the item is dispensed only when the counter contents equals or exceeds the cost of the selected unit. The system may also be employed with point of sale equipment wherein the operator at a register enters the cost of the item selected for purchase and the register is enabled only if the count in the card unit is at least equal to the cost of the selected item, in which case the register creates a record and receipt of the sale and substantially simultaneously therewith reduces the count in the counter unit by an amount equal to the magnitude of the sale. An automatic vending machine may also be operated to vend an item upon receipt of a card unit containing a sufficient count.

For purposes of the present invention, it is sufficient to understand that the control unit serves as the interface for coupling the count in the card unit 10 to display means and possibly to other means for determining the presence of a valid card unit, for example, and for providing an enabling signal when the card reader unit 90 receives a card unit 10 of the proper electrical configuration and containing a non-zero count, these capabilities being designed in a sufficiently universal fashion for use with a wide variety of different machines and/or devices.

The internal wiring arrangement of the card unit 10 relative to its edge connector may be designed so that precise knowledge of the circuit contents of the card unit would be required in order to enable either a card programming unit 30 or a card reader unit 90 thereby providing still further security for the system, in addition to controlling the access to the machine and the extent of said access as a function of the count within the card unit.

The front of acceptor unit 250 is shown in Fig. 4a while Fig. 4b shows a sectional view of its internal physical arrangement. The acceptor unit 250 is provided with an opening 272 for receiving the key unit 200 whose physical arrangement is shown in

Fig. 1a. The rear end of opening 272 is provided with receptacle means 274 in the form of a multi-terminal electrical socket assembly having individual terminals 274a arranged to electrically engage respective ones of the terminals 13a integrally formed within the edge connector assembly 13 of key unit 10.

When key unit 10 is inserted into slot 272 so that its edge connector assembly 13 is properly inserted within multi-terminal socket 274, an electrical circuit is established from the acceptor unit terminals 150 (Fig. 3) to a key unit terminal 51 (Fig. 1) for activating the key unit 10.

In a similar fashion, the outputs of multiplexers 24, 26 of key unit 10 (Fig. 1) each electrically connect with a respective one of the inputs of demultiplexers 92, 94 connected to the multi-socket 274 arranged at the rear of key slot 272.

Although the preferred embodiment described herein is designed to increment the count in a card unit 10 when a count is to be added and to decrement the count when the count is to be removed, the reverse arrangement is also possible. For example, the count in the card unit counter 90 may be exhausted when the count reaches the equivalent of decimal 9999, a count of less than decimal 9999 representing an unexhausted incard unit 10. In such an example, the card unit 10 would be decremented from 9999 to a smaller number under control of the card programming unit and would be incremented from the lower decimal number toward the decimal count 9999, at which time the machine being controlled would then be turned off. By rearranging the wiring of the driver circuits of array 114 the signals may be decoded so that a decimal count of 9999 would be displayed as a decimal count of 0000 thereby adding still further security to the system and rendering a defeat of the system more difficult to unauthorized users who also lack knowledge of the system design.

A latitude of modification, change and substitution is intended in the foregoing disclosure, and in some instances, some features of the invention will be employed without a corresponding use of other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the spirit and scope of the invention herein.

#### CLAIMS

1. Control means for preventing unauthorized use of a device and for controlling the extent of such authorized use comprising:

means operative between a first state for disabling said device and a second state for enabling said device;

a thin, pocket-sized card unit having a miniaturized solid state counter;

a card reader unit having means for receiving said card unit;

electronic display means having a plurality of display portions for displaying a count in a decimal format;

transfer means for transferring the count in said card unit to said display means;

said device including means for generating usage signals representative of a predetermined usage



quality;

said card reader unit further including means for coupling said usage signals to the card unit counter to alter the count contained therein;

5 means responsive to the count displayed by said display means for operating the control device to its first state when the count displayed is other than said predetermined count and for operating said control device to its second state when the count

10 displayed is said predetermined count.

2. The apparatus of Claim 1, in that said counter in said card unit is an up/down counter of the solid state type, having a plurality of counter stages each adapted to represent a decimal digit in binary coded

15 form.

3. The apparatus of Claim 2, wherein said card reader unit comprising means for generating a plurality of binary coded control signals occurring in a predetermined sequence;

20 said card unit transfer means further including means responsive to said control signals for transferring the binary coded count signals to said card reader unit in a sequential fashion, said card reader transfer means comprising solid state multiplexer

25 means.

4. The apparatus of Claim 3, wherein said card reader unit transfer means transfers each binary coded group representing a decimal digit of said count to an associated decimal display position of

30 said display means responsive to said control signals, said card reader unit transfer means comprising solid state demultiplexer means.

5. The apparatus of Claim 4, wherein each display position of said display means comprises a

35 solid state decimal display means of the segmented type and latched decoder driver means for storing a binary coded decimal digit transferred thereto, each of said latched decoder driver means converts the binary coded decimal signals stored therein to

40 signals for activating the respective segments of the segmented type display coupled thereto to create a visually observable decimal number representative of the binary coded decimal number stored in said latched decoder driver means.

45 6. The apparatus of Claim 5, wherein said logical gating means couples selected ones of said decimal display units of the segmented type for operating said control device to said second state when the decimal quantity displayed is zero.

50 7. The apparatus of Claim 3, wherein said card reader unit transfer means further comprises means responsive to said control signals for strobing only that latched decoder driver means whose binary coded decimal signal has been transferred to the

55 card reader unit transfer means, said strobing means comprising solid state binary coded decimal to decimal decoder means.

8. The apparatus of Claim 1, further comprising a miniature battery in said card unit being coupled to

60 said counter means for enabling the contents of the counter means to be stored for an indefinite period.

9. The apparatus of claim 8, wherein said battery is a rechargeable battery arranged to be recharged

65 by the card reader unit when the card unit is coupled to the card reader unit.

10. Means for introducing a preprogrammed count into a card unit, said card unit comprising a solid state counter;

70 said card programming unit being comprising settable switch means;

a receptacle for receiving a card unit;

counter means and means responsive to insertion of a card unit into said receptacle for transferring the count represented by said settable switch means

75 into said counter means and for simultaneously altering the counts in said programming unit counter means and said card unit counter means in reverse directions under the control of clock pulse means; and

80 means for de-energizing said clock pulse means when said card programming unit count means reaches a predetermined count.

11. The apparatus of Claim 10, wherein said card programming unit further includes display means

85 for displaying the count of the card unit counter means in a decimal fashion.

12. The apparatus of Claim 10, wherein said card programming unit further comprises a power source terminal and a power return terminal;

90 said card unit comprising jumper means for coupling said power source terminal to said power return terminal when the card unit is inserted into said receptacle means;

normally reset bistable means being operated to

95 the set state upon insertion of a card unit into said receptacle means;

second normally reset bistable means being set when said first bistable means is set and a switch means coupled therebetween is closed to enable

100 transfer of the decimal number set in said mechanical selective switching means into said programming unit counter means.

13. The apparatus of Claim 11, further comprising gating means responsive to transfer of the

105 desired count to be entered into said card unit counter means for simultaneously passing clock pulses from said clock pulse means to the counter means of said card unit and said programming unit.

14. The apparatus of Claim 13, further comprising means in said card programming unit for

110 operating the card unit counter means, which is an up/down counter, to count in a predetermined direction when the card unit is inserted into the receptacle means of the card programming unit.

15. The apparatus of Claim 14, further comprising logical gating means responsive to said card programming unit counter means reaching a prede-

115 termined count for preventing said logical gating means from passing further pulses to the counter means of said card unit and said programming unit.

16. The apparatus of Claim 15 further comprising means coupling the output of said logical gating means to said first and second bistable means to simultaneously reset said first and second bistable means when the programming unit counter means reaches a predetermined count to clear the card programming unit counter, disable said clock source and prevent said card input from being programmed

120 again due to accidental operation of said programming switch.

17. A method for controlling access and extent of access of machine and employing a card unit, card programming unit and card reading unit said card unit comprising solid state counter means, said card programming unit comprising means for introducing a preprogrammed count into said card unit and said card reader unit including means for displaying said count, means for decrementing said count responsive to machine use and means for controlling the operating state of the machine in accordance with the count stored in the card unit, said method comprising the steps of:

inserting a card unit into said programming unit; incrementing the count in said card unit counter means in accordance with a preselected quantity and displaying the count in said card unit to confirm the transfer of the desired count; inserting the preprogrammed card unit into the card reader unit; enabling the machine coupled to said card reader unit only when said count is other than a predetermined quantity; generating a visual display of said count; altering the count in said card unit counter means as the machine is being used, said count being decremented by an amount commensurate with the use of said machine; disabling said machine when said count reaches said predetermined quantity; and updating the visual display to reflect changes in said count.

18. The method of Claim 17 further comprising the steps of transferring each decimal digit of the count from said card unit to said card reader unit in a predetermined sequence and continually repeating said sequence.

19. A control system for preventing unauthorized use of a device comprising:

a card unit having solid state counter means; a control unit including means for receiving said card unit; security means in said card unit for providing an enabling condition; detector means in said control unit responsive to said enabling condition for generating a device enabling signal; device enabling means responsive to device usage for coupling decrementing pulses to said counter means;

means in said card reader unit responsive to a predetermined count in said counter means for permanently disabling said enabling condition generating means; and

said device enabling means being deactivated in the absence of said enabling condition.

20. The control system of Claim 19, wherein said logic means comprises zero count detector means.

21. A miniaturized portable card unit for use with a control unit, arranged to enable a device coupled thereto when a valid card unit is inserted into the control unit, said card unit comprising:

solid state counter means for storing a preprogrammed count; means for decrementing said preprogrammed count responsive to device usage signals received

from the control means when said device is operated;

zero detection means;

identifying means for generating an identifying code when the card unit is coupled to the control unit;

coupling means having a first condition for normally coupling said identifying means to the control unit and a second condition for decoupling said identifying means from said control unit; and count detecting means responsive to a predetermined count in said counter means for operating said coupling means to said second state.

22. The card unit of Claim 21, wherein said identifying means comprises means for generating a multi-bit binary identifying code.

23. The card unit of Claim 22, wherein the coupling means is inaccessible from the exterior of said card unit.

24. The card unit of Claim 22, including housing means for completely enclosing all of the electronic components of said card unit;

connector means including electrical terminals arranged along the exterior of housing means for electrically connecting the electronic components in said housing means with the control unit.

25. The card unit of Claim 24, wherein said coupling means includes a reset terminal for receiving a reset signal for resetting said coupling means to said first condition; and said reset terminal being inaccessible from the exterior of said housing means.

26. A method for operating a card unit having a counter and arranged for use with a device the access of which is controlled by a control unit designed to enable said device only upon receipt of a valid card unit, said method comprising the steps of:

detecting the presence of a power signal when the card unit is inserted into the control unit;

examining said predetermined count; generating an identity signal and applying the identity signal to the control unit when said count is non-zero;

reducing the count in said counter in the presence of a device usage signal derived from the control unit; and

terminating generation of said identity signal when said count reaches zero.

27. The method of Claim 26, wherein the step of generating an identity signal comprises the step of generating a binary coded identity signal.

28. The method of Claim 26, further comprising the step of increasing the count in said counter in the presence of count setting signals applied to the card unit from an external source; and preventing any further increase of said count upon the receipt of count setting signal.

29. Control means for preventing unauthorized use of a device and for controlling the extent of such authorized use substantially as described with reference to the accompanying drawings.

30. Means for introducing a preprogrammed count into a card unit, as claimed in Claim 10 substantially as described with reference to the accompanying drawings.

31. A method for controlling access and extent of access of machine and employing a card unit as claimed in Claim 17 substantially as described with reference to the accompanying drawings.

5 32. A control system for preventing unauthorized use of a device as claimed in Claim 19 substantially as described in the accompanying drawings.

33. A miniaturized portable card unit for use with a control unit as claimed in Claim 21 substantially as described with reference to the accompanying drawings.

10 34. A method for operating a card unit as claimed in Claim 26 substantially as described by way of example herein.

15 Printed for Her Majesty's Stationery Office by The Tweeddale Press Ltd.,  
Berwick-upon-Tweed, 1983.  
Published at the Patent Office, 25 Southampton Buildings, London, WC2A 1AY,  
from which copies may be obtained.

(21) Application No 8711744  
(22) Date of filing 19 May 1987

(71) Applicant  
**General Electric Company Plc**  
  
(Incorporated in United Kingdom)  
  
1 Stanhope Gate, London

(72) Inventors  
**Anthony Francis Steiner**  
**Richard Edmonds**

(74) Agent and/or Address for Service  
**John Hinton Kensett**  
**GEC Plc, Central Patent Dept, Marconi Research**  
**Centre, West Hanningfield Road, Great Baddow,**  
**Chelmsford, Essex**

(51) INT CL.  
G06F 9/06

(52) Domestic classification (Edition J):  
G4A FL

(56) Documents cited  
GB A 2174261 GB A 2168831 GB A 2087606  
GB A 2004394 EP A2 0217654 US A 4663707

(58) Field of search  
G4A  
Selected US specifications from IPC sub-class  
G06F

(54) Data processing system

(57) The memory area within an electronic token of the 'smart card' type comprising a processor 4, memory 7, 8, 9 and input/output means 5 is divided into an execute only region 7 and a non-volatile read/write region 8, 9. An applications program is loaded into the read/write region 8 by software methods using a coupler unit 2 and may be altered if the use of the card alters.

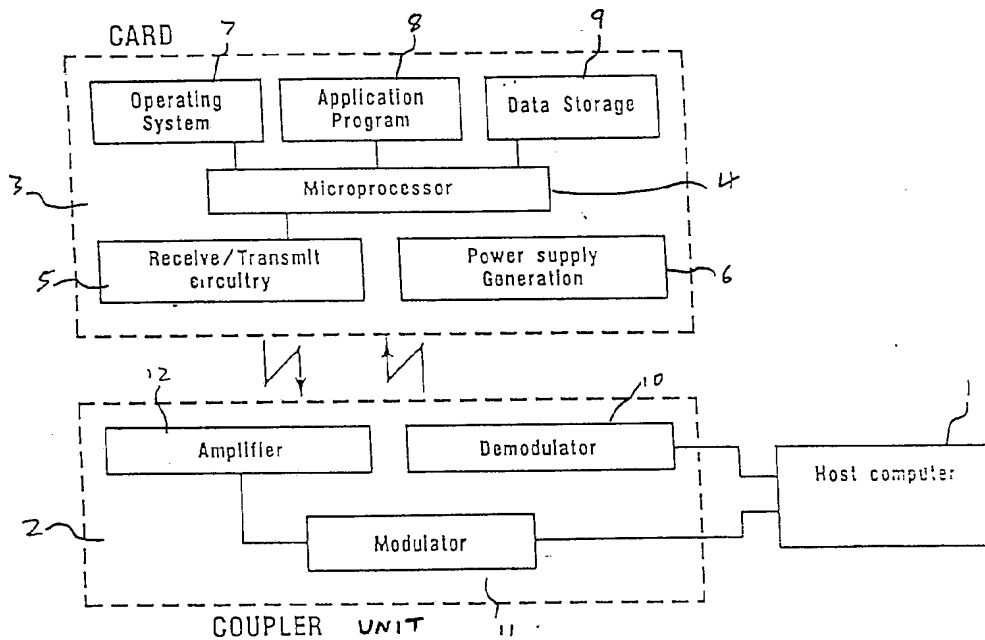


FIGURE 1

1/2

2204973

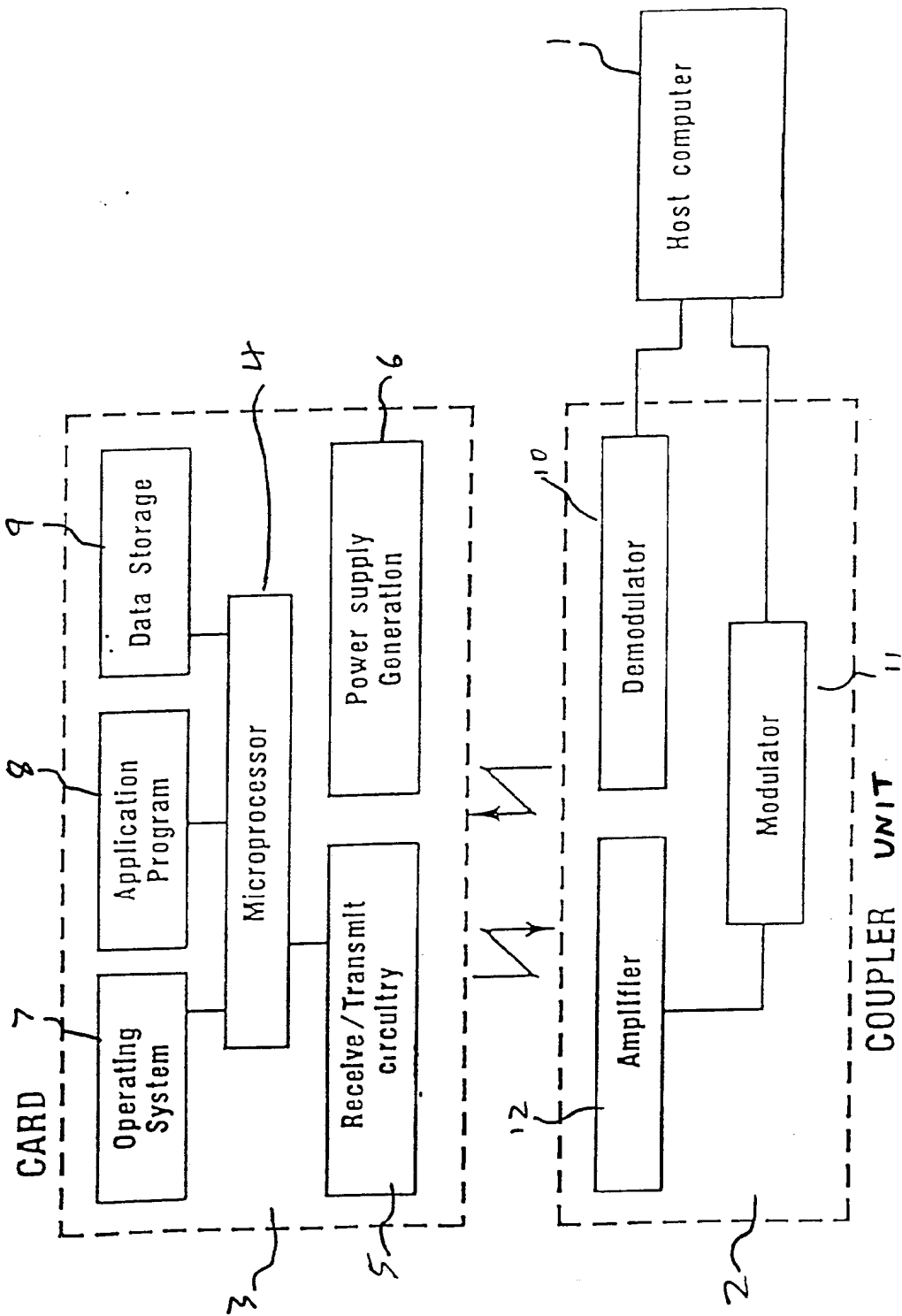


FIGURE 1

2/2

2204973

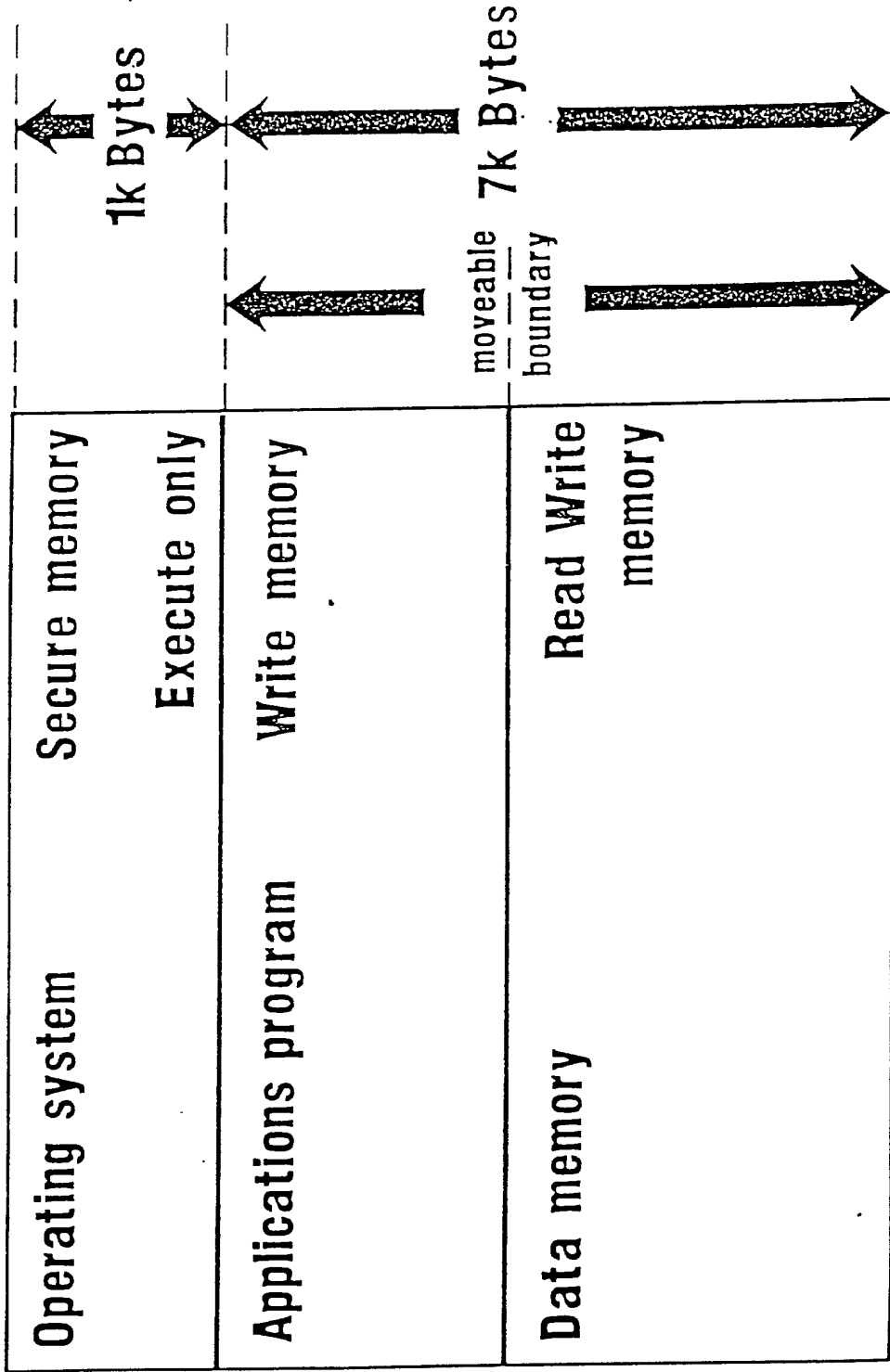


FIGURE 2

Data Processing System

This invention relates to a data processing system of the type comprising one or more portable electronic tokens, each comprising processing means, memory means and input/output means and one or more fixed read/write terminals, and in particular but not exclusively it relates to such a system as is disclosed in United Kingdom published patent application number GB2173623A, which is incorporated herein by reference.

Transactions between such tokens, often known as 'smart cards' and the read/write terminals are performed under the control of software, known as applications software, residing in both the card and the terminals. The algorithms implemented by the applications software in the card generally determines in full the operation of the card. Conventionally, the application software is embedded into the card at manufacture and is contained within a ROM such that it can not be altered. Each ROM is therefore designed with a particular program and application in mind and to change the ROM, and hence the use of the card, necessitates a considerable expenditure and time and requires new masks to be made.

The present invention arose from the need to produce a card, the software within which is relatively easily changeable to satisfy each different application of the card.

According to the present invention in a first aspect there is provided a portable electronic token comprising processing means, memory means and input/output means and a read/write terminal for interacting with the token,  
5 wherein the memory means comprises an execute only memory region and a non-volatile read/write memory region and wherein applications software is stored in the read/write region.

The read/write region may be an E<sup>2</sup> PROM, battery-backed RAM or any other suitable non-volatile read/write  
10 memory.

In a second aspect the invention provides a method of loading software into a portable electronic token of the type comprising processing means, memory means and input/output means and adapted for interaction with a  
15 read/write terminal, wherein the memory means comprises an execute only memory region and a non-volatile read/write region, which method comprises operatively coupling the token and terminal, interchanging messages between the token and terminal to check whether the token and terminal  
20 are authorised, and, if they are authorised; loading a program code adapted to form application software into at least a portion of the read/write memory region.

In a preferred embodiment, the token is adapted to interact with the terminal by inductive coupling and such  
25 coupling is used to load the applications software.



The method may further include the step of establishing a partition between the loaded application program and the remainder of the read/write memory region. The position of this partition can be varied dependent upon the envisaged uses of the token. The application software will then remain within the electronic token even when it is not operatively coupled to a terminal, until it is wished to load a new program.

Advantageously, the execute only memory region may include within it software such that after applications software has been loaded into the read/write region, checked and tested, the software routine alters, by means of software or hardware, the circuitry within the token such that the applications program is permanently stored within the token and may not be removed or altered by means of the loading procedure described above.

Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings in which,

Figure 1 shows in block form elements of the electronic token and coupler embodying the present invention and

Figure 2 shows the arrangement of memory areas within the token.

Referring to Figure 1 the general arrangement of an electronic token or card system is shown. A host computer 1 which may be a personal computer (PC) is connected to a

coupler unit 2. This unit is arranged to inductively couple with a portable electronic token, shown here as card 3. This is a small hand-held token, perhaps of credit-card sized proportion. Coupling between the card and coupler is achieved inductively by means of modulated fields, as is described in the aforementioned British patent application no. GB2173623A. Card 3 comprises a micro-processor 4 of any convenient type, a Receive/Transmit circuit 5 and power supply means 6 which may either be an on board battery or, more preferably, means for tapping off power which is inductively coupled from the coupler 2. The card further includes a memory region which is divided, according to the invention, into three areas; an operating system area 7, applications program area 8 and data storage area 9. Operating system area 7 is of execute only type and areas 8 and 9 are of non volatile read/write memory, and may for instance be E<sup>2</sup> ROM or battery-backed RAM.

Operating system, application program and data storage may occupy adjacent areas of memory within one integrated circuit. The microprocessor and memory may be embodied in a single integrated circuit.

The coupler 2 comprises a demodulator 10 and modulator 11 for processing modulated signals received or transmitted after amplification by an amplifier 12. Unmodulated signals, either after demodulation or before

modulation are fed to or from suitable communication lines of host computer 1.

5 The loading procedure for such a system will now be described. Upon power up i.e. operatively coupling the card 3 and coupler 2, the microprocessor 4 begins to execute instructions residing in the operating system. As stated above, the memory portion storing the operating system is execute only and will be set upon manufacture. The data within it can be neither read nor written to by  
10 any application program. An initialisation sequence follows, an 'answer to reset' character is issued and then a loading routine begins. The card waits to receive a message to indicate that it is in communication with the loading terminal, which in this case is coupled to an host  
15 computer 1. If the card receives a suitable message before a defined time period has elapsed, an interchange of messages between host computer 1 and the card takes place and these messages are used by the card to check whether authorised software is being used within the host  
20 computer 1. Such authorisation procedures will be well known to those skilled in the art and can be used to prevent a card being programmed by means other than that defined by the card manufacturer or user. For instance, coded messages could be exchanged, and authentication or  
25 encryption processes using shared secret keys may be implemented. If the card has been satisfied that the loader, i.e. host computer 1, is authorised, the card will

clear its application memory before receiving a sequence of executable codes which are arranged to form the new application programme. This code is then stored in the application programme area 8 of the card. Finally, the software within the card is used to establish a partition between the applications program area 8 and remainder of the read/write memory region to establish a data storage area 9, in which data relevant to the intended uses of the card can be stored and altered as desired.

The memory areas of the card are shown in Figure 2 where one example is shown having a total memory capability of 8 k bytes. This value may of course be varied as desired. Once the partition mentioned above has been established, then the two memory regions 8 and 9 are set up, although, as shown in figure 2, the exact memory requirements may vary and be movable dependent upon the particular applications program, and memory requirements for data storage.

After the initial programming stage, the card may be removed from the terminal and will retain the applications program. When the card is subsequently powered up and does not receive a "loading" message after issuing its answer to reset, the operating system within the card directs the microprocessor to commence execution of which ever application program is held within its memory.

Should a card not be satisfied of the authenticity of

a loading station, it will not load a new application program and will halt execution.

The loading function within the card can also be disabled by an applications program. Once an application program has been downloaded, debugged and tested, it is often desirable that the card's function be fixed for the remainder of its life. This can be easily achieved by a slight modification to the application program such that it calls a routine held within the operating system which serves to remove a software or hardware link, disabling the loading routine.

CLAIMS

1. A method of loading software into a portable electronic token of the type comprising processing means, memory means and input/output means and adapted for interaction with a read/write terminal, wherein the memory means comprises an execute only memory region and a non-volatile read/write region, which method comprises operatively coupling the token and terminal, interchanging messages between the token and terminal to check whether the token and terminal are authorised, and, if they are authorised; loading a program code adapted to form application software into at least a portion of the read/write memory region.

2. A method as claimed in claim 1 wherein the token is adapted to interact with the terminal by inductive coupling and such coupling is used to load the applications software.

3. A method as claimed in claim 1 or claim 2 including the step of establishing a partition between the loaded application program and the remainder of the read/write memory region.

4. A method as claimed in any of the preceding claims wherein the execute only memory region includes software adapted to alter the software or hardware of the token after an applications program has been loaded such that the applications program cannot be removed or altered.

5. An electronic system comprising a portable electronic token comprising processing means, memory means and input/output means and a read/write terminal for interacting with the token, wherein the memory means
- 5 comprises an execute only memory region and a non-volatile read/write memory region and wherein applications software is stored in the read/write region.
6. A system as claimed in claim 5 wherein the read/write region is an E<sup>2</sup> PROM.
- 10 7. A system as claimed in claim 6 wherein the read/write region is a battery-backed ROM.
8. A software loading procedure substantially as hereinbefore described with reference to, and as illustrated by, the accompanying drawings.

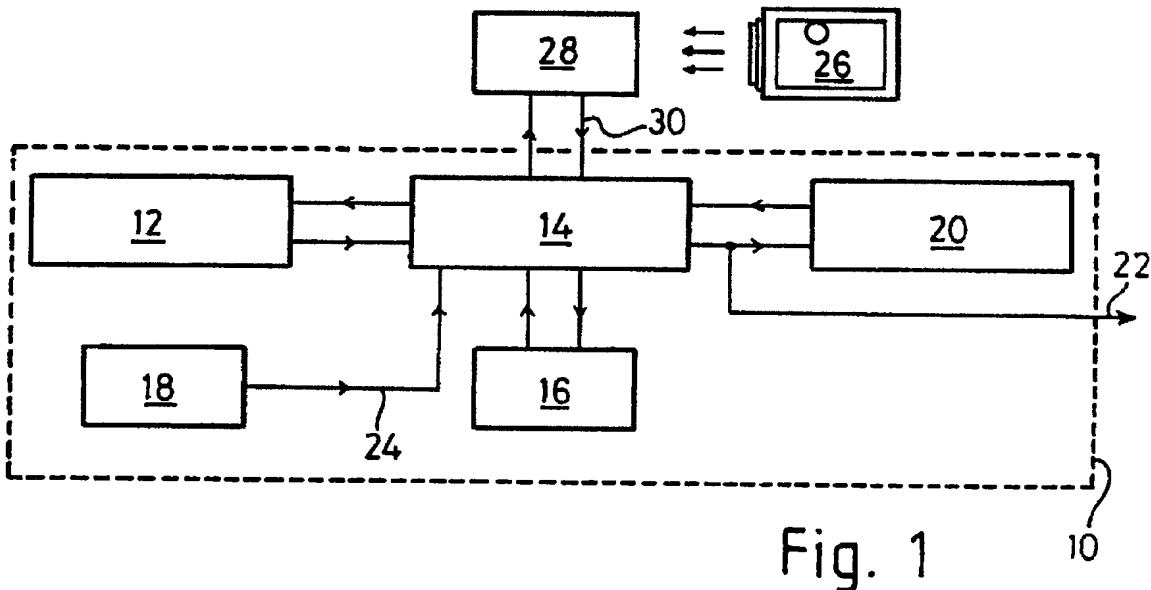
(12) UK Patent Application (19) GB (11) 2 274 009 (13) A

(43) Date of A Publication 06.07.1994

(21) Application No 9227029.7	(51) INT CL <sup>5</sup> G07F 7/00
(22) Date of Filing 29.12.1992	(52) UK CL (Edition M) G4V VAL
(71) Applicant(s) <b>Ampy Automation - Digilog Limited</b>  <b>(Incorporated in the United Kingdom)</b>  <b>Froggnall, Deeping St James, PETERBOROUGH, PE6 8RS, United Kingdom</b>	(55) Documents Cited <b>GB 2254469 A GB 2092796 A GB 2042234 A</b>
(72) Inventor(s) <b>Kenneth Payne</b> <b>Andrew John Robinson</b>	(58) Field of Search UK CL (Edition L) G4V VAA VAC VAK VAL INT CL <sup>5</sup> G07F 7/00 7/02 17/32 17/34 <b>ONLINE DATABASES : WPI</b>
(74) Agent and/or Address for Service <b>Keith W Nash &amp; Co</b> <b>Pearl Assurance House, 90-92 Regent Street, CAMBRIDGE, CB2 1DP, United Kingdom</b>	

(54) Card-operated machines

(57) A machine such as a vending machine or a gaming machine has a card reader (12) and a transceiver (28) adapted to exchange information with a portable unit (26) also having a transceiver, whereby the response of the machine to an inserted card can be altered, for example to alter the quantity of goods or gaming time provided. Information relating to machine operation may be transmitted from transceiver (28) to unit (26) and coded signals may be used.



At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

The claims were filed later than the filing date within the period prescribed by Rule 25(1) of the Patents Rules 1990.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1990.

GB 2 274 009 A



1/1

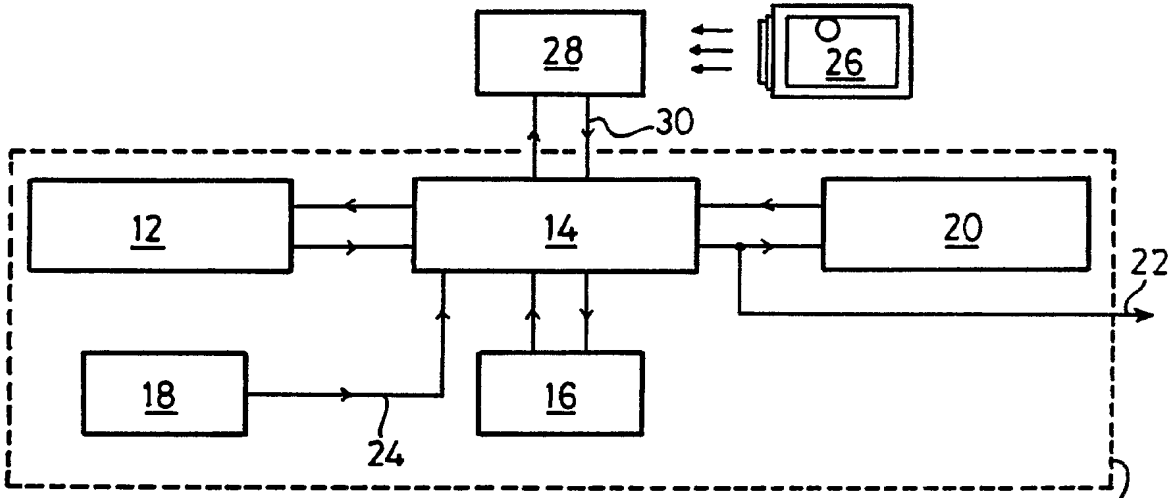


Fig. 1

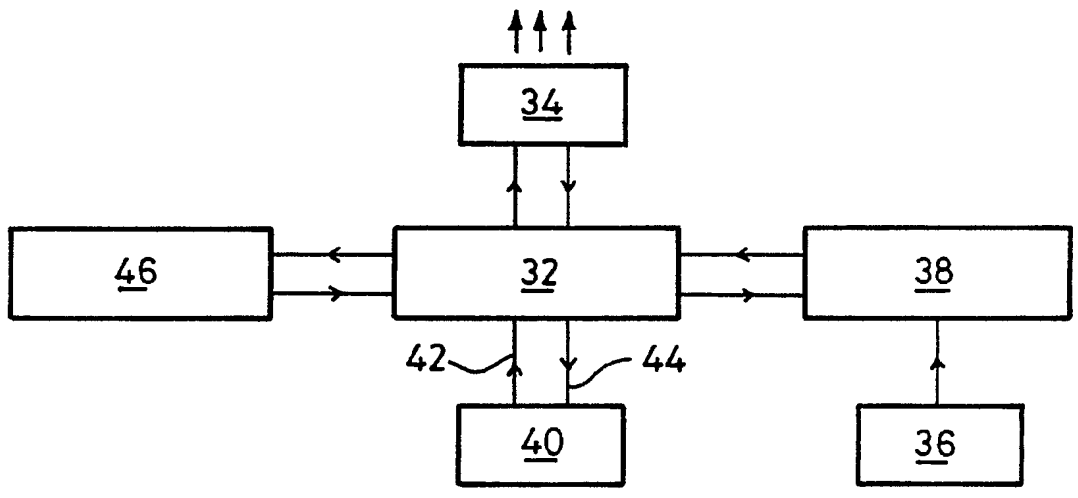


Fig. 2

- 1 -

Title: Improvements in and relating to machines having  
card readers

Field of invention

This invention concerns machine readable cards and card readers, particularly when used in commodity vending equipment, gaming machines and the like, and devices and methods for programming the operation and response of such devices to the insertion of machine readable cards.

Background to the invention

It has been known for some time that machine readable cards such as magnetically encoded cards can be employed in commodity vending or gaming machines to allow the dispensing of a commodity, or credits to the gaming machine. The amount of credit on such cards can be raised up to the maximum amount of credit encoded on the card to enable commodity to be purchased or games to be played.

It is an object of the present invention to facilitate the programming of card readers and associated machines to determine what can be purchased by the use of the card in such machines.

According to the present invention in a machine adapted to provide a response to the insertion of a machine readable card into a programmable card reader associated therewith, receiver means is provided responsive to signals transmitted by portable transmitting devices, for

programming the reader or associated apparatus, so as to alter the response of the machine to the subsequent insertion of a card.

The transmitter and receiver means may be linked for example by radio, infra-red, visible light, magnetic, or electro-acoustic such as audible or ultra-sonic radiation.

Each receiver may include a transmitter and each transmitter a receiver, so that bi-directional communication between the portable unit and the machine is possible, enabling signals to be transmitted from the portable unit to the machine and vice versa, as required.

According therefore to another aspect of the present invention in a machine as aforesaid wherein the portable device and the machine each include combined transmitter and receiver (transceiver) means, the card reader in the machine may include memory means associated with the machine transceiver into which signals obtained by the reader and relating to the type of card, identity of card or coded information contained thereon or the like, is stored for subsequent retrieval by the portable transceiver means.

Likewise memory means may be associated with the portable transceiver into which signals can be stored, obtained either from an entry device such as a keyboard associated with the portable device, or from a transmission received from the machine transceiver.

By employing suitable encoding, different wavelengths, modulation techniques or directional receiving and

transmitting devices, or any combination thereof, so a single portable transceiver device may be employed to communicate with more than one machine transceiver. The different machines may be addressed in turn or in groups or all simultaneously, depending on requirement, transmission medium employed and the like.

The portable device may be hand-held.

Encoding of transmitted signals may be amplitude or frequency or pulse or phase modulation of a suitable carrier and digital encoding is preferred.

A method of altering the response of a machine having a card reader associated therewith upon the insertion of a card, comprises the steps of establishing the communication link between a transceiver in the machine and a transceiver in the portable device, selecting signals to be transmitted to the machine transceiver and transmitting same and thereby altering the programming of a programmable device associated with the machine, to thereby alter the function, or functions, which will be performed by the machine, upon the insertion of a card into the card reader associated therewith.

Typically the functions of the machine are controlled by computer programmes stored in a computer memory associated with a micro-processor (of which at least part of the memory may be an integral part), and either different programmes or commands already stored in the memory are selected by signals transmitted to the machine transceiver from the portable unit or programmes or commands in the said machine memory may be replaced by new ones modified by signals transmitted to the machine transceiver from the

portable unit.

A typical machine response which can be adjusted by the invention is the quantity or quality of some commodity which the machine will delivery for one or more units of credit when debited from a pre-programmed card into the reader associated therewith. Thus for example if the machine vends product the signals transmitted can be employed to adjust the amount of the product obtainable per decoded unit from a suitable pre-programmed machine readable card, when inserted therein.

Where the machine is a gaming machine, the transmitting signals may control the length of the game or number of games which can be obtained per credit unit decoded and debited from a pre-payment machine readable card inserted therein.

Each card may be usable only once and this may be guaranteed by employing the card reader to disfigure or consume the card on use, after all the available credit units have been used up.

Each card may be adapted to be pre-programmed upon suitable payment, and reprogramming apparatus may be provided, associated with a site containing one or more card operated machines, for this purpose.

Where a record of what cards have been used in a machine or how many cards have been used in the machine and how many cards have been used to obtain a given amount of, or number of product, or the identity of cards employed as required, the machine card reader may be programmed to retrieve and store appropriate information from each card

insertion, and make the stored information available upon appropriate interrogation signals being received thereby as from a portable transmitter unit as aforesaid.

The invention also lies in a portable transmitter unit with or without receiver means, for establishing at least one communication with a receiver unit associated with a programmable card read in a machine, and adapted to transmit commands signals to the card reader receiver to alter the programming associated therewith and thereby alter the functioning of the machine.

For security, the signals to be transmitted may be coded and a decoding key, only made available to qualified operators. The key may be a second machine readable card adapted to be inserted into a card reader of the machine, or in a card reader associated with the portable unit, or may be a number or word or combination of letters and numerals, entrusted to and known only to the operator and the portable unit may include keyboard means by which such data can be keyed in by the operator when required, to enable authorised intrusion, reprogramming, data retrieval and the like to be performed.

The invention will now be described by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a block schematic diagram of a system employing an optical link between a portable hand-held device and the machine which is controlled by the insertion of a machine readable card; and

Figure 2 is a block schematic diagram of a hand-held unit as shown in Figure 1.

Detailed description of drawings

In Figure 1 the contents of the dotted outline box 10 are the essential elements of a programmable machine control system which includes a magnetic card reader 12, microprocessor controlled device or micro-controller 14, memory 16, card detector 18 and monitoring device or watchdog 20.

The card reader 12 delivers electrical pulses to the micro-controller 14. The latter decodes the pulses and generates control signals for transmission via a signal path 22 to control circuits (not shown) within the machine and also a monitoring device 20 which for example compares each generated signal with a look-up table and in turn controls the signals released along line 22 and ensures that only correct control signals are supplied to the machine.

The micro-controller 14 also supplies data to a memory 16 or receives from the memory depending on the instructions generated by the micro-processor within the controller 14.

Card detection means 18 as its name suggests simply determines when a card has been inserted into the card reader. Such a device enables the micro-controller to be powered down into a sleep mode to conserve power and a signal from the card detector 18 along line 24 is arranged to change the operating condition of the system so that it is ready to receive and respond to signals from the read head 12.

Further signal paths are shown in Figure 1 on the assumption that the read head is also a writing head and to this end signals from the micro-controller 14 may be supplied to the read/write head for inserting data onto a card for example to indicate the number of credit units left on the card or to cancel information stored on the card or to write information to the card to indicate that the card has been used in a particular machine and cannot be used in that machine again.

Data can be transmitted to the micro-controller from a remote hand-held unit 26 containing an optical transmitting device which is a light emitting diode, laser, modulated light source or the like and a suitable opto-electrical transducer is provided in an optical port 28 for receiving light signals from the remote hand-held unit 26 and decoding same and delivering signals to the micro-controller along the line 30 in response to signals transmitted thereto by the hand-held unit 26.

Where the latter also includes receiver means, the optical port 28 will advantageously include transmitter means so that signals from the micro-controller 14 can be conveyed back to the hand-held unit 26 via the same optical port 28, this time the latter operating as a transmitter and the hand-held unit operating as a receiver.

The establishment of transmission direction may be automatic, may be multiplexed, may be menu-driven or operator controlled.

Alternatively different hand-held units may be employed one for downloading information from the micro-controller and memory 14, 16 and the other adapted to transmit data



to the micro-controller 14 and remainder of the system 10.

In the first case the remote unit includes a transmitter device for triggering via the optical port micro-controller 14 into a read and transmit mode whereafter data stored within the memory 16 and/or additional memory within the micro-controller 14 (not shown) is read out and transmitted via the optical port 28 to the remote hand-held receiver unit 26.

In the other mode of operation, information stored within the hand-held unit 26 can be transmitted to the micro-controller via the optical port 28 and again the hand-held unit 26 includes a suitable transceiver (which may be the same as the first mentioned transceiver) for triggering the micro-controller by the optical port 28 into the appropriate mode. In the second mode of operation, the triggering signal from the remote hand-held unit 26 triggers the micro-controller 14 into a receive mode so that signals subsequently received thereby via the optical port 28 are processed and stored in appropriate memories such as 60 for subsequent use and/or are conveyed via signal paths such as 22 to appropriate elements within the machine or to the watchdog 20.

Figure 2 illustrates the contents of the hand-held unit 26. As with the system of Figure 1, the hand-held unit is micro-processor controlled by a micro-controller 32 and incoming signals from the optical port 28 are received by an optical port 34 associated with the hand-held unit and vice versa. A battery which may be a rechargeable device 36 provides power for the micro-controller via an ON/OFF switch 38 which additionally serves to enable data

transfer when operated. In this way if the battery becomes low or is disconnected, the data transfer enable condition is inhibited so that in a low battery system, corrupting data cannot be transmitted or received.

As before, a memory 40 is provided linked to the micro-controller 32 with data transfer paths 42 and 44 for transferring data to and from the memory 40.

Signals indicating when data transfer has occurred, are generated by data transfer acknowledge circuit 46.

In the event that the hand-held unit is a dedicated receive only device, the optical port 34 only has to decode received data signals. Where the hand-held device is to be a dedicated transmit only device, the optical port 34 is exchanged for a transmitting device which is modulated or otherwise driven by signals from the micro-controller 32. Since it is nevertheless necessary to advise the unit when it is to be interrogated, the optical port 34 additionally includes light sensitive signal detector means for receiving and decoding a precursor to a transmission and end of transmission signal so that the micro-controller 32 and related circuitry can be "woken up" upon receipt of an appropriate precursor and can be powered down into a sleep mode when the end of signal pulse is received.

Since both transmitting and receiving functions are desirable if only to enable a receive only hand-held device to trigger a remote micro-controller into transmit activity via its associated optical port thereby to cause the micro-controller within the machine to power up and interrogate on-board memories and adjoining memories such

as 16 in Figure 1, to assemble data for transmission to the hand-held unit.

Although in the illustrated example optical data transfer is utilised, the optical ports and optical transmitting and receiving devices may be replaced by any suitable signal receiving circuitry.

Both units to advantage utilise an imbedded micro-controller such as a type TMS77C82, to process all signals, including the transmission of digitally encoded information from one device to another.

Typically the optical communication is achieved by means of infra-red photo-diodes and 38KHz AM infra-red receptors serving as the receiver.

Data is preferably transmitted in serial form and modulated at 38KHz by the processor within the micro-controller 32.

The receiver within the optical port 34 converts any received signals to a serial pulse train for subsequent decoding by the micro-controller.

All aspects of the card readers interface with the host machine can be pre-programmed in software and changed at any time to suit individual needs. Thus the variables used in a programme may be stored in the EEPROM 16. It is this information that can be down loaded from the remote hand-held unit to the card reader via the optical port.

The card reader can also send detailed information back to a remote hand-held unit such as shown in Figure 2. The

return information may for example be the number of operations so far, the number of operations when last programmed, the readers identity code and the like. The latter is typically an individual identity code given to each reader or operator, for both security and identification. Thus communication between a remote hand-held unit and a machine mounted unit can be established in a secure manner by forcing entry of a reader identification code before any transmission in reception path has been set up.

As mentioned, two separate remote hand-held units may be used in the system, one to down load programming to the card reader on the machine and one to up lift data from the card reader unit. Both hand-held units may be powered by 9V batteries or the like which are only switched on when the power ON/data transfer push button switch 38 is depressed and typically the micro-controller and remaining circuitry is also switched off by the processor when communication ceases.

The programming information and identity number of the reader to be programmed is generated in a PC using custom software (not shown). The programming information is then down loaded to the remote hand-held unit using for example an optical programming device and the down loaded data is stored in a suitable EPROM such as 40 within the hand-held unit.

The invention thus enables programming of a card reader to be performed simply by pointing the remote hand-held unit towards the reader and depressing the power ON - data transfer push button 38. The remote hand-held unit will first check to ensure that the identity code of the reader

it is communicating with is identical to one that it has been asked to programme. Successful communication is acknowledged by an audio transduced sounding.

A second remote hand-held unit is designed to read only and thereby allow blocks of data which contain information about the card readers current status to be down loaded from the card reader circuits of Figure 1 to the hand-held unit circuits of Figure 2. The hand-held unit is capable of storing information in a significant EPROM in respect of up to 400 individual card readers. The accumulated data can be bulk loaded via a suitable transmission cable into a personal computer (PC) using a programming device for later use in custom applications, software packages such as accountancy packages and the like.

Claims

1. A machine adapted to provide a response to the insertion of a machine readable card into a programmable card reader associated with said machine, wherein receiver means is provided responsive to signals transmitted by a portable transmitting device, for programming the reader or associated apparatus so as to alter the response of the machine to the subsequent insertion of a card.
2. A machine according to claim 1, wherein the receiver means is adapted to be linked to the transmitting device by radio, infra-red, visible light, magnetic, electro-acoustic, audible or ultra-sonic radiation.
3. A machine according to claim 1 or claim 2, in combination with the portable transmitting device.
4. A machine according to claim 3, wherein the receiver means includes a transmitter and the transmitting device includes a receiver, so that bi-directional communication between the portable device and the machine is possible, enabling signals to be transmitted from the portable device to the machine and vice versa, as required.
5. The combination according to claim 4, wherein both the machine and the portable device include a transceiver, and wherein the card reader in the machine includes memory means associated with the machine transceiver into which signals obtained by the reader and relating to the type of card, identity of card or coded information contained

thereon or the like, is stored for subsequent retrieval by the portable transceiver device.

6. The combination according to claim 5, wherein memory means is associated with the portable transceiver device into which signals can be stored, obtained either from an entry device such as a keyboard associated with the portable device, and/or from a transmission received from the machine transceiver.

7. The combination according to any of claims 4 to 6, wherein the portable device is a hand-held unit.

8. The combination according to any of claims 4 to 7, wherein, by employing suitable encoding, different wavelengths, modulation techniques or directional receiving and transmitting devices, or any combination thereof, the single portable transceiver device is adapted to communicate with more than one machine transceiver.

9. The combination according to claim 8, employing encoding of transmitted signals by amplitude or frequency or pulse or phase modulation of a carrier.

10. The combination according to claim 8 or claim 9, employing digital encoding.

11. A method of altering the response of a machine having a card reader associated therewith to the insertion of a card, comprising the steps of establishing the communication link between a transceiver in the machine and a transceiver in a portable device, selecting signals to be transmitted to the machine transceiver and transmitting same and thereby altering the programming of

a programmable device associated with the machine, to thereby alter the function or functions which will be performed by the machine upon the insertion of a card into the card reader associated therewith.

12. A method according to claim 11, wherein the functions of the machine are controlled by a computer program stored in a computer memory associated with a microprocessor (of which at least part of the memory may be an integral part), and either different programs or commands already stored in the memory are selected by signals transmitted to the machine transceiver from the portable unit or programs or commands in the said machine memory are replaced by new programs or commands modified by signals transmitted to the machine transceiver from the portable unit.

13. A method according to claim 12, wherein the machine response altered by transmission of signals from the portable unit is the quantity or quality of a commodity which the machine will deliver for one or more units of credit when debited from a pre-programmed card inserted into the reader associated with the machine.

14. A method according to claim 13, wherein the machine is a gaming machine, and wherein the transmitted signals control the length of the game or number of games which can be obtained per credit unit decoded and debited from a pre-payment machine readable card inserted into the card reader.

15. A method according to claim 14, wherein the machine readable card is usable only once and this is ensured by employing the card reader to disfigure or consume the card



after all the available credit units have been used.

16. A method according to claim 14, wherein the machine readable card is adapted to be pre-programmed upon suitable payment, and reprogramming apparatus may be provided for this purpose, associated with a site containing one or more card operated machines.

17. A method according to any of claims 13 to 16, wherein, in order to obtain a record of what cards have been used in a machine or how many cards have been used in the machine or how many cards have been used to obtain a given amount of, or number of product or the identity of cards employed, the machine card reader is programmed to retrieve and store appropriate information from each card insertion, and make the stored information available upon appropriate interrogation signals being received thereby from the portable transceiver unit.

18. A portable transmitter unit with or without receiver means, for establishing at least one communication with a receiver unit associated with a programmable card reader in a machine, and adapted to transmit command signals to the receiver unit to alter the programming associated therewith and thereby alter the functioning of the machine.

19. A unit according to claim 18, wherein the signals to be transmitted are coded and a decoding key is only made available to qualified operators.

20. A unit according to claim 19, wherein the key is a second machine readable card adapted to be inserted into a card reader of the machine, or in a card reader associated

with the portable unit, or may be a number or word or combination of letters and numerals, entrusted to and known only to the operator and the portable unit may include keyboard means by which such data can be keyed in by the operator when required, to enable authorised intrusion, reprogramming and data retrieval to be performed.

21. A machine having a card reader and signal receiver substantially as hereinbefore described with reference to Figure 1 of the accompanying drawings.

22. A portable unit having a transmitter for communicating with a machine having a card reader and receiver, substantially as hereinbefore described with reference to the accompanying drawings.

23. The combination of the machine of claim 21 and the unit of claim 22.

24. A method of adjusting the response of a machine having a card reader substantially as hereinbefore described.

- 18 -

**Relevant Technical Fields**

- (i) UK Cl (Ed.L)      G4V (VAA, VAC, VAK, VAL)
- (ii) Int Cl (Ed.5)    G07F 7/00, 7/02, 17/32, 17/34

Search Examiner  
 G NICHOLLS

Date of completion of Search  
 20 OCTOBER 1993

**Databases (see below)**

(i) UK Patent Office collections of GB, EP, WO and US patent specifications.

Documents considered relevant following a search in respect of Claims :-  
 1-24

(ii) ONLINE DATABASE: WPI

**Categories of documents**

- X: Document indicating lack of novelty or of inventive step.
- Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.
- A: Document indicating technological background and/or state of the art.
- P: Document published on or after the declared priority date but before the filing date of the present application.
- E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.
- &: Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages	Relevant to claim(s)
X	GB 2254469 A (BARCREST) See especially page 2 lines 16-17 and page 3 lines 15-20	1-3, 11, 12, 18
X	GB 2092796 A (INTERPLAY ELECTRONICS) See especially page 1 lines 12-18 and 35-37	1-3, 11, 18
X	GB 2042234 A (BARCREST) Whole document see especially page 2 lines 43-56	1-4, 8, 11, 12, 18

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).

#### STATEMENT OF RELEVANCY

JP 10-269289 was cited in DEFENDANTS' DISCLOSURE OF PRIOR ART filed as reference 3-1 in the IDS dated Jan 15, 2014 in U.S. Patent Appl. No. 13/438,754. This copy of JP 10-269289 was obtained from the file history of U.S. Patent No. 8,296,239 and contains the machine translation of the referenced filed in that patent.

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-269289

(43)Date of publication of application : 09.10.1998

(51)Int.Cl. G06F 17/60  
G06F 1/00  
G06F 9/06  
G06F 15/00  
G09C 1/00  
H04L 9/08  
H04L 12/14  
H04M 15/00

(21)Application number : 09-074182

(71)Applicant : SONY CORP

(22)Date of filing : 26.03.1997

(72)Inventor : MAARI KOUICHI

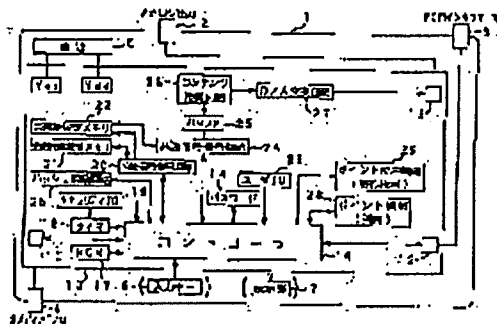
(54) DIGITAL CONTENT DISTRIBUTION MANAGING METHOD, DIGITAL CONTENT REPRODUCING METHOD AND ITS DEVICE

(57)Abstract:

**PROBLEM TO BE SOLVED:** To construct an easily portable and also economical system that makes a player enjoy digital contents at any time in any place and that sufficiently resists application as defence against illegal usage, by decoding the processed digital contents with a content key and also extending and reproducing them.

**SOLUTION:** A player 1 is provided with at least a common key cipher decoding circuit 24 decoding the ciphered digital contents through the use of the content key, an extending circuit 26 being an extending means for extending the compressed digital contents and a D/A converting circuit 27 converting digital data into an analog signal. When the player 1 is the one who is registered in the system, he can freely copy the ciphered contents so as to appreciate the contents only by obtaining the content key.

Therefore, the ciphered contents are easily installed in storage media.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-269289

(43) 公開日 平成10年(1998)10月9日

(51) Int.Cl. <sup>6</sup>	識別記号	F I
G 0 6 F 17/60		G 0 6 F 15/21 3 3 0
1/00	3 7 0	1/00 3 7 0 F
9/06	5 5 0	9/06 5 5 0 Z
15/00	3 3 0	15/00 3 3 0 Z
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 F

審査請求 未請求 請求項の数37 OL (全 39 頁) 最終頁に続く

(21) 出願番号 特願平9-74182  
 (22) 出願日 平成9年(1997)3月26日

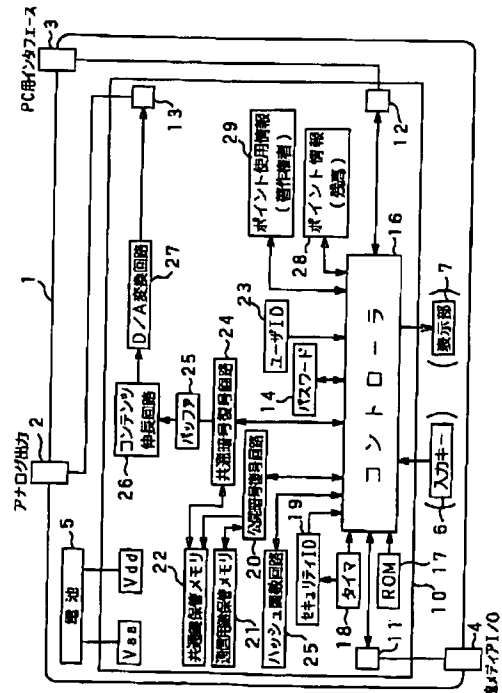
(71) 出願人 000002185  
 ソニー株式会社  
 東京都品川区北品川6丁目7番35号  
 (72) 発明者 真有 浩一  
 東京都品川区北品川6丁目7番35号 ソニー株式会社内  
 (74) 代理人 弁理士 小池 晃 (外2名)

(54) 【発明の名称】 デジタルコンテンツ配付管理方法、デジタルコンテンツ再生方法及び装置

(57) 【要約】

【課題】 簡単に持ち運びができて何時でも何処でもデジタルコンテンツを楽しむことを可能とし、デジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築する。

【解決手段】 暗号化されたコンテンツ鍵を復号化し、セッション鍵を暗号化する公開暗号復号回路20と、コンテンツ鍵やセッション鍵を保管する共通鍵保管メモリ22と、公開暗号方式の鍵情報を保管する通信用鍵保管メモリ21と、ポイント情報を格納するポイント情報格納メモリ29と、ポイント使用情報を格納するポイント使用情報格納メモリ28と、暗号化デジタルコンテンツの復号化し、暗号化ポイント情報の復号化、ポイント使用情報の暗号化を行う共通暗号復号回路24と、圧縮デジタルコンテンツを伸長する伸長回路26と、デジタルコンテンツをD/A変換するD/A変換回路27とを、1チップ化する。



## 【特許請求の範囲】

【請求項1】 デジタルコンテンツを、当該デジタルコンテンツ毎のコンテンツ鍵を用いて暗号化すると共に、圧縮するデジタルコンテンツ加工工程と、上記加工したデジタルコンテンツを、通信相手側からのデジタルコンテンツ送信要求に応じて送信するコンテンツ送信工程と、

上記加工されたデジタルコンテンツの復号化に使用するコンテンツ鍵を暗号化し、通信相手側からのコンテンツ鍵送信要求に応じて送信するコンテンツ鍵送信工程と、上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報を暗号化し、通信相手側からの課金情報送信要求に応じて送信する課金情報送信工程と、通信相手側から送信されてきた暗号化されたコンテンツ使用情報を受信して復号化するコンテンツ使用情報受信工程と、

上記コンテンツ使用情報に基づいて徴収した利用金を、上記デジタルコンテンツの権利者に対して分配する利用金分配工程とを有してなることを特徴とするデジタルコンテンツ配付管理方法。

【請求項2】 上記コンテンツ鍵は共通鍵であることを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項3】 上記コンテンツ鍵を通信相手側の公開鍵を用いて暗号化することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項4】 通信相手側から送信されてきた暗号化された共通鍵を受信して復号化する共通鍵復号化工程を有することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項5】 上記共通鍵はセッション鍵であることを特徴とする請求項4記載のデジタルコンテンツ配付管理方法。

【請求項6】 上記課金情報送信工程では、課金情報を上記共通鍵を用いて暗号化することを特徴とする請求項4記載のデジタルコンテンツ配付管理方法。

【請求項7】 上記コンテンツ使用情報受信工程では、上記暗号化されたコンテンツ使用情報の復号化に上記共通鍵を用いることを特徴とする請求項4記載のデジタルコンテンツ配付管理方法。

【請求項8】 上記コンテンツ使用情報受信工程では、上記通信相手側からの上記課金情報の送信要求に伴って当該通信相手側から送信されてくる上記暗号化されたコンテンツ使用情報を受信することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項9】 上記課金情報送信工程では、上記課金情報と共にコンテンツの使用条件を示す情報を送信することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項10】 暗号化及び圧縮処理によって加工され

たデジタルコンテンツを受信して格納するコンテンツ受信工程と、

上記加工されたデジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を生成するコンテンツ鍵要求情報生成工程と、

上記コンテンツ鍵要求情報を暗号化して送信するコンテンツ鍵要求情報送信工程と、

上記コンテンツ鍵の要求に応じて送信されてきたコンテンツ鍵を受信するコンテンツ鍵受信工程と、

上記コンテンツ鍵に施されている暗号化を復号化するコンテンツ鍵復号化工程と、

上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管工程と、

上記加工されたデジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化工程と、

上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を生成する課金情報要求情報生成工程と、

上記課金情報要求情報を暗号化して送信する課金情報要求情報送信工程と、

上記課金情報の要求に応じて送信されてきた課金情報を受信すると共に当該課金情報に施されている暗号化を復号化して格納する課金情報受信工程と、

上記加工されたデジタルコンテンツを伸長するコンテンツ伸長工程と、

上記加工されたデジタルコンテンツの復号化に応じたコンテンツ使用情報を生成して格納するコンテンツ使用情報格納工程と、

上記コンテンツ使用情報を暗号化して送信するコンテンツ使用情報送信工程とを有することを特徴とするデジタルコンテンツ再生方法。

【請求項11】 コンテンツ使用情報格納工程では、上記格納されている課金情報の残高を確認し、上記加工されたデジタルコンテンツの復号化に応じて上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項12】 上記復号化及び伸長がなされたデジタルコンテンツをデジタル/アナログ変換するデジタル/アナログ変換工程を有することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項13】 上記コンテンツ受信工程では、上記加工されたデジタルコンテンツを外部記憶媒体に格納することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項14】 上記コンテンツ鍵は共通鍵であることを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項15】 上記コンテンツ鍵復号化工程では、上

記コンテンツ鍵を固有の秘密鍵を用いて復号化することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項16】 共通鍵を発生し、当該共通鍵を暗号化して送信する共通鍵送信工程を有することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項17】 上記共通鍵送信工程では、上記共通鍵としてセッション鍵を生成することを特徴とする請求項16記載のデジタルコンテンツ再生方法。

【請求項18】 上記課金情報要求情報送信工程では、上記課金情報要求情報を上記共通鍵を用いて暗号化することを特徴とする請求項16記載のデジタルコンテンツ再生方法。

【請求項19】 上記コンテンツ使用情報送信工程では、上記コンテンツ使用情報の暗号化に上記共通鍵を用いることを特徴とする請求項16記載のデジタルコンテンツ再生方法。

【請求項20】 上記コンテンツ使用情報送信工程では、上記課金情報要求情報生成工程による上記課金情報の要求に伴って、上記暗号化したコンテンツ使用情報を送信することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項21】 上記課金情報受信工程では、上記課金情報と共に暗号化されて送信されてくるコンテンツの使用条件を示す情報をも受信することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項22】 データ通信を行うデータ通信手段と、暗号化及び圧縮処理によって加工されたデジタルコンテンツを受信して記憶媒体に記憶させるコンテンツ記憶制御手段と、

暗号化されたコンテンツ鍵を復号化するコンテンツ鍵復号化手段と、

上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管手段と、

上記加工されたデジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化手段と、

上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報に施されている暗号化を復号化する課金情報復号化手段と、

上記復号化された課金情報を格納する課金情報格納手段と、

上記加工されたデジタルコンテンツを伸長するコンテンツ伸長手段と、

上記加工されたデジタルコンテンツの復号化に応じたコンテンツ使用情報を生成するコンテンツ使用情報生成手段と、

上記コンテンツ使用情報を格納するコンテンツ使用情報格納手段と、

上記コンテンツ使用情報を暗号化するコンテンツ使用情報暗号化手段とを有することを特徴とするデジタルコ

ンテンツ再生装置。

【請求項23】 上記加工されたデジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を暗号化するコンテンツ鍵要求情報暗号化手段と、

上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を暗号化する課金情報要求情報暗号化手段とを有することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項24】 コンテンツ使用情報生成手段は、上記課金情報格納手段に格納されている課金情報の残高を確認し、上記加工されたデジタルコンテンツの復号化に応じて、上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項25】 上記復号化及び伸長がなされたデジタルコンテンツをデジタル/アナログ変換するデジタル/アナログ変換手段を有することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項26】 上記コンテンツ記憶制御手段は、上記加工されたデジタルコンテンツを外部記憶媒体に記憶させることを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項27】 上記コンテンツ鍵は共通鍵であることを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項28】 装置固有の鍵を保管する固有鍵格納手段を有し、

上記コンテンツ鍵復号化手段では、上記固有鍵格納手段に保管している装置固有の秘密鍵を用いて、上記暗号化されているコンテンツ鍵を復号化することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項29】 共通鍵を発生する共通鍵発生手段と、上記共通鍵を暗号化する共通鍵暗号化手段とを有することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項30】 上記共通鍵発生手段は、上記共通鍵としてセッション鍵を生成することを特徴とする請求項29記載のデジタルコンテンツ再生装置。

【請求項31】 上記課金情報復号化手段は、上記課金情報を上記共通鍵を用いて復号化することを特徴とする請求項29記載のデジタルコンテンツ再生装置。

【請求項32】 上記コンテンツ使用情報暗号化手段は、上記コンテンツ使用情報を上記共通鍵を用いて暗号化することを特徴とする請求項29記載のデジタルコンテンツ再生装置。

【請求項33】 上記コンテンツ使用情報暗号化手段は、上記課金情報要求情報暗号化手段による上記課金情



報要求情報の暗号化に伴って、上記コンテンツ使用情報の暗号化を行うを有することを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項34】 上記課金情報復号化工程では、上記課金情報と共に暗号化されているコンテンツの使用条件を示す情報をも復号化することを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項35】 携帯可能に構成されてなることを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項36】 カード状の筐体を有することを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項37】 集積回路化してなることを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばオーディオデータやビデオデータ等のデジタルコンテンツを配布し、それらデジタルコンテンツの利用量に応じて課金するシステムに好適なデジタルコンテンツ配付管理方法、並びにデジタルコンテンツ再生方法及び装置に関する。

【0002】

【従来の技術】コンピュータプログラムやオーディオデータ、ビデオデータ等のデジタルコンテンツの流通を簡便化し、潜在需要を掘り下げ、市場拡大に有利な手法としては、例えば特公平6-19707号公報に記載されるソフトウェア管理方式、特公平6-28030号公報に記載されるソフトウェア利用管理方式、特公平6-95302号公報に記載されるソフトウェア管理方式のような手法が存在する。上記特公平6-19707号公報に記載されたソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、ソフトウェアの利用状況をソフトウェア権利者別などによって把握できるようにしたものである。また、特公平6-28030号公報に記載されるソフトウェア利用管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムを買い取り（買い取った後は無料で使用できる）価格を付し、コンピュータシステム内には購入可能な金額を示すデータを設けておき、有償プログラム購入の際は、同システムにある利用可能なソフトウェアの名称としてテーブルに登録すると共に、当該購入可能な金額を示すデータをソフトウェア価格分だけ減じ、また登録済みソフトウェアを該テーブルから抹消する際には状況に応じて該購入可能な金額を示すデータを増加更新するようにしたものである。また、上記特公平6-95302号公報に記載されるソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラム

につき実際の利用量（利用回数または利用時間など）に応じて利用料金を徴収するために、利用されたプログラムの識別と「利用者識別符号と料金を記録」しておき、該記録を回収することでプログラム権利者が自分の所有するプログラムの利用料金を把握でき、プログラムの利用量に応じたプログラム利用料金を回収する場合のシステムで有効なものである。

【0003】

【発明が解決しようとする課題】ところが、上述したデジタルコンテンツをネットワークを使って配信するシステムは、パーソナルコンピュータ上だけの運用を考慮しており、したがって、簡単に持ち運びができ、何時でも、また何処でも上記デジタルコンテンツを楽しむといったシステムは存在しない。

【0004】一方、上述した各公報記載の手法は、潜在需要を掘り下げ、市場拡大に有利であるが、デジタルコンテンツのコピー或いは不当な使用への防御として不十分であり、且つ経済的なシステムとは言い難い。

【0005】そこで、本発明はこのような状況に鑑みてなされたものであり、簡単に持ち運びができて何時でも何処でもデジタルコンテンツを楽しむことを可能とし、また、デジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築することを可能にするデジタルコンテンツ配付管理方法、並びにデジタルコンテンツ再生方法及び装置を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明によれば、デジタルコンテンツの配付側では、デジタルコンテンツを暗号化及び圧縮して加工し、この加工したデジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手側から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしており、一方、デジタルコンテンツの再生側では、その加工されたデジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報の生成を行い、このコンテンツ使用情報を配付側に送信するようにし、また本発明のデジタルコンテンツ再生装置は、携帯可能となされていることにより、上述した課題を解決する。

【0007】

【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。

【0008】先ず、本発明のデジタルコンテンツ配付方法、デジタルコンテンツ再生方法及び装置の具体的な内容及び構成の説明を行う前に、これらの理解を容易にするために、本発明が適用されるシステム全体の概略構成及びシステムの運用方法について図1から図7までの各図を用いて簡単に説明する。

【0009】図1にはシステム全体の概略的な構成を示す。

【0010】この図1において、ユーザ側200は、本発明のデジタルコンテンツ再生装置（以下、プレーヤ1と呼ぶことにする）及びいわゆるパーソナルコンピュータ（以下、ユーザ端末50と呼ぶことにする）を保有しているものとする。

【0011】ユーザ端末50は、通常のパーソナルコンピュータであるが、本発明に使用する後述する各種ソフトウェアをアプリケーションソフトとして格納してなると共に、表示手段であるディスプレイ装置と放音手段であるスピーカ、及び情報入力手段であるキーボードやマウス等が接続されてなるものである。当該ユーザ端末50は例えばネットワークを介してシステム管理会社210と接続可能であり、また、プレーヤ1との間のインターフェイス手段を有し、データ送受が可能である。

【0012】プレーヤ1は例えば図2に示すような構成を有するものである。

【0013】この図2の構成の詳細な説明については後述するが、当該プレーヤ1は、デジタルコンテンツの処理経路の主要構成要素として、暗号化されているデジタルコンテンツをコンテンツ鍵を用いて復号化する共通鍵暗号復号回路24と、圧縮されているデジタルコンテンツを伸長する伸長手段である伸長回路26と、デジタルデータをアナログ信号に変換するD/A変換回路27とを少なくとも有する。なお、以下に言う復号化とは、暗号化を解くことである。

【0014】また、このプレーヤ1は、使用するデジタルコンテンツの権利情報及び使用状況を示す情報（以下、これら情報をポイント使用情報と呼ぶ）や、デジタルコンテンツを使用する際に必要となる保有金額データ、すなわちデジタルコンテンツを使用する毎に減額される課金データ（以下、ポイント情報と呼ぶ）等を扱う主要構成要素として、上記ポイント使用情報を格納するポイント使用情報格納メモリ29と、上記ポイント情報を格納するポイント情報格納メモリ28とを少なくとも備えている。

【0015】さらに、このプレーヤ1は、後述するような暗号化及び復号化に使用する各種鍵を格納するための構成として共通鍵保管メモリ22及び通信用鍵保管メモリ21と、これらに格納された鍵を用いて暗号化や復号化を行うための構成として共通暗号復号回路24及び公開暗号復号回路20を有している。また、このプレーヤ1は、上記暗号化及び復号化に関連する構成として、システム管理会社210のホストコンピュータと連動した乱数を発生してセキュリティIDを生成するセキュリティID発生回路19及びタイマ18や、後述するいわゆるハッシュ値を発生するハッシュ関数回路25等を有している。

【0016】その他、当該プレーヤ1は、デジタルコ

ンテンツやその他各種のデータ及び各構成要素の制御をROM17に格納されたプログラムに基づいて行う制御手段であるコントローラ16と、携帯時の動作電源としての電池5を備えている。

【0017】ここで、図2のプレーヤ1の各主要構成要素は、セキュリティ上、IC（集積回路）或いはLSI（大規模集積回路）の1チップで構成されることが望ましい。この図2では、各主要構成要素が集積回路10内に1チップ化されている。当該プレーヤ1には、外部とのインターフェイス用として3つの端子（アナログ出力端子2と、PC用インターフェイス端子3と、記録メディア用I/O端子4）を備え、これら各端子が集積回路10のそれぞれ対応する端子13、12、11に接続されている。なお、これら各端子は統合することも、また新たに別の端子を設けることも可能であり、特にこだわるものではない。

【0018】システム管理会社210は、システム全体を管理する管理センタ211と、上記プレーヤ1を販売する販売店212とからなり、仮想店舗230を介してユーザ側200のユーザ端末50との間で、後述するようなデジタルコンテンツの供給に関する情報の送受、コンテンツプロバイダ240が保有するコンテンツを圧縮及び暗号化するデジタルコンテンツの加工、上記加工したデジタルコンテンツの供給、金融機関220との間の情報送受等を行う。なお、システム管理会社210と金融機関220の間では、ユーザ側200の口座番号やクレジット番号、名前や連絡先等の確認や、ユーザ側200との間で取引可能かどうかの情報等のやり取りなどが行われる。金融機関220とユーザ側200の間では、実際の代金振込等の処理が行われる。また、販売店212は、必ずしもシステム管理会社210内に含まれる必要はなく、販売代理店であってもよい。

【0019】上記システム管理会社210の管理センタ211は、例えば図3に示すような構成を有するものである。この図3の構成の詳細な説明については後述するが、主要構成要素として、デジタルコンテンツを管理し、その展示、暗号化及び圧縮等の加工処理、デジタルコンテンツの暗号化及び復号化に使用する鍵情報であるコンテンツ鍵やIDの発生等の各機能を有するコンテンツ管理機能ブロック100と、ユーザ情報を管理し、通信文（メッセージやポイント情報等）の暗号化及び復号化、確認メッセージの発生、セキュリティIDの発生、金融機関230との間での決済申請、ポイントの発生等の各機能の他、ユーザ加入処理等を行うユーザ加入処理機能部118をも備えたユーザ管理機能ブロック110と、ポイント使用情報等を管理する使用情報管理機能ブロック120と、システム全体を管理し、通信機能を有する管理機能ブロック130とを、少なくとも有してなる。

【0020】上述した図1のように構成されるシステム

の実際の運用方法の一例を、図4～図7を用いて説明する。なお、以下の運用方法は、ユーザ側200やシステム管理会社210、金融機関220、コンテンツプロバイダ240等が実際に行う手順である。

【0021】このシステムの運用方法の説明では、プレーヤ1の購入の手順、デジタルコンテンツの検索からプレーヤ1用の記憶メディアに対するデジタルコンテンツのインストールまでの手順、当該デジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該デジタルコンテンツを使用した場合の精算の手順、デジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金の分配の手順について順番に説明する。

【0022】まず、プレーヤ1の購入時の手順としては、図4の(1)及び(5)に示すように、ユーザ側200が実際に店頭あるいは通信販売等により、上記販売店212から上記プレーヤ1を購入する。

【0023】このとき、上記販売店212は、図4の(2)に示すように、上記プレーヤ1の販売時に上記ユーザ側200から提供された個人情報(名前や連絡先等)及び決済情報(銀行口座、クレジット番号等)と、上記販売したプレーヤ1固有の番号(プレーヤ固有鍵等を含む)とをシステム管理会社210の管理センタ211に登録する。

【0024】管理センタ211は、図4の(3)に示すように、金融機関220に対して、上記ユーザ側200から提供された口座番号やクレジット番号等の確認を行い、図4の(4)に示すように金融機関220から取引可能である旨の情報を得る。

【0025】次に、デジタルコンテンツの検索からプレーヤ1用の記憶メディアへのデジタルコンテンツのインストールまでの手順として、上記プレーヤ1を購入したユーザ側200は、当該プレーヤ1とのインターフェイス手段を備えたユーザ端末50を使って、図5の(1)に示すように、希望のデジタルコンテンツの検索、選択、編集、注文等を行う。このときの検索から注文までの処理は、ユーザ端末50がアプリケーションソフトとして格納している検索ソフトを用い、例えばネットワークを介して接続された仮想店舗230に対して行う。

【0026】仮想店舗230は、例えば管理センタ211がネットワーク上の仮想的に設けている店舗であり、この仮想店舗230には、例えば複数のコンテンツの内容を示す情報が展示されている。ユーザ側200は、仮想店舗230にて提供されているこれらの情報に基づいて、所望のコンテンツの注文を行うことになる。なお、仮想店舗230に展示されるコンテンツの内容を示す情報としては、例えばコンテンツが映画等のビデオデータである場合には当該映画等のタイトルや広告、当該映画中の1シーン等の映像などが考えられ、また、コンテン

ツがオーディオデータである場合は曲名やアーティスト名、当該曲の最初の数フレーズ(いわゆるイントロ)等が考えられる。したがって、ユーザ側200のユーザ端末50にて上記仮想店舗230をアクセスした場合には、当該ユーザ端末50上に上記仮想店舗230の複数のコンテンツの内容が仮想的に展示され、これら展示物の中から所望のものを選択することでコンテンツの注文が行われることになる。

【0027】上記ユーザ側200のユーザ端末50からデジタルコンテンツの注文等があったとき、上記仮想店舗230は、図5の(2)に示すように管理センタ211に対してデジタルコンテンツの供給依頼を行う。

【0028】当該デジタルコンテンツの供給依頼を受け取った管理センタ211は、コンテンツプロバイダ240に対して上記供給依頼のあったデジタルコンテンツの配給依頼を行う。これにより、当該コンテンツプロバイダ240は、図5の(4)に示すように上記配給依頼のあったデジタルコンテンツを管理センタ211に配給する。

【0029】管理センタ211は、上記コンテンツプロバイダ240から配給されたデジタルコンテンツに対して暗号化及び所定の圧縮方式を用いた圧縮を施すと共に、この圧縮及び暗号化されたデジタルコンテンツに対して、当該コンテンツのID(コンテンツID)とこのコンテンツの著作権者等の権利者情報と当該コンテンツを使用したときの課金額とコンテンツをユーザ側200に供給する仮想店舗名等とを付加する。なお、コンテンツに対する課金額は、コンテンツプロバイダ240にて事前に決定される。

【0030】上記管理センタ211にて加工されたコンテンツは、図5の(5)に示すように、仮想店舗230に送られ、さらにこの仮想店舗230を介して、図5の(6)のようにユーザ側200のユーザ端末50に供給される。これにより、プレーヤ1には、上記ユーザ端末50からコンテンツが供給され、このコンテンツが当該プレーヤ1に格納されることになる。

【0031】なお、この図5に(2)～(5)までの流れについては、事前に行っておくことも可能である。すなわち、仮想店舗230には、上記複数のコンテンツの内容を示す情報を展示するだけでなく、これら展示に対応した上記加工されたデジタルコンテンツを予め用意しておくようにしても良い。

【0032】次に、上述のようにしてプレーヤ1にインストールされたデジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該デジタルコンテンツを使用した場合の精算の手順では、まず、ユーザ端末50によってプレーヤ1に格納されているポイント情報の不足が確認されて、当該ユーザ端末50からポイント情報の補充要求がなされる。

【0033】このとき、図6の(1)のように、当該ユ

ーザ端末50からは、プレーヤ1にて暗号化されたポイント情報の補充依頼が、管理センタ211に対し転送される。また同時に、既に使用したデジタルコンテンツに対応する著作権者等の権利者の情報すなわちポイント使用情報がプレーヤ1から読み出されて暗号化され、ユーザ端末50を介して管理センタ211に送られる。このように、ポイント情報の補充依頼と同時にポイント使用情報の転送が行われるようにしたのは、当該ポイント使用情報の管理センタ211への送信のみのために、ユーザ側200が管理センタ211にアクセスする手間を省くためである。勿論、このポイント使用情報の転送は、必ずしもポイント情報の購入と同時に進行する必要はなく、独立に行っても良い。

【0034】上記暗号化されたポイント情報の補充依頼及びポイント使用情報を受け取った管理センタ211は、当該暗号を解読することでユーザ側200が要求しているポイント情報の補充量とポイント使用情報の内容を認識する。さらに、当該管理センタ211は、金融機関220に対して図6の(2)のように当該ポイント補充分の決済が可能かどうかの確認を行う。金融機関220にて、ユーザ側200の口座を調べることによって、決済可能であることが確認されると、当該金融機関220から図6の(3)のように決済OKの指示が管理センタ211に送られることになる。

【0035】また、このときの管理センタ211は、図6の(4)に示すように、コンテンツプロバイダ240に対して著作権者等の権利者に支払われることになるポイント使用数、すなわち金額を連絡する。

【0036】その後、管理センタ211では、ポイント補充情報の命令書を暗号化し、これをセキュリティIDと共にポイント補充指示情報として、図6の(5)に示すようにユーザ端末50に送る。このユーザ端末50からプレーヤ1に送られた上記ポイント補充指示情報は、当該プレーヤ1において復号化され、さらにセキュリティIDの確認後に、ポイント情報格納メモリ28へのポイント情報の補充と、ポイント使用情報格納メモリ29からの上記先に連絡した著作権情報等の権利者情報の削除とが行われる。

【0037】次に、デジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金、すなわちポイントの使用情報に応じてユーザの口座から引き落とされることになる代金の分配の手順では、先ず図7の(1)のようにユーザ側200に対して代金振り込み依頼が金融機関220からなされる。このとき、ユーザ側200の口座に十分な残高がある場合には、特に代金振り込み依頼はなされず、口座に十分な残高がない場合には、図7の(2)のようにユーザ側200から金融機関220に対して代金の振り込みがなされる。

【0038】金融機関220は、所定の手数料を差し引いて、図7の(3)のように、ユーザ側200から受け

取った代金を管理センタ211に対して送金する。すなわち管理センタ211では、金融機関220から送金された上記代金から、コンテンツ加工料と金融手数料とシステム管理費等を徴収する。また、当該管理センタ211は、先に使用されたポイントに応じた著作権料を、図7の(4)のようにコンテンツプロバイダ240に対して支払うと共に、仮想店舗230に対しては図7の

(5)のように店舗手数料を支払う。上記著作権料を受け取ったコンテンツプロバイダ240は著作権料を各著作権者に支払い、上記店舗手数料を受け取った仮想店舗230は仮想店舗毎の手数料を各仮想店舗に対して支払う。

【0039】このように、ユーザ側200から支払われた代金は、前記ポイント使用情報に基づいて、著作権料と店舗手数料とコンテンツ加工手数料と決済手数料とシステム管理手数料とに分配され、上記著作権料はコンテンツプロバイダ240に、上記店舗手数料は上記仮想店舗230に、コンテンツ加工手数料はシステム管理会社210に、決済手数料はシステム管理会社と金融機関220に、システム管理手数料はシステム管理会社210に支払われる。

【0040】ここで、本実施の形態のシステム間でのデータ送受、すなわち管理センタ211とプレーヤ1との間のデータ送受の際には、データ通信の安全性を確保するために、通信するデータの暗号化及び復号化が行われる。本発明実施の形態では、暗号化及び復号化の方式として共通鍵暗号方式及び公開鍵暗号方式の何れにも対応可能となっている。

【0041】本発明の実施の形態では、上記デジタルコンテンツ、上記ポイント使用情報、ポイント情報、メッセージやセキュリティID、その他の各種情報の伝送の際の暗号方式としては、処理速度の点から共通鍵暗号方式を採用している。これら各種情報の暗号化及び復号化に使用する共通鍵は、それぞれ各情報に対応して異なるものである。前記図2のプレーヤ1では、管理センタ211から伝送されてくる暗号化された情報の復号化に使用する共通鍵が前記共通鍵保管メモリ22に保管され、この共通鍵保管メモリ22に保管している共通鍵を用いて、前記共通暗号復号回路24が、上記管理センタ211からの暗号化された情報の復号化を行う。

【0042】一方、上記各種情報の暗号化や復号化に使用する上記共通鍵の伝送の際の暗号方式としては、前記プレーヤ1の固有の鍵であるプレーヤ固有鍵が何れの方式に対応しているかによって採用される暗号方式が変わるものである。すなわち、上記プレーヤ固有鍵が共通鍵暗号方式に対応している場合、上記共通鍵は当該プレーヤ固有鍵を用いて暗号化され、また当該暗号化された共通鍵は上記プレーヤ固有鍵を用いて復号化されることになる。これに対して、上記プレーヤ固有鍵が公開鍵暗号方式に対応している場合、上記共通鍵の暗号化には相手

先の公開鍵が用いられ、暗号化された上記共通鍵の復号化にはそれぞれ復号化を行う側の秘密鍵が用いられる。

【0043】例えば上記プレーヤ1から管理センタ211に上記共通鍵（例えば後述するセッション鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記プレーヤ1では通信用鍵保管メモリ21が保管しているプレーヤ固有鍵を用いて上記共通鍵暗号復号回路24が上記共通鍵を暗号化し、管理センタ211では当該管理センタ211が保管しているプレーヤ固有鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。同じく、上記プレーヤ1から管理センタ211に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記プレーヤ1の通信用鍵保管メモリ21が保管している管理センタ211の公開鍵にて上記公開鍵暗号復号回路20が上記共通鍵を暗号化し、管理センタ211では当該管理センタ211が保管している秘密鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。

【0044】逆に、例えば上記管理センタ211からプレーヤ1に上記共通鍵（例えばコンテンツ鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記管理センタ211が保管しているプレーヤ固有鍵にて上記共通鍵が暗号化され、プレーヤ1では上記通信用鍵保管メモリ21にて保管しているプレーヤ固有鍵を用いて、前記共通暗号復号回路24が上記暗号化されてる共通鍵の復号化を行う。同じく、上記管理センタ211からプレーヤ1に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記管理センタ211が保管しているプレーヤ1の公開鍵にて上記共通鍵が暗号化され、プレーヤ1では上記通信用鍵保管メモリ21にて保管しているプレーヤ固有鍵すなわち秘密鍵を用いて、前記公開暗号復号回路20が上記暗号化されてる共通鍵の復号化を行う。

【0045】上述したようなプレーヤ固有鍵自身の暗号方式は、当該プレーヤ固有鍵の配送（システム管理会社210からプレーヤ1への配送）が容易か否かによって決定されている。すなわち、コスト的には共通鍵暗号方式の方が有利であるので、プレーヤ固有鍵の配送が容易であれば共通鍵暗号方式を採用するが、当該プレーヤ固有鍵の配送が困難であるときにはコスト高であるが公開鍵暗号方式を採用する。プレーヤ固有鍵をハードウェアに実装する場合には共通鍵暗号方式を、ソフトウェアに実装する場合には公開鍵暗号方式を採用する。

【0046】以下、本発明の実施の形態では、プレーヤ固有鍵自身の暗号方式としてソフトウェアに実装する場合の互換性を考慮して、上記公開鍵暗号方式を採用する例を挙げて説明することにする。すなわち、上記管理センタ211とプレーヤ1との間で前記共通鍵の伝送が行

われる場合において、上記プレーヤ1側で共通鍵（セッション鍵）が暗号化されるときには管理センタ211の公開鍵を用いて暗号化がなされ、管理センタ211では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。逆に、上記管理センタ211側で共通鍵（コンテンツ鍵）が暗号化されるときには、プレーヤの公開鍵にて暗号化がなされ、プレーヤ1では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。

【0047】前述したような各手順と暗号方式を用いて運用されるシステムを構成する上記プレーヤ1とユーザ端末50と管理センタ211の実際の動作を、以下に順番に説明する。

【0048】先ず、上述したポイント補充すなわちポイント購入時のプレーヤ1、ユーザ端末50、管理センタ10における処理の流れについて、図8から図11を用い、前記図2及び図3を参照しながら説明する。

【0049】図8には、ポイントを購入する際のプレーヤ1における処理の流れを示している。

【0050】この図8において、ステップST1では、ユーザ端末50すなわちパーソナルコンピュータに予めインストールされているポイント購入用のソフトウェアの立ち上げが行われ、この間のプレーヤ1のコントローラ16は、当該ポイント購入用のソフトウェアが立ち上がるまで待っている。

【0051】上記ポイント購入用のソフトウェアが立ち上がると、ステップST2にて、プレーヤ1のコントローラ16は、上記ユーザ端末50に入力された情報を、当該ユーザ端末50から受信する。このときのユーザ端末50に入力される情報とは、上記ポイント購入用のソフトウェアに従って、上記ユーザ端末50を操作するユーザに対して当該ユーザ端末50から入力要求がなされるものであり、例えばパスワードや購入したいポイント情報数等の情報である。

【0052】これらユーザ端末50からの情報は、プレーヤ1のPC用インターフェース端子3及び当該プレーヤ1内にチップ化された集積回路10の端子12を介して、コントローラ16に受信される。当該ユーザ端末50からの情報を受信したコントローラ16は、ステップST3にて、当該プレーヤ1の集積回路10内のパスワード格納メモリ14が格納するパスワードと、上記受信した情報中のパスワードとの比較を行い、上記受信パスワードが正しいかどうかの確認を行う。

【0053】上記パスワードが正しいと確認したコントローラ16は、ステップST4にて、ポイントを購入したい旨の情報（ポイント購入の主旨）と購入したいポイント情報数その他の情報を生成すると同時に、セキュリティID発生回路19からセキュリティIDを発生させ、次のステップST5にてこれらの情報を共通暗号復号回路24にて暗号化させる。コントローラ16は、次

にステップST6にて、ユーザID格納メモリ23からユーザIDを読み出し、当該ユーザIDを上記暗号化した情報に付加し、さらに、ステップST7にて、当該ユーザIDを付加して作成したデータを上記端子12及びPC用インターフェース端子3を介してユーザ端末50に転送する。このユーザ端末50からは、上記作成データが管理センタ211に送られることになる。

【0054】このとき、上記作成データの暗号化には前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ16では、上記共通鍵として、例えば乱数発生手段であるセキュリティID発生回路19からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だつて、プレーヤ1から管理センタ211に対して送られることになる。ここで、当該共通鍵は前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ16では、上記共通鍵であるセッション鍵を公開暗号復号回路20に送ると同時に、通信用鍵保管メモリ21に予め保管されている管理センタ211の公開鍵を取り出して上記公開暗号復号回路20に送る。これにより当該公開暗号復号回路20では、上記管理センタ211の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵はユーザIDと共に、上記作成データの伝送に先だつて管理センタ211に送られている。

【0055】なお、前述したように、ポイント情報の要求と共にポイント使用情報の転送も行う場合、コントローラ16は、ポイント使用情報格納メモリ29から前記権利者情報等を含むポイント使用情報を読み出し、これらも上記共通暗号復号回路26に送って暗号化させる。この暗号化したポイント使用情報は、上記作成データと共に伝送される。また、ポイント使用情報の転送と同時に、ポイント情報の残高をも同様にして転送することも可能である。

【0056】その後、コントローラ16は、ステップST8にて、ユーザ端末50を通して管理センタ211から送られてきた暗号化されているデータを受信する。この管理センタ211から送られてきたデータは、先に当該プレーヤ1から転送した上記購入したいポイント情報数に応じたポイント情報とセキュリティID等の情報が、上記セッション鍵と同じ共通鍵を用いて暗号化されたデータである。

【0057】コントローラ16は、上記管理センタ211からのデータを受信すると、ステップST9にて、当該データを上記共通暗号復号回路24に送ると共に、先に発生して共通鍵保管メモリ22に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路24に送る。当該共通暗号復号回路24では、上記共通鍵を用いて上記管理センタ211からの暗号化されたデータを復

号化する。

【0058】次に、上記コントローラ16は、ステップST10にて、上記復号化されたデータのセキュリティIDを、上記セキュリティID発生回路19からのセキュリティIDとの比較によって確認し、その確認後、ステップST11にて、上記ポイント情報格納メモリ28に格納されていたポイント情報を、上記新たに送られてきたポイント情報にて修正する。

【0059】上記ポイント情報の修正等の処理が終了すると、コントローラ16は、ステップST12にて、処理完了のサインを生成し、上記共通鍵保管メモリ22から読み出した共通鍵と共に上記共通暗号復号回路24に送り、当該共通暗号復号回路24にて暗号化させる。その後、コントローラ16は、ステップST13にて当該暗号化された処理完了のサインを、端子12及び3を介してユーザ端末50に転送し、管理センタ211に送る。

【0060】以上により、ポイント購入の際のプレーヤ1における処理の流れが終了する。

【0061】次に、上記ポイント購入時のユーザ端末50における処理の流れを、図9を用いて説明する。

【0062】この図9において、ユーザ端末50は、ステップST21にて、ポイント購入用のソフトウェアの立ち上げを行う。当該ポイント購入用ソフトウェアが立ち上がると、このユーザ端末50では、ステップST22にて、上記ポイント購入用のソフトウェアに従い当該ユーザ端末50を操作するユーザに対して上述したパスワードや購入したいポイント数等の情報の入力要求を行い、ユーザからこれらの情報が入力されると、当該入力された情報を前記図8のステップST2のように上記プレーヤ1に転送する。

【0063】次に、ユーザ端末50は、ステップST23にて、上記プレーヤ1から前記図8のステップST7のように作成されたデータを受信すると、ステップST24にて、当該プレーヤ1から転送されたデータを、予め登録されているアドレスすなわち管理センタ211へ転送する。

【0064】上記データの転送を行った後のユーザ端末50は、管理センタ211からの返送を待ち、管理センタ211からのデータ返送があると、ステップST25にて当該管理センタ211からのデータをそのままプレーヤ1に転送する。

【0065】当該ユーザ端末50は、ステップST26にて、上記プレーヤ1から前記図8のステップST13のように処理完了のサインを受信すると、当該ポイント購入等の処理が終了したことをユーザに知らせるために、ステップST27にて処理完了のサインをディスプレイに表示し、ユーザに確認させる。

【0066】その後、当該ユーザ端末50は、上記プレーヤ1から送られてきた処理完了のサインの暗号文を管

理センタ211に転送する。

【0067】以上により、ポイント購入の際のユーザ端末50における処理の流れが終了する。

【0068】次に、ポイント購入時の管理センタ211における処理の流れを、図10を用いて説明する。

【0069】この図10において、管理センタ211は、ステップST31のように、コントロール機能部131にて全体が制御される管理機能ブロック130の通信機能部133によって、前記図8のステップST7及び図9のステップST24のようにユーザ端末50を介して転送されたプレーヤ1からの上記暗号化されたデータを受信する。このデータを受信すると、管理センタ211のユーザ管理機能ブロック110は、ステップST32のように、コントロール機能部111の制御の元で、当該受信したデータに添付されたユーザIDに基づいて、データベース部112から共通鍵を入手すると共にセキュリティID発生機能部116からセキュリティIDを入手する。

【0070】なお、この時の共通鍵は、前記プレーヤ1から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、当該管理センタ211のユーザ管理機能ブロック110において、上記管理センタ211の公開鍵暗号方式の秘密鍵が取り出され、この秘密鍵と上記暗号化されているセッション鍵とが通信文暗号/復号機能部114に送られる。当該通信文暗号/復号機能部114では、上記管理センタ211の公開鍵を用いて上記暗号化されたセッション鍵の復号化が行われる。このようにして得られたセッション鍵(共通鍵)が上記データベース部112に格納されている。

【0071】上記データベース部112から上記ユーザIDに対応する共通鍵を入手すると共にセキュリティID発生機能部116からセキュリティIDを入手すると、ステップST33に示すように、管理センタ211のユーザ管理機能ブロック110の通信文暗号/復号機能部114において、上記共通鍵を用いて、上記プレーヤ1からの上記暗号化されたデータの復号化を行い、さらにコントロール機能部111において、当該復号化したデータ中のセキュリティIDと上記セキュリティID発生機能部116から読み出したセキュリティIDとの比較によって、アクセスしてきたユーザ側200(プレーヤ1)が正当な使用者であるかどうかの内容確認を行う。

【0072】上記アクセス元の正当性を確認した管理センタ211では、ステップST34のように、ユーザ管理機能ブロック110のポイント発生機能部113にて、上記ユーザ端末50から送られてきたデータの内容に応じたポイント情報の発行を行い、また、決済請求機

能部117にて、ユーザの決済機関(金融機関220)への請求準備を行う。

【0073】さらに、管理センタ211は、ステップST35のように、例えばコントロール機能部111において、プレーヤ1からのポイント情報の残高とポイント使用情報に不正が無いことを確認し、後の処理のために情報のまとめを行う。すなわち、ポイント情報の残高と実際に使用したポイント情報の数とから不正な使用がないかどうかの確認とまとめを行う。なお、この確認とまとめは、必ず行わなければならないものではないが、望ましくは行った方がよい。

【0074】管理センタ211のユーザ管理機能ブロック110ではまた、上記ステップST35の処理の後、ステップST36のように、セキュリティID発生機能部115において上記プレーヤ1(ユーザ)への新たなセキュリティIDを例えば乱数発生に基づいて算出し、さらに、例えばコントロール機能部110にて、上記セキュリティIDを上記ポイント情報と共に暗号化する。このときの暗号化も前記プレーヤ1から予め送られてきている前記セッション鍵(共通鍵)を用いて行う。

【0075】上記暗号化が終了すると、管理センタ211の管理機能ブロック130の通信機能部133では、コントロール機能部131の制御の元、上記暗号化したデータを前記図9のステップST25及び図8のステップST8のようにユーザ端末50を介してプレーヤ1に転送する。

【0076】その後、管理センタ211の通信機能部133において、ステップST38のように、前記図9のステップST28に示したユーザ端末50からの処理完了サインを受信して復号化すると、管理センタ211のユーザ管理機能ブロック110の決済請求機能部117では、ステップST39のように、当該処理完了サインに基づいて金融機関220に決済を請求する。この金融機関220に対する決済請求は、管理機能ブロック130の通信機能部132から行われる。

【0077】以上により、ポイント購入の際の管理センタ211における処理の流れが終了する。

【0078】上述した図8から図10の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図11に示すように表すことができる。

【0079】すなわちこの図11において、入力情報転送T1では、前記図8のステップST2及び図9のステップST22のように、ユーザ端末50からプレーヤ1に対して、前記パスワードやポイント数等の入力情報が転送される。

【0080】作成データ転送T2では、前記図8のステップST7及び図9のステップST23のように、プレーヤ1からユーザ端末50に対して、前記プレーヤ1にて作成したデータが転送される。また、データ転送T3

では、前記図9のステップST24及び図10のステップST31のように、ユーザ端末50から管理センタ211に対して、前記プレーヤ1が作成したデータが転送される。

【0081】データ転送T4では、前記図10のステップST37及び図9のステップST25のように、管理センタ211からユーザ端末50に対して、管理センタ211にて暗号化したデータが転送される。また、転送T5では、前記図9のステップST25及び図8のステップST8のように、管理センタ211からのデータをユーザ端末50がそのままプレーヤ1に転送される。

【0082】処理完了サイン転送T6では、前記図8のステップST13及び図9のステップST26のように、プレーヤ1からの処理完了サインがユーザ端末50に転送される。さらに、処理完了サイン暗号文転送では、前記図9のステップST28及び図10のステップST38のように、プレーヤ1からの暗号化された処理完了サインが管理センタ211に転送される。

【0083】次に、上述したデジタルコンテンツの入手時のプレーヤ1、ユーザ端末50、管理センタ211における処理の流れについて、図2及び図3を参照しながら、図12から図15を用いて説明する。

【0084】図12には、デジタルコンテンツの入手時のプレーヤ1における処理の流れを示している。

【0085】この図12において、コントローラ16は、ステップST41のように、ユーザ端末50すなわちパーソナルコンピュータに予めインストールされているデジタルコンテンツ入手用のソフトウェアの立ち上げが行われるまで待っている。

【0086】上記デジタルコンテンツ入手用のソフトウェアが立ち上がると、コントローラ16は、ステップST42のように、ユーザ端末50を介して管理センタ211からデジタルコンテンツを含むデータを受信する。このときユーザ端末50から端子3及び12を介して受信するデータは、前述したようにコンテンツ鍵（コンテンツ毎に異なる共通鍵）で暗号化されたデジタルコンテンツと、当該デジタルコンテンツに対応するコンテンツIDとを少なくとも有してなる。したがって、この暗号化されたデジタルコンテンツを使用するには、コンテンツ鍵を管理センタ211から入手しなければならない。このコンテンツ鍵の入手の方法については後述する。

【0087】このユーザ端末50からのデータを受信したコントローラ16は、このデータすなわち暗号化されたデジタルコンテンツを、集積回路10の端子11を介し、記憶メディア用I/O端子4に接続されている記憶メディアに格納する。なお、この記憶メディアとしては、書き換え可能な光ディスクや半導体メモリ等の各種の記憶媒体が考えられるが、ランダムアクセス可能なものが望ましい。

【0088】以上により、デジタルコンテンツの入手時のプレーヤ1における処理の流れが終了する。

【0089】次に、デジタルコンテンツの入手時のユーザ端末50における処理の流れを、図13を用いて説明する。

【0090】この図13において、ユーザ端末50は、ステップST51にて、デジタルコンテンツ入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末50では、ステップST52にて、上記デジタルコンテンツ入手用のソフトウェアに従い、予め登録されているアドレスの管理センタ211にアクセスする。

【0091】このとき、当該管理センタ211は、前記仮想店舗230を用いて複数のデジタルコンテンツを展示している。ユーザ端末50からは、ステップST53にて、この仮想店舗230に展示されている複数のデジタルコンテンツのなかから、ユーザの選択操作に応じた所望のデジタルコンテンツが指定される。すなわち、ユーザ端末50は、ステップST54のように、仮想店舗230に展示されたデジタルコンテンツの中の所望のデジタルコンテンツを指定するためのコンテンツの指定情報を管理センタ211に送信する。

【0092】ステップST55のように、上記コンテンツ指定情報に応じて管理センタ211から返送されたデータ、すなわち前記暗号化されたデジタルコンテンツ及びコンテンツIDからなるデータを受信すると、当該ユーザ端末50は、ステップST56のように、内部の例えばハードディスクやメモリ等の格納手段に上記データを一旦格納する。

【0093】その後、ユーザ端末50は、当該格納したデータ（暗号化されたデジタルコンテンツ及びコンテンツID）を、前記図12のステップST42のようにプレーヤ1に転送する。

【0094】以上により、デジタルコンテンツの入手時のユーザ端末50における処理の流れが終了する。

【0095】次に、デジタルコンテンツ入手時の管理センタ211における処理の流れを、図14を用いて説明する。

【0096】ここで、図3に示す管理センタ211は、前述した仮想店舗230に複数のコンテンツを展示させている。具体的には、管理センタ211のコンテンツ管理機能ブロック100において、前記仮想店舗230を生成しており、この仮想店舗230に上記複数のデジタルコンテンツの展示を行っている。

【0097】このように仮想店舗230にデジタルコンテンツを展示している状態で、図14のステップST61のように、前記図13のステップST54にてユーザ端末50からコンテンツ指定情報を受信する。

【0098】当該ユーザ端末50から上記コンテンツ指定情報を受信すると、コンテンツ管理機能ブロック10



0のコントロール機能部101は、このコンテンツ指定情報を管理機能ブロック130に送る。管理機能ブロック130のコントロール機能部131は、上記コントロール管理機能ブロック100から受け取ったコンテンツ指定情報を、権利者の通信機能部134を通して、前記コンテンツプロバイダ240に転送する。これにより当該コンテンツプロバイダ240からは、上記コンテンツ指定情報にて要求されたデジタルコンテンツが転送されてくる。上記コンテンツプロバイダ240から入手したデジタルコンテンツは、管理機能ブロック130からコンテンツ管理機能ブロック100に送られ、このコンテンツ暗号・圧縮化機能部104に入力される。このとき、コントロール機能部101は、コンテンツ鍵・ID発生機能部103にて発生されてデータベース102に格納されているコンテンツ鍵を、上記コンテンツ暗号・圧縮化機能部104に送る。このコンテンツ暗号・圧縮化機能部104では、上記デジタルコンテンツに対して上記コンテンツ鍵を用いた暗号化を施し、さらに所定の圧縮処理を施す。コントロール機能部101は、上記暗号化及び圧縮処理されたデジタルコンテンツに対して、データベース102から取り出したコンテンツIDを付加し、管理機能ブロック130に送る。なお、デジタルコンテンツがオーディオ信号である場合の所定の圧縮処理としては、例えば近年製品化されているいわゆるMD（ミニディスク：商標）にて使用されている技術である、いわゆるATRAC（Adaptive Transform Acoustic Coding）のように、人間の聴覚特性を考慮してオーディオデータを高効率圧縮する処理を一例とした挙げることができる。

【0099】その後、図14のステップST62に示すように、管理機能ブロック130のコントロール部131は、ユーザ端末との通信機能部133を通して、上記暗号化及び圧縮処理されてコンテンツIDが付加されたデジタルコンテンツを、上記ユーザ端末50に送信する。

【0100】デジタルコンテンツ入手時の管理センタ211における処理の流れは以上である。

【0101】上述した図12から図14の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図15に示すように表すことができる。

【0102】すなわちこの図15において、入力情報転送T11では、前記図13のステップST54のように、ユーザ端末50から管理センタ211に対して、前記コンテンツ指定情報が転送される。コンテンツ転送T12では、管理センタ211から、前記図14のステップST62のように、暗号化されたデジタルコンテンツとコンテンツIDがユーザ端末50に転送される。

【0103】コンテンツ転送T13では、前記図13のステップST57及び図12のステップST42のよう

に、ユーザ端末50に一旦格納された上記暗号化されたデジタルコンテンツとコンテンツIDがプレーヤ1に転送される。

【0104】次に、上述したデジタルコンテンツを使用する際に必要となるコンテンツ鍵とその使用条件の入手時のプレーヤ1、ユーザ端末50、管理センタ211における処理の流れについて、図2及び図3を参照しながら、図16から図19を用いて説明する。

【0105】図16には、コンテンツ鍵及び使用条件の入手時のプレーヤ1における処理の流れを示している。

【0106】この図16のステップST71では、プレーヤ1のコントローラ16において、ユーザ端末50に予めインストールされているコンテンツ鍵及び使用条件入手用のソフトウェアの立ち上げが行われるまで待っている。

【0107】上記ユーザ端末50の上記コンテンツ鍵及び使用条件入手用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末50に入力された情報が、ステップST72のように、前記PC用インターフェース端子3及び集積回路10の端子12を介して受信される。このときの上記ユーザ端末50から供給される入力情報は、鑑賞したいデジタルコンテンツの暗号化を解くのに必要なコンテンツ鍵を要求するための情報である。なお、この例では、上記コンテンツ鍵の要求情報として、このコンテンツ鍵を使用するデジタルコンテンツの指定情報を用いている。

【0108】このコンテンツ指定情報を上記ユーザ端末50から受信したコントローラ16は、ステップST73にて、当該コンテンツ指定情報にて指定されたデジタルコンテンツのIDと、セキュリティID発生回路19からのセキュリティIDとを作成し、この作成したデータを共通暗号復号回路24にて暗号化させる。また、コントローラ16は、当該作成したデータにユーザID格納メモリ23から読み出したユーザIDを付加し、上記端子12及びPC用インターフェース端子3を介してユーザ端末50に転送する。このユーザ端末50からは、上記作成データが管理センタ211に送られることになる。

【0109】このときの作成データの暗号化にも、前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ16では、上記共通鍵として、例えば乱数発生手段であるセキュリティID発生回路19からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だって、プレーヤ1から管理センタ211に対して送られることになる。当該共通鍵は、前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ16では、上記共通鍵であるセッション鍵を公開暗号復号回路20に送ると同時に、通信用鍵保管メモリ21に予

め保管されている管理センタ211の公開鍵を取り出して上記公開暗号復号回路20に送る。これにより当該公開暗号復号回路20では、上記管理センタ211の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵が、上記作成データの伝送に先だて管理センタ211に送られている。

【0110】その後、コントローラ16は、ステップST75にて、後述するようにユーザ端末50を介して管理センタ211から送付されてきた暗号化されたデータを受信する。このときの管理センタ211から送られてきたデータは、後述するように上記コンテンツ鍵と使用条件とセキュリティID等が暗号化されたものである。

【0111】上記管理センタ211からの暗号化されたデータを受信すると、プレーヤ1では、ステップST76のように、上記暗号化されたデータを復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ16は、上記復号化されたデータのセキュリティIDを、上記セキュリティID発生回路19からのセキュリティIDとの比較によって確認することによる正当性の評価を行う。

【0112】ここで、コンテンツ鍵については後述するように公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティIDについては共通鍵暗号方式にて暗号化がなされている。したがって、当該暗号化されているコンテンツ鍵を復号化するには、公開鍵暗号方式の秘密鍵が必要であり、本実施の形態のプレーヤ1では前述したようにプレーヤ固有鍵を秘密鍵として使用することになっているので、当該プレーヤ固有鍵が通信用鍵保管メモリ21から取り出される。このプレーヤ固有鍵は、上記暗号化されたコンテンツ鍵と共に公開暗号復号回路20に送られる。この公開暗号復号回路20では、上記暗号化されているコンテンツ鍵を上記プレーヤ固有鍵を用いて復号化する。このように復号化されたコンテンツ鍵は、共通鍵保管メモリ22に保管される。一方、上記共通鍵暗号方式にて暗号化されている使用条件とセキュリティIDを復号化する場合には、これらのデータを上記共通暗号復号回路24に送ると共に、先に発生して共通鍵保管メモリ22に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路24に送る。当該共通暗号復号回路24では、上記共通鍵を用いて上記使用条件とセキュリティIDを復号化する。このように復号化された使用条件は、ポイント使用情報格納メモリ29に格納される。なお、ここで重要なのは、当該復号化されたコンテンツ鍵・使用条件は、当該プレーヤ1の外部、具体的には図2の集積回路10内に設けられたコントローラ16や共通鍵保管メモリ22、ポイント使用情報格納メモリ29から外部には取り出されないことである。

【0113】上記正当性の確認後、コントローラ16は、ステップST77のように、上記復号したコンテン

ツ鍵を上記コンテンツIDと共に上記共通鍵保管メモリ22に格納させる。

【0114】その後、コントローラ16は、ステップST78にて、上記コンテンツ鍵を入手した旨を示すメッセージを作成し、このメッセージを前述同様に共通鍵暗号復号回路24に送り、予め発生して共通鍵保管メモリ22に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路24に送る。当該共通暗号復号回路24では、上記共通鍵を用いてメッセージを暗号化する。

【0115】当該メッセージの暗号化が終了すると、コントローラ16は、ステップST79のように、この暗号化されたメッセージを端子12及び3を介してユーザ端末50に送信する。この暗号化されたメッセージは、その後、管理センタ211に転送させる。

【0116】以上により、コンテンツ鍵・使用条件入手時のプレーヤ1における処理の流れが終了する。

【0117】次に、コンテンツ鍵・使用条件入手時のユーザ端末50における処理の流れを、図17を用いて説明する。

【0118】この図17において、ユーザ端末50は、ステップST81にて、コンテンツ鍵・使用条件入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末50では、ステップST82にて、上記ソフトウェアに従い当該ユーザ端末50を操作するユーザに対して、希望のコンテンツの指定入力要求を行い、ユーザからコンテンツの指定がなされると、その指定情報を生成する。ユーザ端末50は、上記ステップST83にて、上記コンテンツの指定情報をプレーヤ1に対して送信する。

【0119】次に、ユーザ端末50は、ステップST84にて、前記図16のステップST74のように上記プレーヤ1にて作成されて転送されたデータを受信すると、ステップST85にて、当該プレーヤ1から転送されたデータを、予めアドレスが登録されている管理センタ211へ転送する。

【0120】上記管理センタ211に対してデータの転送を行った後のユーザ端末50は、管理センタ211からの返送を待ち、ステップST86にて、管理センタ211から上記コンテンツIDで指定されたコンテンツ鍵・使用条件とセキュリティID等が暗号化されたデータの返送があると、ステップST87にて当該管理センタ211からのデータをそのままプレーヤ1に転送する。

【0121】上記プレーヤ1に対してデータの転送を行った後のユーザ端末50は、プレーヤ1からの返送を待ち、ステップST88にて、プレーヤ1から前記図16のステップST79のように、上記コンテンツ鍵を入手した旨の暗号化されたメッセージの返送があると、ステップST89にて当該ユーザ端末50に接続されたディスプレイ装置に対して上記コンテンツ鍵入手が完了した旨の表示を行ってユーザに知らせる。

【0122】その後、上記プレーヤ1から返送された上記暗号化されたメッセージを、ステップST90にて、管理センタ211に送付する。

【0123】以上により、コンテンツ鍵・使用条件入手時のユーザ端末50における処理の流れが終了する。

【0124】次に、コンテンツ鍵・使用条件入手時の管理センタ211における処理の流れを、図18を用いて説明する。

【0125】この図18において、管理センタ211のユーザ端末との通信機能部133は、ステップST91にて、前記図16のステップST74及び図17のステップST85のようにユーザ端末50にてを介してプレーヤ1から送信されてきたコンテンツID、ユーザID、メッセージ、セキュリティIDの暗号化データを受信する。この受信したデータは、ユーザ管理機能ブロック110に送られる。

【0126】当該ユーザ管理機能ブロック110のコントロール機能部111は、上記受信した暗号化データに付加されたユーザIDに基づいて、当該暗号化を解くための共通鍵をデータベース部112から取り出し、通信文暗号・復号機能部114ではこの共通鍵を用いて上記暗号化データを復号する。また、コントロール機能部111は、データベース部112から読み出したユーザIDとセキュリティID発生機能部116からのセキュリティIDとを用いて、上記受信して復号化したデータの正当性を確認する。

【0127】なお、この時の共通鍵は、前記プレーヤ1から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、前述同様に当該管理センタ211において、上記管理センタ211の公開鍵暗号方式の秘密鍵が取り出され、当該通信文暗号・復号機能部114にて上記暗号化されているセッション鍵が当該秘密鍵を用いて復号化される。このようにして得られたセッション鍵（共通鍵）が上記データベース部112に格納されている。

【0128】上記受信したデータの正当性を確認すると、コントロール機能部111は、コンテンツ管理機能ブロック100に対して上記コンテンツIDにて指定されたコンテンツ鍵と使用条件を要求し、当該要求を受けたコンテンツ管理機能ブロック100のコントロール機能部101は、上記コンテンツIDにて指定されたコンテンツ鍵と使用条件とをデータベース部102から読み出してユーザ管理機能ブロック110に転送する。コントロール機能部111は、ステップST93に示すように、これらコンテンツ鍵と使用条件はセキュリティIDと共に通信文暗号・復号機能部114に送る。

【0129】ここで、コンテンツ鍵については前述した公開鍵暗号方式にて暗号化がなされ、使用条件及びセキ

ュリティIDについては前述した共通鍵暗号方式にて暗号化がなされる。したがって、当該コンテンツ鍵を暗号化する時には、前記データベース部112からユーザ側200の公開鍵（プレーヤ1に対応して予め格納されている公開鍵）が上記ユーザIDに基づいて取り出されて通信文暗号・復号機能部114に送られる。当該通信文暗号・復号機能部114では、上記公開鍵を用いて上記コンテンツ鍵を暗号化する。一方、上記使用条件及びセキュリティIDを暗号化する時には、上記データベース部112から上記ユーザIDで指定された共通鍵（セッション鍵）が取り出されて通信文暗号・復号機能部114に送られる。このときの通信文暗号・復号機能部114では、上記使用条件及びセキュリティIDを上記共通鍵を用いて暗号化する。

【0130】上記暗号化されたコンテンツ鍵と使用条件及びセキュリティIDは、管理機能ブロック130に送られ、ステップST94のように、ユーザ端末との通信機能部133からユーザ端末50に送信される。このユーザ端末50に送信されたデータは、前記図17のステップST87及び図16のステップST75のようにユーザ端末50を介してプレーヤ1に送付されることになる。

【0131】その後、管理センタ211は、前記図16のステップST79及び図17のステップST90のようにプレーヤ1にて生成されてユーザ端末50を介して送信された暗号化メッセージの受信を待ち、ステップST95のように上記通信機能部133が上記プレーヤ1が生成した暗号化メッセージを受信すると、当該管理センタ211は、ステップST96のように、当該暗号化メッセージを共通鍵で復号化し、その復号メッセージから上記プレーヤ1がコンテンツ鍵と使用条件を入手したことを確認する。

【0132】以上により、コンテンツ鍵・使用条件入手時の管理センタ211における処理の流れが終了する。

【0133】上述した図16から図18の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図19に示すように表すことができる。

【0134】すなわちこの図19において、コンテンツ指定情報転送T21では、前記図17のステップST83のように、ユーザ端末50からプレーヤ1に対して、前記コンテンツ指定情報が転送される。作成データ転送T22では、前記のステップST74のように、プレーヤ1にて作成されたデータがユーザ端末50に転送される。作成データ転送T23では、当該ユーザ端末50から上記プレーヤ1にて作成されたデータが管理センタ211に転送される。暗号化されたデータ送付T24では、前記図18のステップST94のように、管理センタ211にて暗号化されたデータがユーザ端末50に送付され、さらに、暗号化されたデータ送付T25では、

当該暗号化されたデータがプレーヤ1に送付される。

【0135】メッセージ転送T26では、前記図16のステップST79のように、コンテンツ鍵入手完了を示すメッセージを暗号化したデータがプレーヤ1からユーザ端末50に転送され、さらに暗号化されたデータ送付T27では、上記プレーヤ1からの暗号化されたメッセージが、ユーザ端末50から管理センタ211に送付される。

【0136】次に、上述したようにしてポイント情報とデジタルコンテンツとコンテンツ鍵とを受け取ったプレーヤ1において、ユーザ端末50を用いてデジタルコンテンツを実際に鑑賞する際の処理の流れについて、図2を参照しながら図20を用いて説明する。

【0137】ここで、プレーヤ1の端子4には、前記デジタルコンテンツが記憶された記憶メディアが接続されているとする。

【0138】この状態で、ステップST101のように、当該プレーヤ1に対して、ユーザ端末50から鑑賞を希望するデジタルコンテンツが指定される。このとき、当該指定は、例えばユーザ端末50をユーザが操作することによりなされる。

【0139】このとき、プレーヤ1のコントローラ16は、ステップST102のように、上記ユーザ端末50からのコンテンツ指定情報に応じて、上記記憶メディアに対するアクセスを行い、コンテンツのIDを読み取る。

【0140】上記コントローラ16は、ステップST103のように、上記記憶メディアから読み取ったコンテンツIDに基づき、前記共通鍵保管メモリ22に対してアクセスを行い、コンテンツ鍵が格納されているかどうかを確認すると共に、前記ポイント使用情報格納メモリ29に対してアクセスを行い、使用条件が格納されているかどうかを確認する。

【0141】ここで、上記共通鍵保管メモリ22やポイント使用情報格納メモリ29内に、上記コンテンツ鍵と使用条件が格納されていないことを確認したとき、コントローラ16は、ユーザ端末50に対して当該コンテンツ鍵等が存在しない旨の情報を送り、これによりユーザ端末50からは上記コンテンツ鍵等の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合は、前述したコンテンツ鍵入手用のフローチャートのようにしてコンテンツ鍵等を入手する。このように、新たにコンテンツ鍵等を入手した場合には、ステップST104にて前述したように、その暗号化されているコンテンツ鍵等を復号化する。

【0142】次に、コントローラ16は、ステップST105に示すように、上記復号化された使用条件を元に、ポイント情報格納メモリ28に格納されているポイント情報の残高が足りているかどうかを確認する。上記ポイント情報格納メモリ28に格納された上記ポイント

情報の残高が足りないときには、コントローラ16からユーザ端末50に対して当該ポイント情報の残高が足りない旨の情報が送られ、これによりユーザ端末50は、上記ポイント情報の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合、前述したようなポイント情報入手用のフローチャートのようにしてポイント情報を入手する。

【0143】ここで、実際にデジタルコンテンツの鑑賞を行うとき、コントローラ16は、ステップST106のように、当該鑑賞するデジタルコンテンツに応じて上記ポイント情報格納メモリ28からポイント情報数を減額し、さらに当該ポイント情報の使用状態に応じた新たなポイント使用情報を、ポイント使用情報格納メモリ29に格納する（ポイント使用情報の更新を行う）。このようにポイント使用情報格納メモリ29に対して新たに格納されるポイント使用情報としては、上記鑑賞したデジタルコンテンツに対応する権利者情報（著作権者等）と減額されたポイント情報数の情報その他の情報などである。

【0144】その後、コントローラ16は、ステップST107のように、これらポイント情報の減額やポイント使用情報の新たな格納等の課金用処理が完了したことを確認すると、記憶メディアからデジタルコンテンツを読み出す。

【0145】この記憶メディアから読み出されたデジタルコンテンツは暗号化されているため、コントローラ16は、ステップST109のように、上記暗号化されたデジタルコンテンツを共通暗号復号回路24に転送する。

【0146】この共通暗号復号回路24では、ステップST110のように、コントローラ16からの指示に基づいて、先に復号化して共通鍵保管メモリ22に保管されているコンテンツ鍵を用いて、上記暗号化されているデジタルコンテンツの復号化を行う。

【0147】また、このデジタルコンテンツは前述したように所定の圧縮処理がなされているため、コントローラ16は、ステップST111のように、上記暗号が復号化された上記圧縮処理されているデジタルコンテンツを、上記共通暗号復号回路24から伸長回路26に転送させ、ここで上記所定の圧縮処理に対応する伸長処理を行わせる。

【0148】その後、当該伸長されたデジタルコンテンツは、ステップST112のように、D/A変換回路27にてアナログ信号に変換され、ステップST113のように、集積回路10の端子13と当該プレーヤ1のアナログ出力端子2とを介して外部（例えばユーザ端末50等）に出力される。

【0149】以上により、コンテンツ鑑賞時のプレーヤ1における処理の流れが終了し、ユーザはデジタルコンテンツの鑑賞が可能となる。

【0150】次に、上述したようなデジタルコンテンツの鑑賞に伴って前記プレーヤ1のポイント使用情報格納メディア29に新たに格納されたポイント使用情報を、管理センタ211に返却する際の、プレーヤ1、ユーザ端末50、管センタ310における処理の流れについて、図2と図3を参照しながら、図21から図24を用いて説明する。

【0151】図21には、ポイント使用情報返却時のプレーヤ1における処理の流れを示している。

【0152】この図21において、コントローラ16は、ステップST121に示すように、ユーザ端末50に予めインストールされているポイント使用情報返却用のソフトウェアの立ち上げが行われるまで待つ。

【0153】上記ユーザ端末50の上記ポイント使用情報返却用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末50に入力された情報が、ステップST122のように、前記PC用インターフェース端子3及び集積回路10の端子12を介して受信される。このときの上記ユーザ端末50から供給される入力情報は、ユーザにより入力されるパスワード等である。

【0154】このコンテンツ指定情報を上記ユーザ端末50から受信したコントローラ16は、ステップST123にて、当該ユーザ端末50から供給されたパスワードと、パスワード格納メモリ14に格納されているパスワードとを比較して、当該パスワードが正しいかどうかの確認をする。

【0155】上記パスワードの確認において正しいパスワードであると確認されたとき、コントローラ16は、ステップST124のように、ポイント情報格納メモリ28に格納されているポイント情報の残高と、ポイント使用情報格納メモリ29に格納されているポイント使用情報とをそれぞれ読み出し、これら情報を暗号化する。

【0156】上記ポイント情報の残高とポイント使用情報の暗号化が終了すると、コントローラ16は、ステップST125のように、ユーザID格納メモリ23からユーザIDを読み出して上記暗号化したデータに添付する。

【0157】このユーザIDが添付されたデータは、ステップST126のように、コントローラ16から端子12及びPC用インターフェース端子3を介してユーザ端末50に転送される。このデータはその後管理センタ211に転送される。

【0158】なお、このときの暗号化にも前述したように共通鍵暗号方式が採用されている。すなわち、当該データの伝送に先立ち、前述同様に共通鍵の生成が行われ、この生成された共通鍵が前記公開鍵暗号方式にて暗号化(管理センタ211の公開鍵を用いた暗号化)され、ユーザIDと共に管理センタ211に送られている。

【0159】上述のようにしてユーザ端末50にデータ

を転送した後、コントローラ16は、上記管理センタ211から後述するデータがユーザ端末50を介して転送されてくるのを待つ。

【0160】ここで、ステップST127のように上記管理センタ211からのデータを受信すると、プレーヤ1では、ステップST127のように、共通鍵暗号方式を使用して暗号化されている受信データを、前述同様に共通鍵を用いて復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ16は、上記復号化されたデータのセキュリティIDを、上記セキュリティID発生回路19からのセキュリティIDとの比較によって確認することによる正当性の評価を行う。

【0161】また、上記管理センタ211から転送されてくるデータには、上記共通鍵を用いて暗号化された処理完了のメッセージも含まれている。したがって、上記セキュリティIDの確認が終了した後のコントローラ16は、上記暗号化された処理完了メッセージを共通暗号復号回路24に送り、ここで共通鍵を用いた復号化を行わせ、この復号化した処理完了メッセージを受け取ることで、上記管理センタ211での処理が完了したことを確認する。

【0162】以上により、ポイント使用情報返却時のプレーヤ1における処理の流れが終了する。

【0163】次に、ポイント使用情報返却時のユーザ端末50における処理の流れを、図22を用いて説明する。

【0164】この図22において、ユーザ端末50は、ステップST131にて、ポイント使用情報返却用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末50では、ステップST132にて、上記ソフトウェアに従い当該ユーザ端末50を操作するユーザに対して、パスワード等の入力要求を行い、ユーザからパスワードの入力がなされると、そのパスワードをプレーヤ1に転送する。

【0165】次に、ユーザ端末50は、ステップST133にて、前記図21のステップST126のように上記プレーヤ1にて作成されて転送されたデータを受信すると、ステップST134にて、当該プレーヤ1から転送されたデータを、予めアドレスが登録されている管理センタ211へ転送する。

【0166】上記管理センタ211に対してデータの転送を行った後のユーザ端末50は、管理センタ211からの返送を待ち、ステップST135にて、管理センタ211からプレーヤ1に対して送られるデータを受信すると、当該データをそのままプレーヤ1に転送する。

【0167】上記プレーヤ1に対してデータの転送を行った後のユーザ端末50は、処理が完了した旨をユーザに知らしめるための表示をディスプレイ装置に行い、ユーザからの確認を受ける。

【0168】以上により、ポイント使用情報返却時のユ

ーザ端末50における処理の流れが終了する。

【0169】次に、ポイント使用情報返却時の管理センタ211における処理の流れを、図23を用いて説明する。

【0170】管理センタ211のユーザ端末との通信機能部133において、ステップST141のように、前記図21のステップST126及び図22のステップST134によって前記ユーザ端末50を介してプレーヤ1から送信されてきたポイント使用情報等のデータを受信する。

【0171】このデータを受信すると、管理センタ211のユーザ管理機能ブロック110は、ステップST142のように、コントロール機能部111の制御の元で、当該受信したデータに添付されたユーザIDに基づいて、データベース部112から前述同様に予め受け取って格納している共通鍵を入手すると共にセキュリティIDを入手する。

【0172】上記データベース部112から上記ユーザIDに対応する共通鍵とセキュリティIDを入手すると、ステップST143に示すように、管理センタ211のユーザ管理機能ブロック110の通信文暗号／復号機能部114において、上記共通鍵を用いて、上記プレーヤ1からの上記暗号化されたポイント使用情報等のデータの復号化を行い、さらにコントロール機能部111において、当該復号化したデータ中のセキュリティIDと上記データベース部112から読み出したセキュリティIDとの比較によって、アクセスしてきたユーザ側200（プレーヤ1）が正当な使用者であるかどうかの内容確認を行う。

【0173】上記正当性と内容の確認後のデータは、使用情報管理機能ブロック120に転送される。この使用情報管理機能ブロック120のコントロール機能部121は、ステップST144に示すように、上記プレーヤ1から送られてきたポイント情報の残高とポイント使用情報とを用い、データベース部122に格納されている情報を用いて上記ユーザ側200の使用に不正がないかどうかの確認を行う。同時に、当該不正なきことを確認した場合には、使用情報演算機能部123においてポイント情報の残高とポイント使用情報をまとめる演算を行う。

【0174】その後、ステップST145に示すように、ユーザ管理機能ブロック110のコントロール機能部111は、セキュリティID発生機能部116を制御してセキュリティIDを算出させ、さらに確認メッセージ発生機能部115を制御して処理完了のメッセージを生成させる。これらセキュリティIDと処理完了メッセージは、ユーザ管理機能ブロック110の通信文暗号／復号機能部114にて前記共通鍵を用いて暗号化される。

【0175】上記暗号化されて生成されたデータは、ス

テップST146に示すように、ユーザ端末との通信機能部133からユーザ端末50に送られ、前記図22のステップST135と図21のステップST127のように当該ユーザ端末50からプレーヤ1に転送されることになる。

【0176】以上により、ポイント使用情報返却時の管理センタ211における処理の流れが終了する。

【0177】上述した図21から図23の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図24に示すように表すことができる。

【0178】すなわちこの図24において、入力情報転送T31では、前記図22のステップST132のように、ユーザ端末50からプレーヤ1に対して、前記パスワード等の入力情報が転送される。作成データ転送T32では、前記図21のステップST126のように、プレーヤ1が作成したデータがユーザ端末50に転送される。作成データ転送T33では、前記図22のステップST134のように、上記プレーヤ1にて作成されたデータが上記ユーザ端末50から管理センタ211に転送される。データ転送T34では、前記図23のステップST146のように、管理センタ211にて作成されたデータが、ユーザ端末50に転送される。データ転送T35では、前記図21のステップST127のように、管理センタ211にて作成されたデータがユーザ端末50を介してプレーヤ1に転送される。

【0179】本実施の形態のシステムのプレーヤ1とユーザ端末50と管理センタ211の実際の動作は、上述したような流れとなる。

【0180】ここまでは、本実施の形態のシステムにおける全体の処理の流れを説明してきたが、これ以降は、本実施の形態のシステムの主要部の個々の動作を詳細に説明する。

【0181】まず、本発明実施の形態における暗号化及び圧縮と、伸長及び復号化の動作についての説明を行う。

【0182】上述した実施の形態のシステムのように、ネットワークを使ってデジタルコンテンツを配信する際には、そのデータ量を抑えるために圧縮／伸長技術を使用し、コピー防止或いは課金のために暗号化／圧縮技術が使われる。すなわち、配信側（上述の例では管理センタ211側）でデジタルコンテンツを圧縮し、さらに暗号化処理することが行われる。上述の例のように送信側（管理センタ211側）にて生成されたデジタルコンテンツ（暗号化／圧縮データ）をネットワークを使って配信するとき、受信側（上述の例ではプレーヤ1）では上記暗号化及び圧縮されたデジタルコンテンツを受信後に復号化し、さらに伸長してデジタルコンテンツを復元することが行われる。なお、上記暗号化と圧縮、復号化と伸長の処理の順番は入れ替わる場合もあ

る。

【0183】上記デジタルコンテンツに著作権等が存在する場合、上記受信側は、上記デジタルコンテンツを上記復号化と伸長する際に、上記著作権者等の意思に従い、課金されることになる。この課金は、主として復号化の鍵すなわちコンテンツ鍵を購入することにより行われるが、このコンテンツ鍵を購入する方法には種々ある。

【0184】ここで、上述したように、デジタルコンテンツを圧縮して暗号化し、復号化して伸長するような処理手順に従った場合、例えば悪意を持ったユーザは上記復号化済みの圧縮データを比較的簡単に入手することができることになる。すなわちデジタルコンテンツの圧縮データは、一般に容量が大きく、したがって例えば受信側の一般的なコンテンツ再生装置の内部メモリではなく、安価が外部メモリに蓄積される場合が多いため、この外部メモリから直接、或いは外部メモリとの接続部分で上記圧縮されたデジタルコンテンツを不正に取り出すことが容易だからである。

【0185】また、圧縮に対する伸長方式のアルゴリズムは公開されている場合が多く、また伸長方式のアルゴリズムには一般的な暗号の鍵のようにそれぞれ隠しておけば処理できないようなものも存在していない。しかも、上記復号化された圧縮デジタルコンテンツは、上記送信側から配信された暗号化と圧縮とがなされたデジタルコンテンツと比較して、データ量的に変わず、したがって、上記復号化された圧縮デジタルコンテンツを悪意を持って配信するのも容易である。すなわち、上記圧縮した後に暗号化されてデジタルコンテンツを配信する方式によると、誰でも容易に伸長できる圧縮デジタルコンテンツが、悪意を持ったユーザに容易に盗難され、このため著作権者等の意思の届かないところでさらに配信されたり、伸長されたりする危険性が大きい。

【0186】そこで、本発明の実施の形態では、このような状況に鑑み、ネットワークを使って配信するデジタルコンテンツの安全性を向上させることを可能にするため、上記図2のプレーヤ1において、以下の図25のフローチャートに示すような処理を行っている。

【0187】すなわち図2のプレーヤ1の共通暗号復号回路24における復号化処理と上記伸長回路26における伸長処理では、前記記憶メディアから読み出された暗号化と圧縮処理されたデジタルコンテンツのデータを、ステップST151のように、先ず、復号化処理のアルゴリズムの処理単位Xビットと、伸長処理のアルゴリズム処理単位Yビットとの最小公倍数 $l\text{cm}(X, Y)$ の単位に分割する。

【0188】次に、上記最小公倍数 $l\text{cm}(X, Y)$ の単位に分割された上記暗号化と圧縮処理がなされているデジタルコンテンツのデータは、ステップST152

に示すように、当該最小公倍数 $l\text{cm}(X, Y)$ の単位毎に、上記共通暗号復号回路24にて復号化処理が行われる。

【0189】当該復号化処理により得られた最小公倍数 $l\text{cm}(X, Y)$ の単位の圧縮されているデジタルコンテンツのデータは、ステップST154に示すように、当該単位分の全ての圧縮データに対して上記伸長回路26にて伸長処理が行われる。

【0190】その後、この最小公倍数 $l\text{cm}(X, Y)$ の単位毎の復号化及び伸長処理は、上記暗号化と圧縮処理されたデジタルコンテンツの全データについての処理が終了するまで続けられる。すなわち、ステップST155に示すように、最小公倍数 $l\text{cm}(X, Y)$ の単位毎の復号化及び伸長処理がデジタルコンテンツの全データに対して完了したか否かの判断がなされ、完了していない時にはステップST152に戻り、完了したときに当該処理のフローチャートが終了する。

【0191】これにより全データの復号化及び伸長されたデジタルコンテンツが得られることになる。

【0192】なお、当該プレーヤ1における図25のフローチャートの処理でも、上記最小公倍数 $l\text{cm}(X, Y)$ 単位の復号化データは存在することになるが、当該復号化データのデータ量は少ない。このため、比較的高価でも安全性の高い内部メモリに保存することができるようになり、したがって前述したような外部メモリに保存する場合のように盗まれる可能性は非常に低いものとなる。

【0193】また、本実施の形態における上記プレーヤ1では、上記安全性を確保するための内部メモリとして、図2のバッファメモリ25が上記共通暗号復号回路24と伸長回路26との間に設けられている。すなわちこのバッファメモリ25は、1チップの集積回路10内に設けられており、外部からアクセスされ難く、したがってデータが外部に取り出されることはない。

【0194】上述のフローチャートでは、最小公倍数 $l\text{cm}(X, Y)$ の単位分の全てのデータに対して復号化及び伸長処理を行うようにしており、このための具体的な構成としては、例えば図26に示す構成のように、最初に復号化処理のアルゴリズムの処理単位Xビットにデジタルコンテンツのデータを分割し、このXビットのデータに復号化処理を施し、その後当該復号化処理されたXビットの圧縮されているデータを、伸長処理のアルゴリズム処理単位Yビット分まとめ、当該Yビットの圧縮データを伸長することで、上述のように最小公倍数 $l\text{cm}(X, Y)$ の単位での復号化及び伸長処理を実現するようにしている。

【0195】このことを実現するプレーヤ1の共通暗号復号回路24は、入力部30と暗号復号部31とからなり、上記伸長回路26は、伸長部32と出力部33とからなる。これら共通暗号復号回路24と伸長回路26の

間に前記バッファメモリ25が設けられている。

【0196】ここで、より具体的な例として、上記デジタルコンテンツに対する暗号化処理が例えばDES(Data Encryption Standard)暗号を用いて行われているのであれば、当該暗号化処理とそれに対応する復号化処理は、64ビット単位で行われることになる。

【0197】また、圧縮されたデジタルコンテンツに対する伸長処理の場合、その圧縮率やサンプリング周波数によっても異なるが、現状では1K~2Kビット/チャンネル単位で処理される場合が多い。ここでは、便宜的に1.28Kビット毎に処理されると仮定する。

【0198】したがって、上記DES暗号化方式と上記1.28Kビット毎の圧縮伸長方式を用いたシステムの場合、上記最小公倍数lcmは1.28Kとなる。

【0199】このような条件のもと、図26の共通暗号復号回路24の入力部30には、前記暗号化されて圧縮されたデジタルコンテンツが入力される。当該入力部31では、上記暗号化されて圧縮されたデジタルコンテンツを、上記復号化処理のアルゴリズムの処理単位Xビット、すなわち64ビットづつのデータに分割して暗号復号部31に出力する。

【0200】この暗号復号部32では、上記Xビットすなわち64ビットのデータを、当該64ビット毎に復号化処理する。この64ビット毎の復号化により得られた64ビットの圧縮されているデータは、バッファメモリ25に送られる。

【0201】当該バッファメモリ25は、前記コントローラ16からの指示に従い、伸長処理のアルゴリズム処理単位Yビット、すなわち1.28Kビット分の圧縮データがたまった時点で、当該1.28Kビット分の圧縮データを一括して出力し、この圧縮データが上記伸長回路26の伸長部32に送られる。

【0202】上記伸長部26は、上記入力された1.28Kビット分の圧縮データを伸長して出力部33に出力する。

【0203】また、コントローラ16は、バッファメモリ25にたまったデータ量をモニタしながら、復号化部31の処理と伸長部32の処理をコントロールする。

【0204】なお、このケースであれば、復号化処理を20個(=1280/64)並列で処理すれば、より高速な処理システムになる。

【0205】その他、前記図2や図26のようなハードウェア構成ではなく、プログラマブルデバイスにて上述した処理を行う場合には、バッファメモリ25の状況に応じて、例えばコントローラ16が復号化プログラム或いは伸長プログラムに基づいて処理を行うことになる。

【0206】上述の説明では、圧縮した後に暗号化したデジタルコンテンツがプレーヤ1に供給され、プレーヤ1ではこの圧縮及び暗号化されたデジタルコンテンツを復号化した後に伸長する例を挙げたが、暗号化した

後に圧縮されたデジタルコンテンツを伸長して復号化する場合であっても、上述同様の効果を得ることができる。

【0207】また、本発明は、圧縮/伸長並びに暗号化/復号化のアルゴリズムが限定されることはなく、いかなる方式に対しても有効である。

【0208】このように、本発明によれば、ネットワークを使って配信するデジタルコンテンツの安全性が向上する。

【0209】次に、前記セキュリティIDの発生動作についての説明を行う。

【0210】本実施の形態のように、ポイント情報を予め入手しておき、デジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、前述したように、ネットワーク上の管理センタ211は、ユーザ側200のユーザ端末50からのポイント情報の購入依頼の通信を受けた後に、金融機関220その他と任意の確認を行った後、そのポイント情報を暗号化して、ユーザ側200のプレーヤ1にネットワーク経由で送る。

【0211】本実施の形態のように、ポイント情報を予め入手しておき、デジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、管理センタ211とプレーヤ1(ユーザ端末50)との間で、ポイント情報の購入の度に、毎回同じようなデータのやり取りを行う(例えば暗号化された「3000円分のポイント情報の補充要求」及びそれに対応した「3000円分のポイント情報」といった情報のやり取りを行う)と、例えば悪意を持つ者による、金融機関220へのいわゆる「成り済まし」による金額補充が問題点となる。なお、ここに言う金融機関への「成り済まし」とは、上記悪意を持った者が本来のユーザ(本実施の形態ではユーザ側200)に成り済まして、不正にポイント情報を入手するようなことを言う。

【0212】すなわち、ポイント情報の購入の度に毎回同じようなデータのやり取りを行っている、例えば悪意を持った者が当該データを通信回線から盗み出して同じデータを生成し、管理センタ211に対して送り先を自分(悪意を持った者)にしてポイント情報の入手を依頼したような場合、当該悪意を持った者がポイント情報を入手できることになり、さらにこのポイント情報の購入代金の請求は本来のユーザ側200になされることになるという問題が発生するおそれがある。

【0213】そこで、こういった不正を防止するために、本発明実施の形態のシステムでは、予め受信側(プレーヤ1側)と配信側(管理センタ211側)の両者で連動している乱数発生機能により発生させられた乱数を安全性向上のために使用している。本実施の形態では、上記乱数として前記セキュリティIDを発生している。なお、両者間で乱数発生を連動させるには、例えばユーザの登録手続きなどの際に、例えばタイマ18を初期化



するなどして、両者間の動作を同期させれば良い。

【0214】すなわち、この乱数（セキュリティID）を用いた場合の管理センタ211からプレーヤ1への例えばポイント情報入手時の動作は、以下のような流れとなる。

【0215】ポイント情報の購入時、管理センタ211からプレーヤ1に対して送られるデータは、前述したように例えばプレーヤ1から予め入手した共通鍵（セッション鍵）を用いて暗号化されたポイント情報と上記発生されたセキュリティIDからなるデータとなされる。

【0216】プレーヤ1のコントローラ16は、当該管理センタ211から受け取ったデータを前述したように共通暗号復号回路24に送り、ここで前記共通鍵を用いて復号化処理を行う。これにより、管理センタ211から送られてきたポイント情報とセキュリティIDとが得られることになる。

【0217】その後、プレーヤ1のコントローラ16は、上記管理センタ211から送られてきたセキュリティIDと、自身のセキュリティID発生回路19にて発生したセキュリティIDとを比較する。この比較において、コントローラ16は、管理センタ211からのセキュリティIDと、上記自身が発生したセキュリティIDとが一致したときのみ、上記管理センタ211から送られてきたポイント情報を、前記ポイント情報格納メモリ28に格納する。

【0218】これにより、正当なユーザ側200のプレーヤ1のみがポイント情報を入手できることになる。言い換えれば、正当なユーザ側200のプレーヤ1と同じようなプレーヤを持っている悪意の者が、前記成り済ましによって不正にポイント情報を入手しようとしても、当該悪意の者が持っているプレーヤのセキュリティIDと上記管理センタ211から送られてきたセキュリティIDとは一致しないため、この悪意を持った者は前記成り済ましによる不正なポイント情報入手ができないことになる。

【0219】勿論、ユーザ側200のプレーヤ1で発生するセキュリティIDは、当該プレーヤ1の集積回路10内に設けられたセキュリティID発生回路19によって発生されるものであり、外部には取り出せないものであるため、悪意を持った者が当該セキュリティIDを盗むことはできない。

【0220】上記セキュリティIDとしての乱数を発生する構成には種々のものがあるが、その一例を図27に示す。この図27の構成は、前記図2のセキュリティID発生回路19の一具体例である。

【0221】この図27において、一方向関数発生部40は、いわゆる一方向性関数を発生する。なお、上記一方向性関数とは、比較的計算が簡単な関数で逆関数があるかに計算が困難なものである。この一方向関数は、予め秘密通信等で受け取って当該一方向関数発生部40に

保存しておくことも可能である。なお、一方向関数発生部40は、前記図2の集積回路10内に設けられたタイマ18からの時間情報を入力関数として上記一方向関数を発生するようにすることも可能である。上記一方向関数は、乱数決定部43に送られる。

【0222】また、ユーザ定数発生部41は、ユーザ毎に定められた所定のユーザ定数を発生する。このユーザ定数は、予め秘密通信等で送付されて当該ユーザ定数発生部41に保存されるものである。なお、このユーザ定数は、例えば前記ユーザID格納メモリ23が格納するユーザIDを用いることもできる。

【0223】乱数データベース42は、乱数を格納するものであり、例えば99個の乱数を格納している。

【0224】通信回数記憶部44は、例えばコントローラ16から送られてくる通信回数情報を記憶するものである。この通信回数情報とは、プレーヤ1と管理センタ211との間の通信回数を示す情報である。

【0225】これら一方向関数とユーザ定数と通信回数情報は、乱数決定部43に送られる。当該乱数決定部43は、例えば前記タイマ18からの時間情報に基づき、上記一方向関数とユーザ定数から、予め乱数データベース部42に記憶された範囲の乱数を発生させる（例えば99個）。

【0226】すなわち、この乱数決定部43では、上記通信回数情報が例えば1回目の通信であれば、99個目の乱数を上記乱数データベース部42から取り出し、また例えば通信回数情報がn回目の通信であれば100-n個目の乱数を上記乱数データベース部42から取り出し、この取り出した乱数を前記セキュリティIDとして出力する。

【0227】このセキュリティID発生の構成は、プレーヤ1と管理センタ211とで同じものを有している。

【0228】なお、乱数データベース部42に格納している全ての乱数を使い終わったときには、上記乱数決定部42において100個～199個目の乱数を計算するか、或いは新たな乱数や1方向性関数を秘密通信するなどして、乱数データベース部42に再格納したり、一方向性関数発生部40に再構築する。

【0229】また、上述した説明では、乱数（セキュリティID）を発生させて通信毎の安全性を高めるようにしているが、本実施の形態では、前述のようにユーザ側200と管理センタ211側との間で通信を行う毎に、毎回異なる共通鍵（セッション鍵）をプログラムブルに発生させるようにもしているため、さらに安全性が高められている。

【0230】ここで、実際に送信される送信文（例えばメッセージ等）について上記乱数が挿入されると共に、セッション鍵による暗号化がなされる様子と、受信文から乱数が取り出されて正当性の確認がなされる様子を図28と図29を用いて説明する。なお、これら図28、

図29の例では、送信文に署名（デジタル署名）を付加するようにもしている。

【0231】この図28において、先ず、前記共通鍵を公開鍵暗号方式にて暗号化して送信する流れとして、通信用共通鍵発生工程P7では前記セッション鍵を通信用に用いる共通鍵として発生し、この共通鍵は公開鍵暗号化工程P8にて受信側の公開鍵で暗号化される。この暗号化された共通鍵は、受信側に送られる。

【0232】一方、送信文としてのメッセージを共通鍵暗号方式にて暗号化して送信する場合の流れとして、例えばメッセージ生成行程P1ではメッセージMが生成されると共に、乱数発生工程P5にて乱数（前記セキュリティID）が発生される。これらメッセージMと乱数は、共通鍵暗号化工程P6に送られる。この共通鍵暗号化工程P6では、上記通信用共通鍵発生工程P7にて発生した共通鍵を用いて、上記メッセージMと乱数を暗号化する。

【0233】さらに、上記デジタル署名を付加する場合、上記メッセージMはハッシュ値計算工程P2に送られる。当該ハッシュ値計算工程P2では、上記メッセージMからいわゆるハッシュ値が計算される。なお、ハッシュ値とはハッシュ法にて求められるアドレス情報であり、ハッシュ法とはデータ（この場合はメッセージM）の内容の一部（キーワード）に所定の演算を施し、その結果をアドレスとして使用するものである。このメッセージから生成されたハッシュ値（M）はデジタル署名として、秘密鍵暗号化工程P4に送られる。この秘密鍵暗号化工程P4では、送信側の秘密鍵で上記デジタル署名を暗号化する。この暗号化されたデジタル署名は、共通鍵暗号化工程P6に送られる。これにより共通鍵暗号化工程P6では、上記通信用共通鍵発生工程P7にて発生した共通鍵を用いて、上記デジタル署名を暗号化する。

【0234】これらメッセージMとデジタル署名と乱数が受信側に送信される。

【0235】次に、図29を用いて、図28に対応する受信側での処理の流れを説明する。

【0236】この図29において、先ず、前記共通鍵を公開鍵暗号方式にて復号化する流れとして、秘密鍵復号化工程P11では、上記送信側から送信されてきた共通鍵を当該受信側の秘密鍵で復号化する。

【0237】一方、前記共通鍵暗号方式にて暗号化されたメッセージMを復号化する流れとして、共通鍵復号工程13では、上記送信されてきたメッセージMを上記秘密鍵復号化工程P11にて復号化した共通鍵を用いて復号化する。この復号化されたメッセージMは、他機能送信工程P20にて他の工程に送られることになる。

【0238】また、デジタル署名を復号する流れでは、上記共通鍵復号化工程P13にて復号化されたハッシュ値が、公開鍵復号化工程P14にて送信側の公開鍵

を用いて復号化される。同時に、ハッシュ値計算工程P17では、上記メッセージMからハッシュ値を計算する。これら公開鍵復号化工程P14により復号化されたハッシュ値と上記ハッシュ値計算工程P17にて計算されたハッシュ値とは、比較工程P19にて比較され、改竄されていないことの確認が行われる。

【0239】さらに、送信された乱数については、上記共通鍵復号化工程P13にて復号化された乱数と、当該受信側の乱数発生工程P21にて発生された乱数とが、正当正確確認工程P22にて比較され、正当性の確認が行われる。

【0240】ところで、前述した図1に示した本実施の形態のシステムでは、ユーザ側200に対するシステム側として、システム管理会社210と仮想店舗230とコンテンツプロバイダ240とが設けられている。なお、図1の金融機関220は、例えば外部の銀行等である。

【0241】上記システム管理会社210の管理センタ210は、仮想店舗230におけるデジタルコンテンツの展示や配信の管理、金融機関220との間でユーザ側200の課金情報や各種情報の収集、分配及びそれらの管理、コンテンツプロバイダ240からのデジタルコンテンツの暗号化、扱う情報のセキュリティ管理など、システム側の主要な作業のほぼ全てを行っている。

【0242】しかし、上述したようなネットワークを使ってデジタルコンテンツを配信するシステムにおいて、ユーザ側がシステム側からデジタルコンテンツを入手する際や、デジタルコンテンツの使用に伴う課金の際には、システム側に通信が集中することになり、ユーザ側に対して満足のいくレスポンスが得られなくなるおそれがある。

【0243】そこで、本発明の他の実施の形態では、システム管理会社210の機能、より具体的には管理センタ211の機能を、以下のように分割することで、上述したような通信の集中を防ぎ、通信のレスポンスを向上させることを可能にしている。

【0244】すなわち、本発明の他の実施の形態では、図30に示すように、ユーザ側200に対するシステム側の構成を、デジタルコンテンツを展示、配信する機能を有するコンテンツ展示配信機関310と、一定の地域のユーザの課金情報を管理する機能を有する課金情報管理機関320と、デジタルコンテンツを暗号化する等のデータ生成と上記コンテンツ展示配信機関310への生成データの配信と上記課金情報管理機関320からの情報収集と収益分配とシステム全体のセキュリティ管理その他を行う機能を有するシステム管理機関330とに分割し、各機関310、320、330がそれぞれ独立にユーザ側200と通信可能になされている。

【0245】この図30のような構成において、コンテンツ展示配信機関310は、世界中のネットワーク上に

散らばって複数配置可能なものであり、ユーザ側200は通信費さえ支払えばどの地域のコンテンツ展示配信機関310へでもアクセスできる。例えばユーザ側200がデジタルコンテンツを入手したい場合には、ユーザ側200から上記コンテンツ展示配信機関310にアクセスして、デジタルコンテンツを入手する。このときのデジタルコンテンツは、システム管理機関330によって暗号化等されたデジタルコンテンツ、すなわちユーザ側200にネットワークを使って直接送信可能な状態になされたものである。

【0246】また、課金情報管理機関320は、課金情報を扱うため、余り多くのユーザを抱え込むことは安全性管理上好ましくなく、したがって、適度な数のユーザ毎に設置する。但し、あまり多く設置すると、悪意を持った第三者からの攻撃ポイント（課金情報管理機関320）を増やすことになり、トレードオフになるので、最適化することが望ましい。例えばユーザ側200が課金に関する通信を行う場合には、ユーザ側200から上記課金情報管理機関320に対してアクセスする。

【0247】上記システム管理機関330は、ユーザのシステムへの加入や決済方法の登録、ユーザからの集金や前記権利者、コンテンツ展示配信機関310、課金情報管理機関320等の利益受益者への利益配付など、セキュリティ上重要な情報の管理をまとめて行うことで、セキュリティを向上させる。但し、当該システム管理機関330は世界に1箇所のみ設けるわけではなく、あるまとまった単位、例えば国などの単位で設置するのが望ましい。例えば、ユーザ側200がこのシステムへの加入や決済方法の登録などセキュリティ上重要な通信を行う場合には、ユーザ側200から上記システム管理機関330に対してアクセスして行う。当該ユーザからの集金と利益受益者への利益配付は上記課金情報管理機関320から情報を入手した当該システム管理機関330がまとめて行う。また、著作権者等が有するソースデータすなわちコンテンツは、当該システム管理機関330に供給され、ここで暗号化等がなされたデジタルコンテンツに変換され、上記コンテンツ展示配信機関310に配信される。

【0248】上述のように、システム側の機能を例えば3つの機関310、320、330に振り分け、ユーザ側200と各機関310、320、330との間で直接アクセス可能とすることにより、通信の集中を防ぎ、通信のレスポンスを向上させることが可能となる。また、コンテンツ展示配信機関310によれば、既存のいわゆるバーチャルモールのようなものにも対応でき、販売促進にも有効であり、ユーザにとって魅力のあるものになる。課金情報管理機関320を別に分けることにより、コンテンツの展示や販売機能と結託した不正防止に役立つ。また、管理するユーザを一定の数に抑えられるため、不正に対する管理機能もより効果的である。

【0249】以下に、上述した図30に示した本発明の他の実施の形態のシステムにおいて、ユーザのシステムへの加入、ポイント情報の購入や暗号化されたデジタルコンテンツの復号用のコンテンツ鍵等の入手時の情報の流れ、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れ、コンテンツの使用に伴う課金情報の流れについて説明する。

【0250】まず、図31を用いて、ユーザのシステムへの加入時の流れの主要部を説明する。

【0251】ユーザのシステムへの加入登録の際には、システム管理機関330のユーザ加入サポート機能ブロック402による以下の手順の従って登録作業が行われる。

【0252】ユーザ側200すなわち前記プレーヤ1及びユーザ端末50からは、先ず加入意思送付T41のように、システムへの加入の意思を示す情報が、システム管理機関330に対してネットワークを介して送付される。システム管理機関330の通信機能ブロック401に入力された上記加入意思の情報は、ユーザ加入サポート機能ブロック402に送られる。

【0253】当該ユーザ加入サポート機能ブロック402は、上記加入意思情報を受信すると、加入必要ファイル送付T42のように、加入に必要なファイルの情報を通信機能ブロック401を介してユーザ側200に送られる。

【0254】ユーザ側200では、上記システム管理機関330から送られてきた加入必要ファイルに基づいて、所定のフォーマットに従った加入申請書の作成が行われる。当該作成された加入申請書は、加入申請書送付T43のように、システム管理機関330に送付される。

【0255】上記加入申請書を受け取ったユーザ加入サポート機能ブロック402は、クライアント機能送付T44のように、クライアントの機能を解説する情報を、ユーザ側200に送付する。

【0256】当該クライアント機能の情報を受け取ったユーザ側200からは、ユーザ情報送付T45のように、ユーザ側の情報、例えば前述したような口座番号やクレジット番号、名前や連絡先等のユーザ情報を、システム管理機関330に送付する。

【0257】当該ユーザ情報の送付を受けたユーザ加入サポート機能ブロック402は、登録手続き完了通知T46のように、加入の登録手続きが完了した旨の情報を、ユーザ側200に通知する。

【0258】また、このユーザ加入登録の手続き完了後、システム管理機関330のユーザ加入サポート機能ブロック402は、ユーザ情報送付T47のように、通信機能ブロック401を介して、課金情報管理機関320に対してユーザ情報を転送する。このユーザ情報を受け取った課金情報管理機関320は、当該ユーザ情報を

データベース機能ブロック367に保存する。

【0259】以上より、ユーザのシステムへの加入時の主な流れが終了する。なお、この図31に挙げられている他の構成についての説明は後述する。

【0260】次に、図32を用いて、ポイント情報の購入や暗号化されたデジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明する。なお、上記ポイント情報の購入や暗号化されたデジタルコンテンツの復号用のコンテンツ鍵の情報は、コンテンツを使用するための情報であるので、以下の説明では、これらを簡略化して使用権情報と呼ぶことにする。

【0261】ユーザがシステムで使用する重要な情報（ここでは、コンテンツの使用権）を入手する際は、予めユーザ側200毎に担当割当がなされている課金情報管理機関320に対し、ユーザ側200からアクセスがなされる。上記ユーザ側200から送られてくるコンテンツ使用権情報の入手要求のアクセスに対しては、課金情報管理機関320の使用権発行機能ブロック362が対応し、以下の手順に従って使用権の発行が行われる。

【0262】先ず、ユーザ側200からは、購入依頼書送付T51のように、使用権を購入したい旨の情報が課金情報管理機関320に対して送付される。使用権を購入したい旨の情報は、ユーザ側200によって所定のフォーマットに従った購入依頼書の情報である。このようにネットワークを介し、この課金情報管理機関320の通信機能ブロック361に入力された上記購入依頼書の情報は、使用権発行機能ブロック362に送られる。

【0263】当該使用権発行機能ブロック362では、上記購入依頼書の情報を受け取ると、データベース機能ブロック367に保存されたユーザ情報を元にして、新しい使用権の情報を生成し、新規使用権送付T52のように、当該使用権の情報をユーザ側200に対して送付する。

【0264】ユーザ側200は、上記新規使用権の情報の受取を確認すると、所定のフォーマットに従った受取確認書を作成し、受取確認書送付T53のように、課金情報管理機関320の使用権発行機能ブロック362に送付する。

【0265】以上より、使用権の購入時の主な流れが終了する。なお、この図32に挙げられている他の構成についての説明は後述する。

【0266】次に、図33を用いて、コンテンツとコンテンツ鑑賞用の情報（ここでは使用条件とコンテンツ鍵）の流通の際の流れの主要部を説明する。

【0267】先ず、コンテンツ展示配信機関310のコンテンツ入手機能ブロック342は、コンテンツ請求書送付T62のように、システム管理機関330に対して、デジタルコンテンツを請求する。

【0268】当該コンテンツ請求書を受け取ったシステム管理機関330は、コンテンツ配布機能ブロック40

4において、要求されたコンテンツを流通できるように加工する。すなわち、このコンテンツ配布機能ブロック404では、ユーザ側200に送付可能な状態のデジタルコンテンツ（暗号化されたデジタルコンテンツ）を生成する。この加工されたデジタルコンテンツは、コンテンツ送付63のように、コンテンツ展示配信機関310に送られる。

【0269】当該コンテンツ展示配信機関310では、上記加工されたデジタルコンテンツを、コンテンツデータベース機能ブロック345に保存する。

【0270】また、システム管理機関330のコンテンツ配布機能ブロック404では、コンテンツ鑑賞用の情報として、コンテンツIDと使用条件と暗号化されたコンテンツを復号するためのコンテンツ鍵とを、コンテンツ鑑賞用情報送付T64のように、課金情報管理機関320に送付する。

【0271】課金情報管理機関320では、上記コンテンツ鑑賞用の情報を、コンテンツ鍵・使用条件受取機能ブロック363にて受取り、データベース機能ブロック367に保存する。

【0272】次に、ユーザ側200は、コンテンツ入手依頼T61のように、コンテンツ展示配信機関310に対してアクセスし、コンテンツを入手する。すなわち、コンテンツ展示配信機関310は、通信機能ブロック341を介して上記ユーザ側200からコンテンツの入手の要求がなされると、コンテンツデータベース機能ブロック354に保存している暗号化されたデジタルコンテンツを読み出し、当該読み出したデジタルコンテンツをユーザ側200の送付する。

【0273】その後、ユーザ側200は、コンテンツ鑑賞用情報請求T65にて課金情報管理機関320に対してアクセスし、コンテンツ鑑賞用情報送付T66のようにコンテンツ鑑賞用の情報を入手する。すなわち、課金情報管理機関320では、通信機能ブロック361を介して、上記ユーザ側200からコンテンツ鑑賞用の情報として使用条件とコンテンツ鍵の請求がなされると、コンテンツ鍵・使用条件発行機能ブロック364からコンテンツ鍵と使用条件とを発行し、これらを通信機能ブロック361を介してユーザ側200に送付する。

【0274】以上より、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れが終了する。なお、この図33に挙げられている他の構成についての説明は後述する。

【0275】次に、図34を用いて、コンテンツが実際に鑑賞されたときの精算、すなわちコンテンツ使用料金の精算の流れの主要部を説明する。

【0276】先ず、ユーザ側200にてコンテンツの鑑賞が行われた後、当該ユーザ側200からは、精算書送付T71のように、例えば前述のようにしてポイント使用情報すなわちコンテンツの使用記録が課金情報管理機

関320に対して送付される。このように通信機能ブロック361を介して上記ユーザ側200から上記コンテンツ使用記録の送付を受けると、課金情報管理関320の精算手続き受付機能ブロック365にて当該コンテンツ使用記録を受け取り、これに対応する精算確認書を発行する。当該精算確認書は、精算確認書送付T73のように、同じく通信機能ブロック361を介してユーザ側200に送付される。これにより、ユーザ側200は精算が行われたことを知ることができる。

【0277】次に、課金情報管理関320の精算手続き受付機能ブロック365は、使用権発行機能ブロック362から使用権発行情報を発行させる。この使用権発行情報は、上記ユーザ側200から送られてきたコンテンツ使用記録と共に、通信機能ブロック361を介し、ユーザ決済・コンテンツ使用記録送付T74としてシステム管理関330に送付される。

【0278】システム管理関330は、集金及び分配機能ブロック405にて、各地に分散している課金情報管理関320から送付されてきた情報をまとめ、集金額と集金先とお金の分配先を集計し、実際の金融機関を通して決済する。

【0279】以上により、コンテンツ使用料金の精算の流れが終了する。なお、この図34に挙げられている他の構成についての説明は後述する。

【0280】上述の図30から図34までの説明において、コンテンツ展示配信関310、課金情報管理関320、システム管理関330とユーザ側200との間のデータ送受や、コンテンツ展示配信関310、課金情報管理関320とシステム管理関330との間のデータ送受においても、前述同様にデータの暗号化と復号化が行われていることは言うまでもない。またこの暗号化と復号化においても、公開鍵暗号方式と共通鍵暗号方式の何れを用いても良いし、前述したようにコンテンツ鍵や共通鍵の暗号化方式としては公開鍵暗号方式を使用し、メッセージや各種の書類等の暗号化方式としては共通鍵暗号方式を使用することができる。また、これら暗号化と共に前記乱数を用いたセキュリティ向上の手法や、コンテンツを扱う際の暗号化と圧縮の処理単位の最小公倍数化を使用することも可能である。

【0281】次に、上述した各関310、320、330の具体的な構成について簡単に説明する。

【0282】先ず、図35を用いてコンテンツ展示配信関310の構成の説明を行う。

【0283】この図35において、当該コンテンツ展示配信関310は、大別して、ユーザ側200とシステム管理関330との間の通信機能を担当する通信機能ブロック341と、コンテンツの入手機能を担当するコンテンツ入手機能ブロック342と、コンテンツの展示機能を担当するコンテンツ展示機能ブロック343と、精算を担当する精算機能ブロック344と、コンテンツ

を保存するコンテンツデータベース機能ブロック345とからなる。

【0284】上記コンテンツ入手機能ブロック342は、システム管理関330に対してコンテンツを請求するときの請求書の作成を担当するコンテンツ請求書作成機能部351と、システム管理関330からコンテンツを受け取ったときの受領書の作成を担当するコンテンツ受領書作成機能部352と、これらあつかったコンテンツとコンテンツデータベース機能ブロック345に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部353とからなる。

【0285】上記コンテンツ展示機能ブロック343は、実際に仮想店舗にコンテンツを展示する機能を担当するコンテンツ展示機能部354と、これら展示しているコンテンツと上記コンテンツデータベース機能ブロック345に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部355とからなる。

【0286】上記精算機能ブロック344は、領収書を発行する機能を担当する領収書発行機能部356と、金融関220との間の対応を担当する金融関対応機能部357とからなる。

【0287】次に、図36を用いて、課金情報管理関320の構成の説明を行う。

【0288】この図36において、当該課金情報管理関320は、大別して、ユーザ側200とシステム管理関330との間の通信機能を担当する通信機能ブロック361と、使用権を発行する機能を担当する使用権発行機能ブロック362と、コンテンツ鍵と使用条件の受け取りを担当するコンテンツ鍵・使用条件受取機能ブロック363と、コンテンツ鍵と使用条件の発行を担当するコンテンツ鍵・使用条件発行機能ブロック364と、精算手続きの受け付け機能を担当する精算手続き受付機能ブロック365と、分配と受け取りの機能を担当する分配受取機能ブロック366と、データベース機能ブロック376とからなる。

【0289】上記使用権発行機能ブロック362は、購入依頼書の確認機能を担当する購入依頼書確認機能部371と、クライアントすなわちユーザ側200の使用権の残高（ポイント情報の残高）や使用記録（ポイント使用情報）等のデータの確認を担当するポイントデータ確認機能部372と、使用権を発生する機能を担当する使用権発生機能部373と、使用権の送付書を作成する機能を担当する使用権送付書作成機能部374と、使用権と使用権送付書を実際に送付する機能を担当する送付機能部375と、使用権の受け取り書の確認を担当する使用権受取確認機能部376と、発行した使用権の情報を保存する機能を担当する使用権発行情報保存機能部377とからなる。

【0290】上記コンテンツ鍵・使用条件受取機能ブロック363は、コンテンツ鍵と使用条件の受取を担当す

る受取機能部378と、コンテンツ鍵と使用条件を保存する保存機能部379とからなる。

【0291】上記コンテンツ鍵・使用条件発行機能ブロック364は、コンテンツ鍵と使用条件の入手依頼を受信する機能を担当する受信機能部380と、コンテンツ鍵と使用条件をデータベース機能ブロック367から検索して探し出す機能を担当する検索機能部381と、コンテンツ鍵と使用条件を暗号化して送付する機能を担当する送信機能部382と、コンテンツ鍵と使用条件の受取書の確認機能を担当する確認機能部383とからなる。

【0292】上記精算手続き受付機能ブロック365は、暗号化されているコンテンツ使用記録（ポイント使用情報）を受信して復号化する機能を担当するコンテンツ使用記録受信機能部384と、コンテンツ使用記録の確認を担当するコンテンツ使用記録確認機能部385と、コンテンツ使用記録をデータベース機能ブロック367の保存する機能を担当するコンテンツ使用記録保存機能部386と、精算手続きの完了書を作成する機能を担当する完了書作成機能部387と、コンテンツ使用記録をまとめて編集する機能を担当するまとめ機能部389とからなる。

【0293】上記分配受取機能ブロック366は、集金を行う際の資料を請求する資料請求書の確認機能を担当する請求書確認機能部390と、システム管理機関330に対して提出するコンテンツ使用記録の報告書を作成する機能を担当する使用記録報告書作成機能部391と、システム管理機関330に対して提出する使用権発行情報の報告書を作成する機能を担当する使用権発行報告書作成機能部392と、報告書の受信確認書の確認機能を担当する確認書確認機能部393とからなる。

【0294】データベース機能ブロック367は、使用権のデータを保存する機能を担当する使用権データベース機能部394と、コンテンツ鍵と使用条件のデータを保存する機能を担当するコンテンツ鍵・使用権データベース機能部395と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部396と、ユーザに関する情報を保存するユーザ管理データベース機能部397とからなる。

【0295】次に、図37を用いて、システム管理機関330の構成の説明を行う。

【0296】この図37において、当該システム管理機関330は、大別して、ユーザ側200、コンテンツ展示配信機関310、及び課金情報管理機関320との間の通信機能を担当する通信機能ブロック401と、ユーザ加入の際のサポートを行うユーザ加入サポート機能ブロック402と、コンテンツの配布を担当するコンテンツ配布機能ブロック404と、データベース機能ブロック403と、集金と分配の機能を担当する集金及び分配機能ブロック405とからなる。

【0297】上記ユーザ加入サポート機能ブロック402は、加入申請書の作成と送信を担当する加入申請書作成送信機能部411と、暗号化された共通鍵を受信して復号化する機能を担当する共通鍵受信機能部412と、ユーザ側200から送信されてきた加入申請書の確認機能を担当する加入申請書確認機能部413と、クライアントIDすなわちユーザIDを発生する機能を担当するID発生機能部414と、加入申請書をデータベース機能ブロック403に保存する機能を担当する加入申請書保存機能部415と、クライアント機能を生成するクライアント機能生成機能部416と、登録情報をデータベース機能ブロック403に保存する機能を担当する登録情報保存機能部417とからなる。

【0298】データベース機能ブロック403は、ユーザの情報を保存管理するユーザ管理データベース機能部418と、コンテンツを保存するコンテンツデータベース機能部419と、課金情報管理機関320の情報を保存管理する課金情報管理機関データベース機能部420と、コンテンツ展示配信機関310の情報を保存管理するコンテンツ展示配信機関データベース機能部421とからなる。

【0299】コンテンツ配信機能ブロック404は、コンテンツの請求書の確認機能を担当する請求書確認機能部422と、生コンテンツすなわち加工前のコンテンツ（ソースデータ）をデータベース機能ブロック403のコンテンツデータベース機能部419から検索する機能を担当するコンテンツ検索機能部423と、コンテンツIDを生成するコンテンツID生成機能部424と、コンテンツ鍵を生成するコンテンツ鍵生成機能部425と、コンテンツ使用条件を生成するコンテンツ使用条件生成機能部426と、生コンテンツすなわち加工前のコンテンツを圧縮するコンテンツ圧縮機能部427と、コンテンツの暗号化を行うコンテンツ加工機能部428と、コンテンツIDとコンテンツ鍵と使用条件とをデータベース機能ブロック403のコンテンツデータベース機能部419に保存する機能を担当する保存機能部429と、コンテンツを通信機能ブロック401を介して送付する機能を担当するコンテンツ送付機能部430と、コンテンツの受領書を確認する機能を担当するコンテンツ受領書確認機能部431と、コンテンツIDとコンテンツ鍵と使用条件を通信機能ブロック401を介して送付する機能を担当するID・鍵・使用条件送付機能部432と、コンテンツIDとコンテンツ鍵と使用条件の受領書を確認する機能を担当するID・鍵・使用条件受領書確認機能部433とからなる。

【0300】集金及び分配機能ブロック405は、集金に使用する資料の請求書を作成する資料請求書作成機能部434と、コンテンツ使用権を通信機能ブロック401を介して受信する機能を担当するコンテンツ使用権受信機能部435と、コンテンツ使用記録を通信機能ブ

ック401を介して受信する機能を担当するコンテンツ使用記録受信機能部436と、受信の確認書を作成する機能を担当する受信確認書作成機能部437と、ユーザへ請求する請求額の計算と請求書の作成を行う請求書の作成を行う計算・請求書作成機能部438と、使用により集金した使用金を権利者に分配する際の分配金の計算と納付書の作成を行う計算・納付書作成機能部439とからなる。

【0301】次に、当該他の実施の形態のシステムに対応するユーザ側200の構成を、図38を用いて説明する。なお、この図38は、前記プレーヤ1とユーザ端末50の各機能をまとめて表している。

【0302】この図38において、当該ユーザ側200の構成は、大別すると、システム管理機関330、コンテンツ展示配信機関310、及び課金情報管理機関320との間の通信機能を担当する通信機能ブロック451と、コンテンツの入手を担当するコンテンツ入手機能ブロック452と、ポイント情報やコンテンツ鍵、使用条件等の使用権の購入を担当する使用権購入機能ブロック453と、コンテンツ鍵と使用条件の入手を担当するコンテンツ鍵・使用条件入手機能ブロック454と、精算手続きを担当する精算手続き機能ブロック455と、システムへの加入をサポートする機能を担当するユーザ加入サポート機能ブロック456と、コンテンツの鑑賞と課金の機能を担当するコンテンツ鑑賞課金機能ブロック457と、データベース機能ブロック458とからなる。

【0303】上記コンテンツ入手機能ブロック452は、実際にコンテンツを入手する機能を担当するコンテンツ入手機能部461と、コンテンツを記憶メディアに保存させる機能を担当するコンテンツ保存機能部462とからなる。

【0304】使用権購入機能ブロック453は、使用権の購入依頼書を作成する購入依頼書作成機能部463と、クライアント(ユーザ)の使用権の残高(ポイント残高)や使用記録(ポイント使用情報)等のデータのまとめを担当するまとめ機能部464と、使用権としての各情報をインストールする機能を担当する使用権インストール機能部465と、使用権受取書を作成する使用権受取書作成機能部467とからなる。

【0305】コンテンツ鍵・使用条件入手機能ブロック454は、コンテンツ鍵と使用条件の入手依頼書を作成する入手依頼書作成機能部468と、コンテンツ鍵と使用条件の受信を担当する受信機能部469と、コンテンツ鍵と使用条件の受取書を作成する受取書作成機能部470とからなる。

【0306】精算手続き機能ブロック455は、コンテンツ使用記録(ポイント使用情報)のまとめを行うまとめ機能部471と、精算手続きの完了書の受信を担当する完了書受信機能部472とからなる。

【0307】上記ユーザ加入サポート機能ブロック456は、加入申請書の作成を担当する加入申請書作成機能部473と、クライアント機能のインストールすなわちユーザのプレーヤ1の初期化を担当するクライアント機能インストール機能部474、登録情報を作成する機能を担当する登録情報作成機能部475とからなる。

【0308】コンテンツ鑑賞課金機能ブロック457は、記憶メディアに保存されたコンテンツの検索を担当するコンテンツ検索機能部476と、使用権の確認を担当する使用権確認機能部477と、例えばコンテンツの選択を行うときに簡易的にコンテンツを再生する簡易コンテンツ鑑賞機能部478と、課金情報(ポイント情報)の管理を行う課金機能部479と、暗号化されているコンテンツを復号化するコンテンツ復号機能部480と、圧縮されているコンテンツを伸長するコンテンツ伸長機能部481と、例えば記憶メディアに保存されているコンテンツの内容を認識可能にするためのコンテンツビューア機能部482とからなる。

【0309】データベース機能ブロック458は、使用権のデータを保存する使用権データベース機能部483と、コンテンツ鍵と使用条件を保存するコンテンツ鍵・使用条件データベース機能部484と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部485と、ユーザ情報を保存するユーザ情報データベース機能部486とからなる。

【0310】次に、上述したような各実施の形態のプレーヤ1とユーザ端末50の具体的な使用形態について、図39と図40を用いて説明する。

【0311】図39に示すように、プレーヤ1は、前記アナログ出力端子2とPC用インターフェース端子3と記憶メディア用I/O端子4がプレーヤ1の筐体外に突き出た状態で配置されており、上記記憶メディア用I/O端子4には、記憶メディア61が接続されるようになっている。また、これらプレーヤ1と記憶メディア61は、例えばケース60内に収納可能に形成されており、このケース60の例えば一端側に上記プレーヤ1のアナログ出力端子2とPC用インターフェース端子3が配置されるようになされている。

【0312】このプレーヤ1及び記憶メディア61が収納されたケース60は、上記プレーヤ1のアナログ出力端子2とPC用インターフェース端子3が配置される側から、上記ユーザ端末50としてのパーソナルコンピュータ50の入出力ポート53に挿入接続可能なように形成されている。

【0313】当該パーソナルコンピュータ50は、コンピュータ本体に、ディスプレイ装置52とキーボード54とマウス55とを備えた一般的な構成を有するものであるが、上記入出力ポート53内には上記プレーヤ1のアナログ出力端子2及びPC用インターフェース端子3と対応したインターフェースが形成されている。したが

って、上記プレーヤ1及び記憶メディア61が収納されたケース60を上記パーソナルコンピュータ50の入出力ポート53に挿入するだけで、上記プレーヤ1のアナログ出力端子2とPC用インターフェース端子3が上記パーソナルコンピュータ50と接続されるようになる。

【0314】上記図39の例では、パーソナルコンピュータ50の入出力ポート53内に、上記プレーヤ1のアナログ出力端子2及びPC用インターフェース端子3と対応したインターフェースを形成するようにしているが、例えば図40に示すように、パーソナルコンピュータ50の汎用入出力ポートのインターフェースに対応できるアダプタ62を、上記プレーヤ1のアナログ出力端子2及びPC用インターフェース端子3の間に配置することも可能である。

【0315】以上述べてきたことから、本発明の実施の形態のシステムにおいては、デジタルコンテンツはシステムの共通鍵であるコンテンツ鍵にて暗号化されているので、本実施の形態のシステムに登録したユーザ（プレーヤ1）であれば、この暗号化されたコンテンツを自由にコピーでき、コンテンツ鍵を入手しさえすればこのコンテンツの鑑賞も可能である。したがって、このコンテンツ（暗号化されたコンテンツの）記憶メディアへのインストールも簡単に行える。一方、本実施の形態システムに準拠していない端末装置では、暗号化されたデジタルコンテンツを復号できないので、コンテンツの著作権や当該コンテンツの権利者の権利は保護される。

【0316】また、本発明の実施の形態システムによれば、ポイント情報をプリペイド方式（料金前払い方式）により補充することにし、コンテンツ鑑賞時にポイント情報が減額されるようにするとともに、そのポイントの使用情報を収集するようにしているので、使用済みのポイントに関する権利をもつ権利者（著作権者等）及びコンテンツ販売店舗等は、鑑賞代金の回収が可能である。

【0317】さらに、ポイント情報やポイント使用情報のデータのやりとりの際には、前述したように暗号化が施されているので、セキュリティ性が向上している。例えば全く前回のデータと同じものを偽造して課金用のポイント情報を盗もうとしても、前述したように、システム側とプレーヤ側とで連動した乱数（セキュリティID）を使用し、両者が一致していることを確認してから取引を行うものとしているので、安全である。

【0318】またさらに、プレーヤの主要構成要素は1チップ化されており、鍵情報や復号化されたデジタルコンテンツを外部に取出すことが困難となっている。このプレーヤ1は、当該プレーヤ1の破壊によるデータ横取りを防ぐためにプレーヤ1自体にタンパーレジスタンス機能を備えている。

【0319】上述したように、本発明の実施の形態によれば、セキュリティ上強度の高いデジタルコンテンツ配信システムが構築されている。

【0320】なお、上述のデジタルコンテンツとしては、デジタルオーディオデータの他に、デジタルビデオデータ等の各種のものを挙げることができる。上記デジタルビデオデータとして動画像データ（オーディオデータも含む）を使用した場合、前記圧縮の手法としては、例えばMPEG（Moving Picture Image Coding Experts Group）等の圧縮手法を使用できる。なお、上記MPEGは、ISO（国際標準化機構）とIEC（国際電気標準会議）のJTC（Joint Technical Committee）1のSC（Sub Committee）29のWG（Working Group）11においてまとめられた動画像符号化方式の通称であり、MPEG1、MPEG2、MPEG4等がある。

【0321】さらに、上記暗号化の手法としては、前述したように、例えばいわゆるDES（Data Encryption Standard）と呼ばれている暗号化手法を使用することができる。なお、DESとは、米国のNIST（National Institute of Standards and Technology）が1976年に発表した標準暗号方式（暗号アルゴリズム）である。具体的には、64ビットのデータブロック毎にデータ変換を行うものであり、関数を使った変換を16回繰り返す。上記デジタルコンテンツやポイント情報等は、当該DESを用い、いわゆる共通鍵方式にて暗号化されている。なお、上記共通鍵方式とは、暗号化するための鍵データ（暗号鍵データ）と復号化するための鍵（復号鍵データ）が同一となる方式である。

【0322】また、前記図1のプレーヤ1の共通鍵保管メモリ22や通信用鍵保管メモリ21、ポイント使用情報格納メモリ29、ポイント情報格納メモリ28等には、例えばいわゆるEEPROM（電氣的に消去可能なROM）を使用できる。

【0323】他に記憶メディアとしては、例えばハードディスクやフロッピィディスク、光磁気ディスク、相変化型光ディスク等の記録媒体、或いは半導体メモリ（ICカード等）の記憶メディアを使用できる。

【0324】その他、上述の実施の形態では、コンテンツの選択や仮想店舗230に展示されたコンテンツの内容確認等の際には、ユーザ端末50のキーボード54やマウス55、ディスプレイ装置52を使用して選択、確認等を行っていたが、これらキーボードやマウス、ディスプレイ装置に機能を簡略化して、プレーヤ1に持たせることも可能である。すなわち、図2のように、入力キー部6や表示部7をプレーヤ1に設けることも可能である。

【0325】

【発明の効果】以上の説明で明らかのように、本発明によれば、簡単に持ち運びができて何時でも何処でもデジタルコンテンツを楽しむことが可能であり、また、デジタルコンテンツのコピー或いは不当な使用への防衛として十分運用に耐え、且つ経済的なシステムを構築す



ることをも可能である。

【図面の簡単な説明】

【図1】本発明の実施の形態のデジタルコンテンツ配布システムの全体構成を示すシステム構成図である。

【図2】本発明の実施の形態のシステムに対応するプレーヤの具体的構成を示すブロック回路図である。

【図3】本発明の実施の形態のシステムに対応する管理センタの具体的構成を示すブロック回路図である。

【図4】本実施の形態のシステムにおいてプレーヤの購入時の手順の説明に用いる図である。

【図5】本実施の形態のシステムにおいてデジタルコンテンツの検索からプレーヤ用の記憶メディアへのデジタルコンテンツのインストールまでの手順の説明に用いる図である。

【図6】実施の形態のシステムにおいて課金用のポイント情報の購入と当該デジタルコンテンツを使用した場合の精算の手順の説明に用いる図である。

【図7】実施の形態のシステムにおいて課金代金の分配の手順の説明に用いる図である。

【図8】実施の形態のシステムにおいてポイント購入時のプレーヤにおける処理の流れを示すフローチャートである。

【図9】実施の形態のシステムにおいてポイント購入時のユーザ端末における処理の流れを示すフローチャートである。

【図10】実施の形態のシステムにおいてポイント購入時の管理センタにおける処理の流れを示すフローチャートである。

【図11】実施の形態のシステムにおいてポイント購入時の情報送受のシーケンスを示す図である。

【図12】実施の形態のシステムにおいてデジタルコンテンツの入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図13】実施の形態のシステムにおいてデジタルコンテンツの入手時のユーザ端末における処理の流れを示すフローチャートである。

【図14】実施の形態のシステムにおいてデジタルコンテンツの入手時の管理センタにおける処理の流れを示すフローチャートである。

【図15】実施の形態のシステムにおいてデジタルコンテンツの入手時の情報送受のシーケンスを示す図である。

【図16】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図17】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のユーザ端末における処理の流れを示すフローチャートである。

【図18】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の管理センタにおける処理の流れ

を示すフローチャートである。

【図19】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の情報送受のシーケンスを示す図である。

【図20】実施の形態のシステムにおいてプレーヤとユーザ端末を用いてデジタルコンテンツを実際に鑑賞する際の処理の流れを示すフローチャートである。

【図21】実施の形態のシステムにおいてポイント使用情報返却時のプレーヤにおける処理の流れを示すフローチャートである。

【図22】実施の形態のシステムにおいてポイント使用情報返却時のユーザ端末における処理の流れを示すフローチャートである。

【図23】実施の形態のシステムにおいてポイント使用情報返却時の管理センタにおける処理の流れを示すフローチャートである。

【図24】実施の形態のシステムにおいてポイント使用情報返却時の情報送受のシーケンスを示す図である。

【図25】暗号化と圧縮の処理単位の最小公倍数にて復号化と伸長を行う際の処理の流れを示すフローチャートである。

【図26】暗号化と圧縮の処理単位の最小公倍数の単位毎の復号化及び伸長処理を行う構成を示すブロック回路図である。

【図27】セキュリティIDとしての乱数を発生する具体的構成を示すブロック回路図である。

【図28】共通鍵を公開鍵暗号方式にて暗号化して送信する際に乱数が挿入される様子を説明するための図である。

【図29】受信文から乱数が取り出されて正当性の確認がなされる様子を説明するための図である。

【図30】システム側の機能を分割したときの各機関の説明に用いる図である。

【図31】システム側の機能を分割した実施の形態において、ユーザのシステムへの加入時の流れの主要部を説明するための図である。

【図32】システム側の機能を分割した実施の形態において、ポイント情報の購入や暗号化されたデジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明するための図である。

【図33】システム側の機能を分割した実施の形態において、コンテンツとコンテンツ鑑賞用の情報の流通の流れの主要部を説明するための図である。

【図34】システム側の機能を分割した実施の形態において、コンテンツが実際に鑑賞されたときの精算の流れの主要部を説明するための図である。

【図35】システム側の機能を分割した実施の形態において、コンテンツ展示配信機関の構成を示すブロック図である。

【図36】システム側の機能を分割した実施の形態にお

いて、課金情報管理機関の構成を示すブロック図である。

【図37】システム側の機能を分割した実施の形態において、システム管理機関の構成を示すブロック図である。

【図38】システム側の機能を分割した実施の形態において、ユーザ側の構成を示すブロック図である。

【図39】プレーヤとユーザ端末の具体的な使用形態の一例の説明に用いる図である。

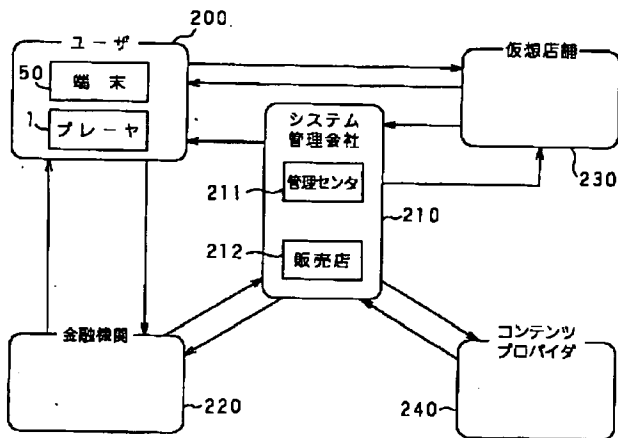
【図40】プレーヤとユーザ端末の具体的な使用形態の他の例の説明に用いる図である。

【符号の説明】

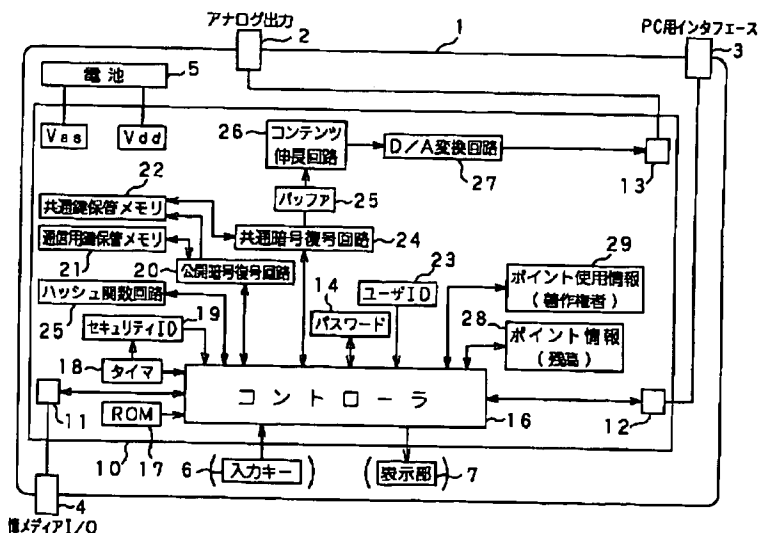
1 プレーヤ、 2 アナログ出力端子、 3 PC用

インターフェース端子、 4 記憶メディア用I/O端子、 16 コントローラ、 19 セキュリティID発生回路、 20 公開暗号復号回路、 21 通信用鍵保管メモリ、 22 共通鍵保管メモリ、 23 ユーザID格納メモリ、 24 共通暗号復号回路、 25 バッファメモリ、 26 伸長回路、 27 D/A変換回路、 50 ユーザ端末、 100 コンテンツ管理機能ブロック、 110 ユーザ管理機能ブロック、 120 使用情報管理機能ブロック、 130 管理機能ブロック、 200 ユーザ側、 210 システム管理会社、 211 管理センタ、 220 金融機関、 230 仮想店舗、 240 コンテンツプロバイダ

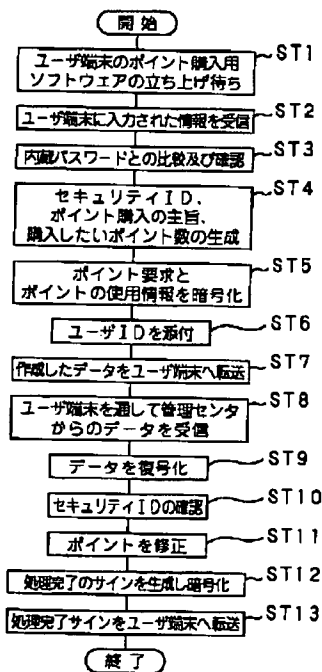
【図1】



【図2】

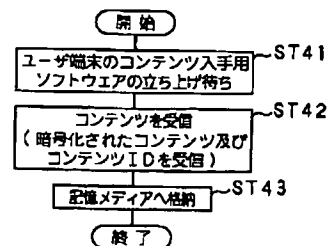


【図8】



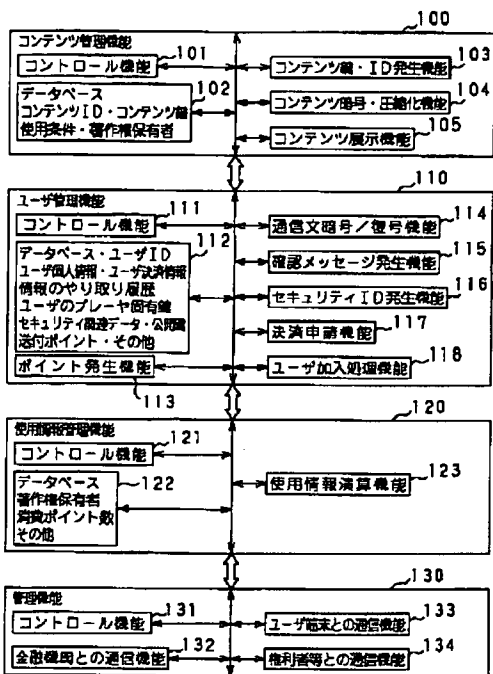
ポイント購入時のプレーヤのフローチャート

【図12】

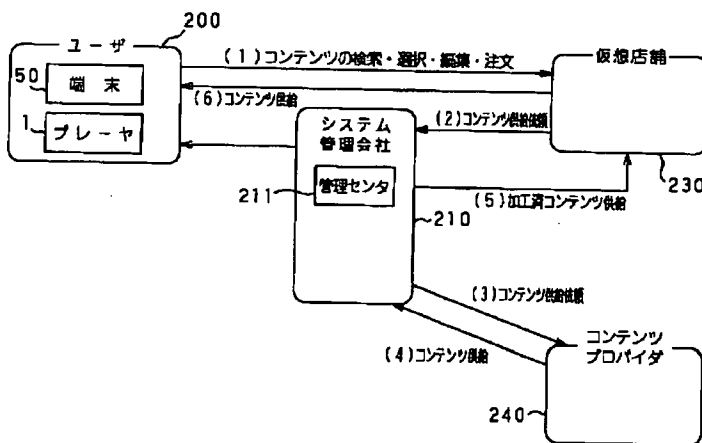


コンテンツ入手時のプレーヤのフローチャート

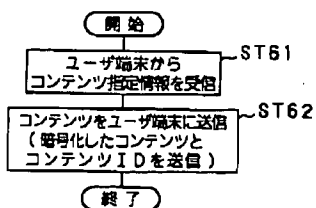
【図3】



【図5】

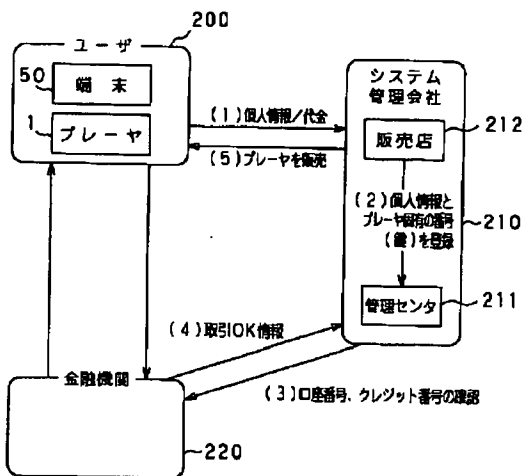


【図14】

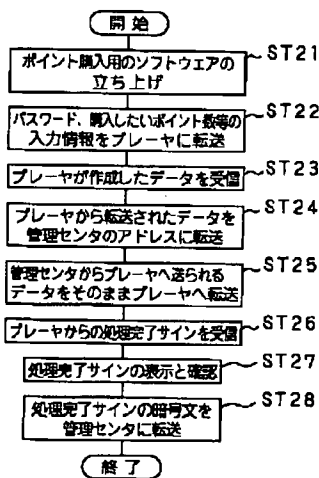


コンテンツ入手時の管理センタのフローチャート

【図4】

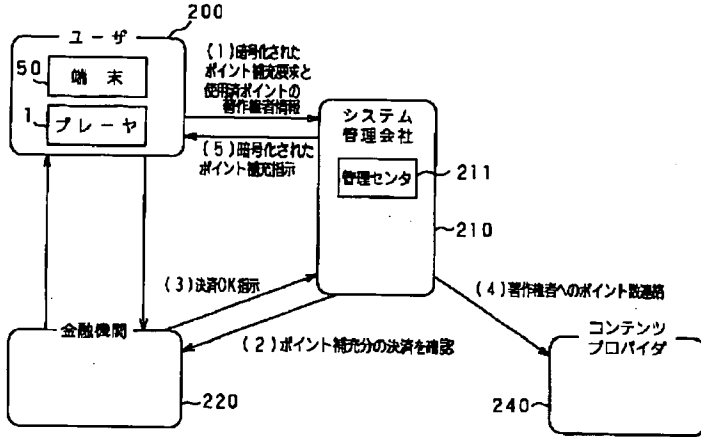


【図9】

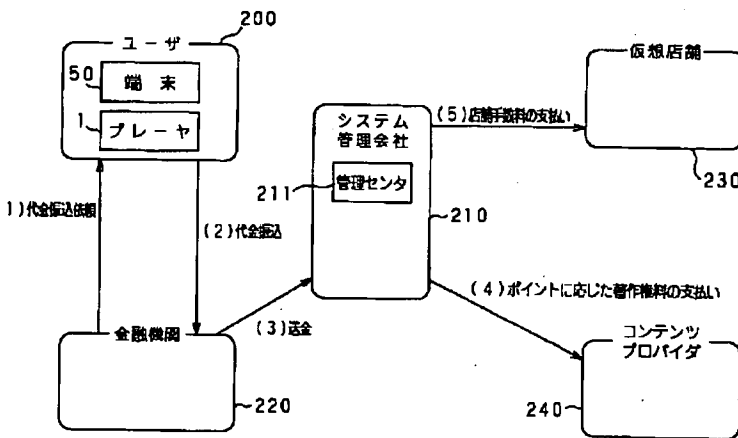


ポイント購入時のユーザ端末のフローチャート

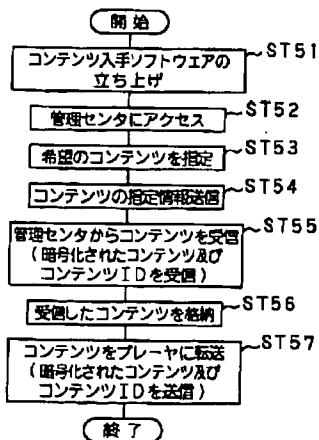
【図6】



【図7】

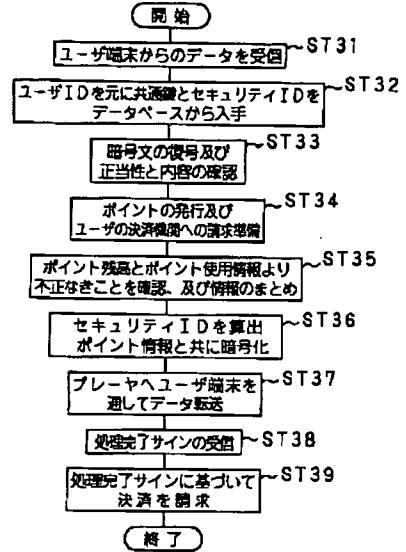


【図13】



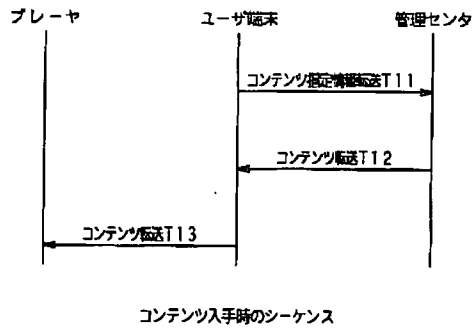
コンテンツ入手時のユーザ端末のフローチャート

【図10】



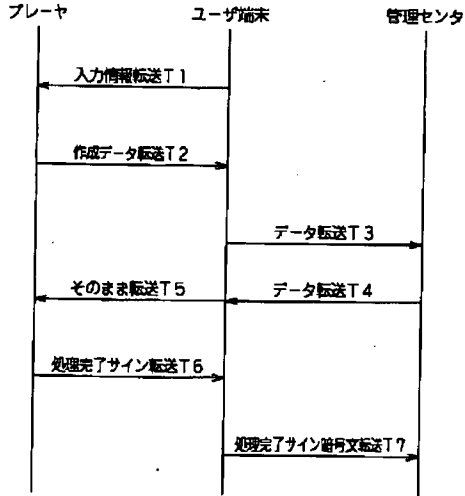
ポイント購入時の管理センターのフローチャート

【図15】



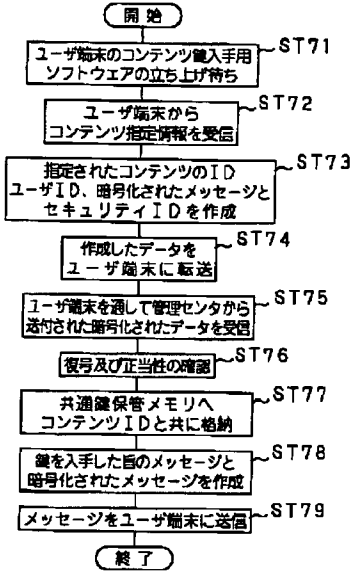
コンテンツ入手時のシーケンス

【図11】



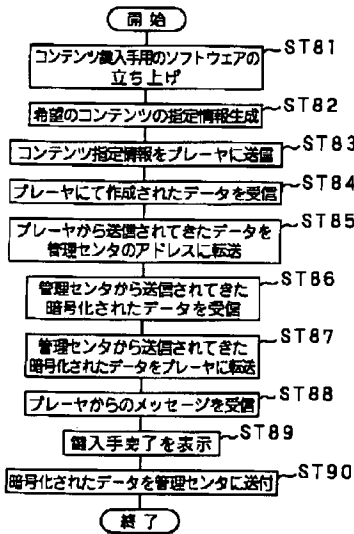
ポイント購入時のシーケンス

【図16】



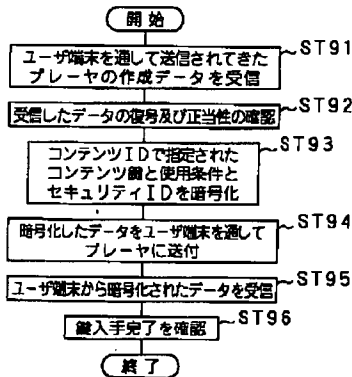
コンテンツ購入・入手時のプレーヤのフローチャート

【図17】



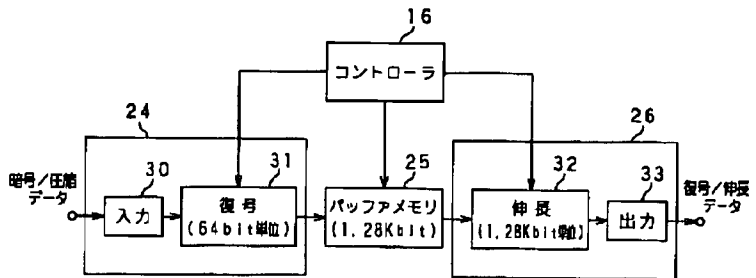
コンテンツ購入・使用条件入手時のユーザー端末のフローチャート

【図18】

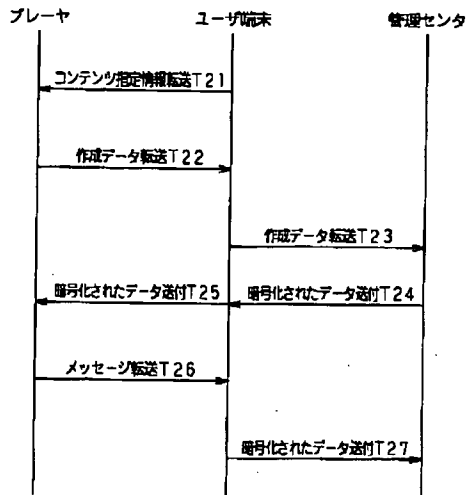


コンテンツ購入・使用条件入手時の管理センタのフローチャート

【図26】

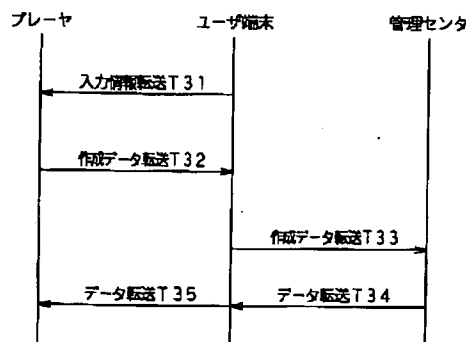


【図19】



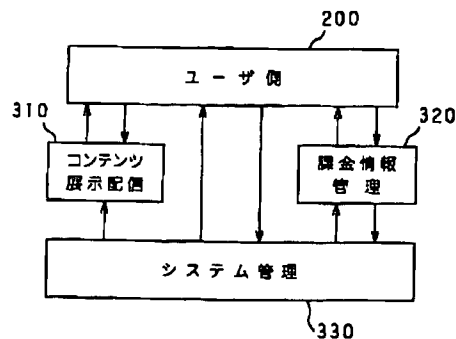
コンテンツ備・使用条件入手時のシーケンス

【図24】

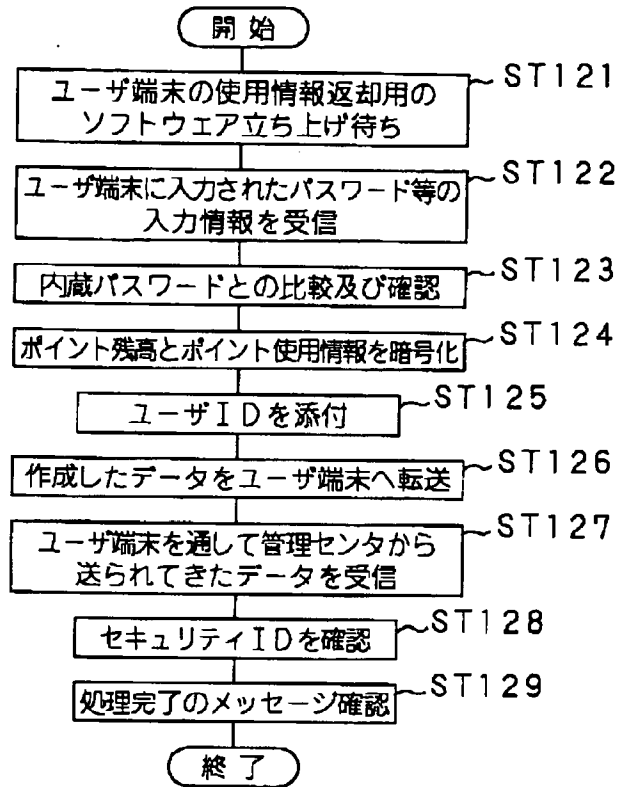


使用情報返却時のシーケンス

【図30】

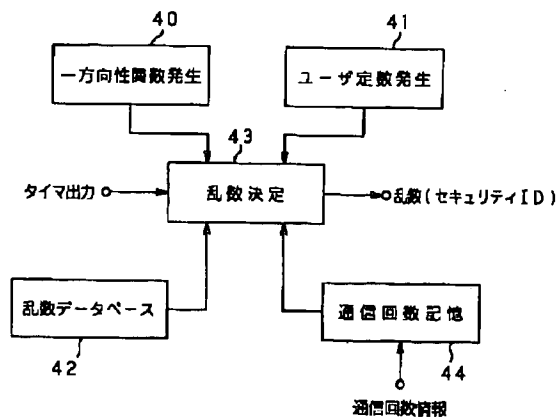


【図21】

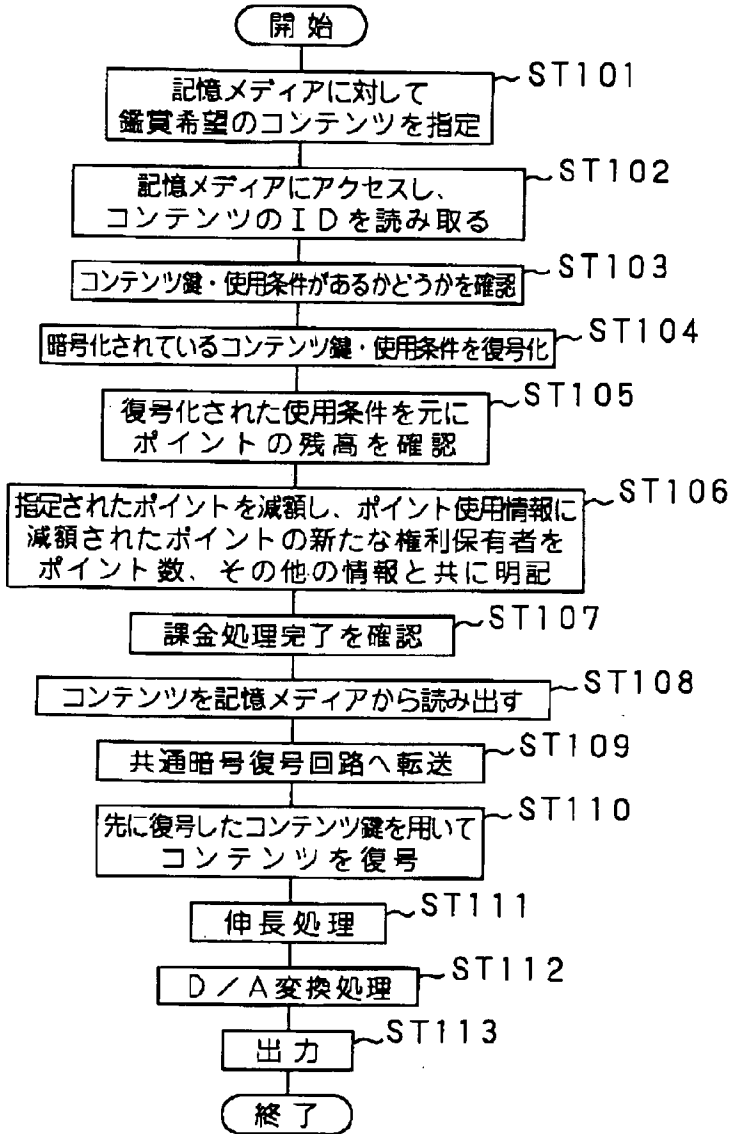


使用情報返却時のプレーヤのフローチャート

【図27】

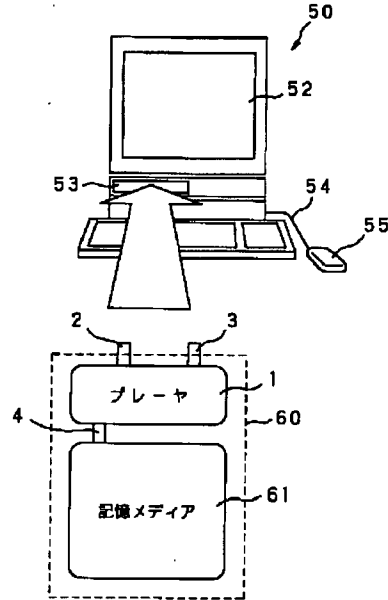


【図20】

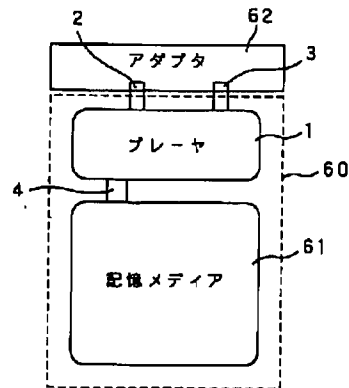


コンテンツ鑑賞時のプレーヤのフローチャート

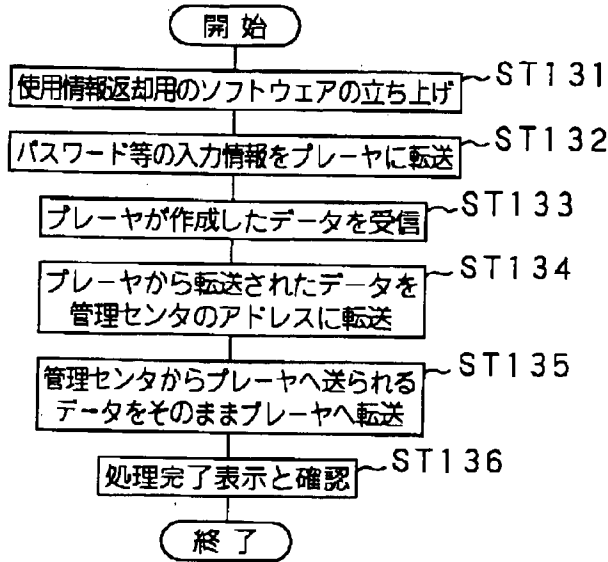
【図39】



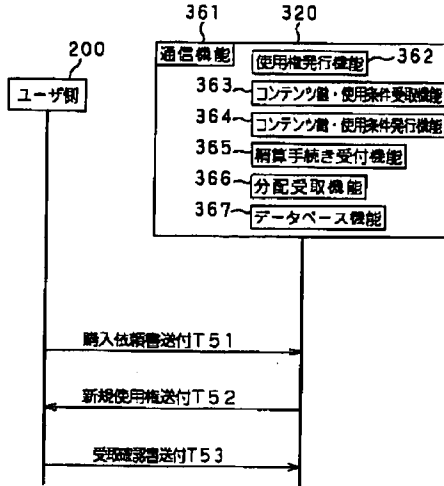
【図40】



【図22】

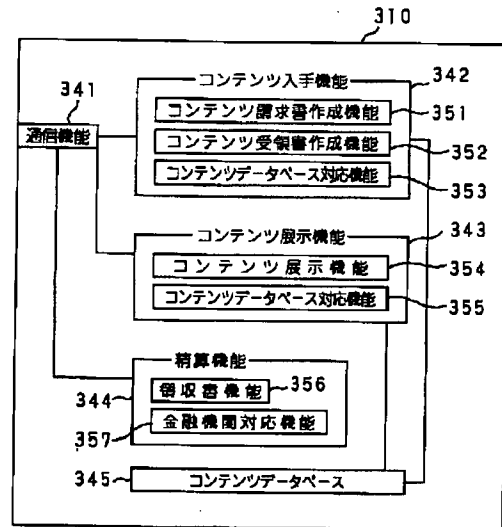


【図32】

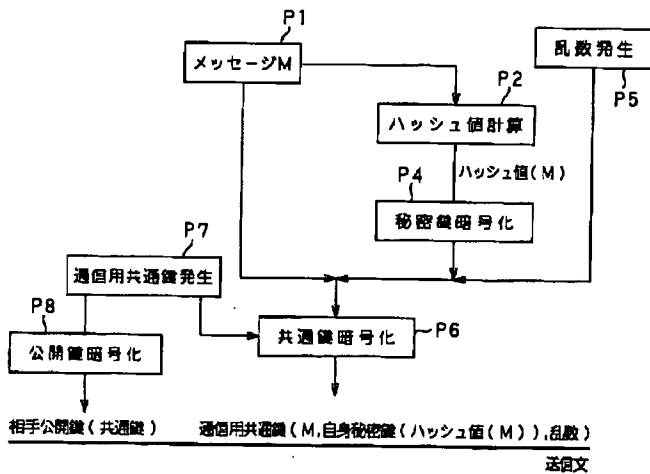


【図35】

使用情報返却時のユーザ端末のフローチャート

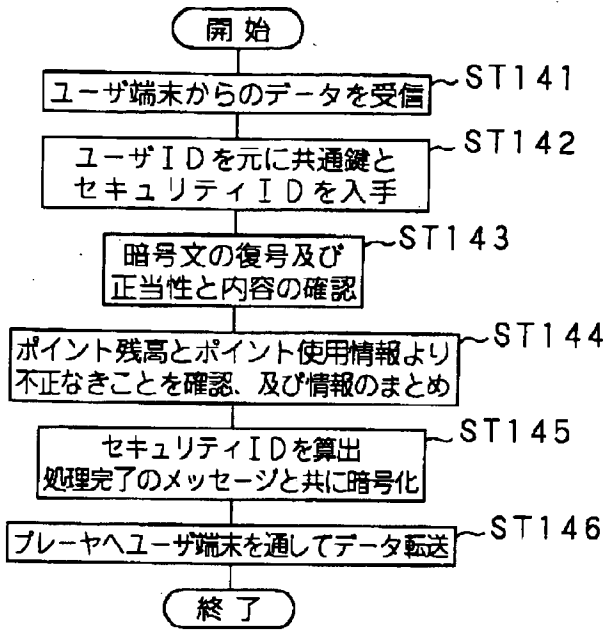


【図28】



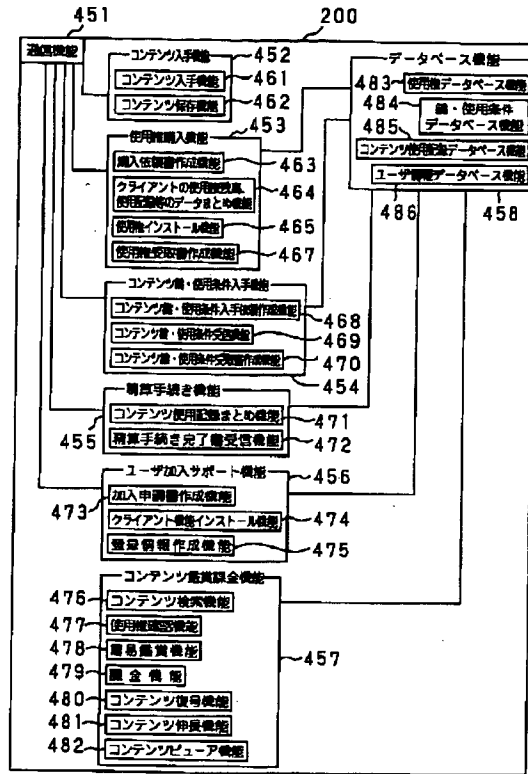


【図23】

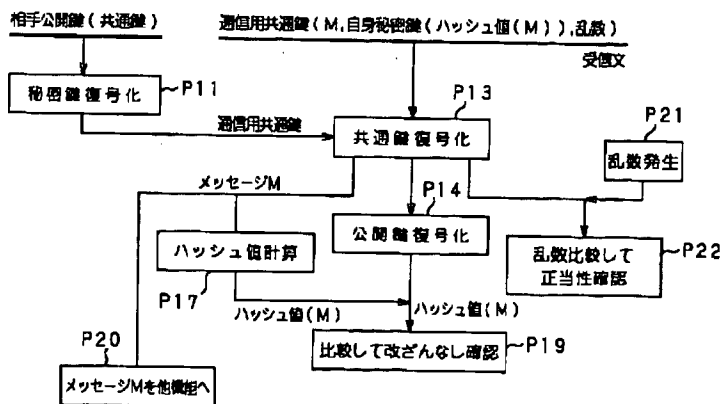


使用情報返却時の管理センタのフローチャート

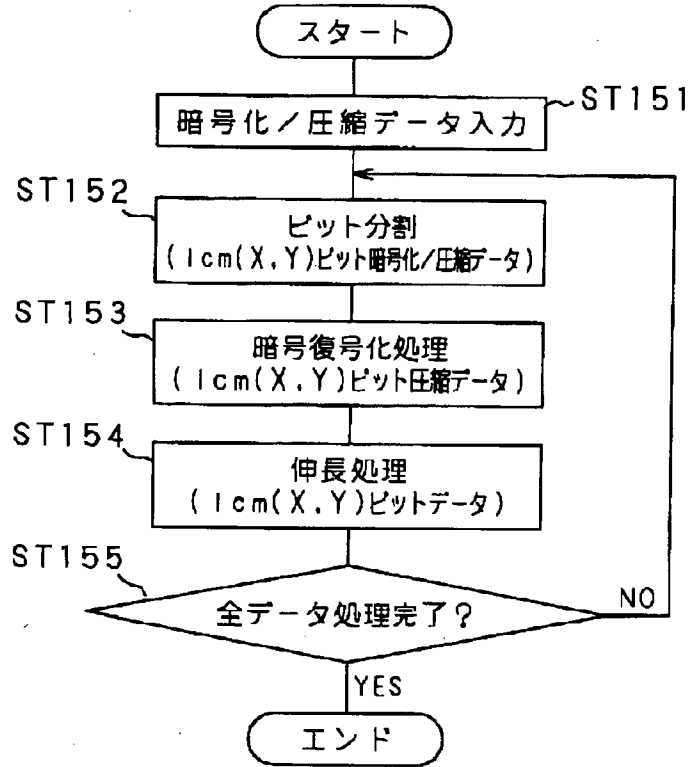
【図38】



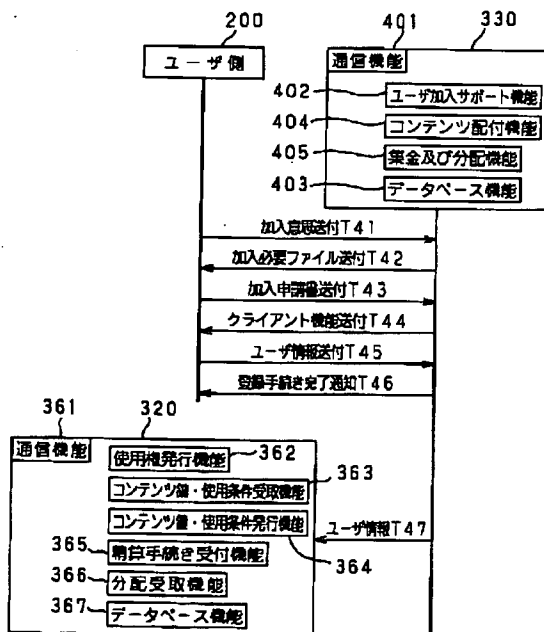
【図29】



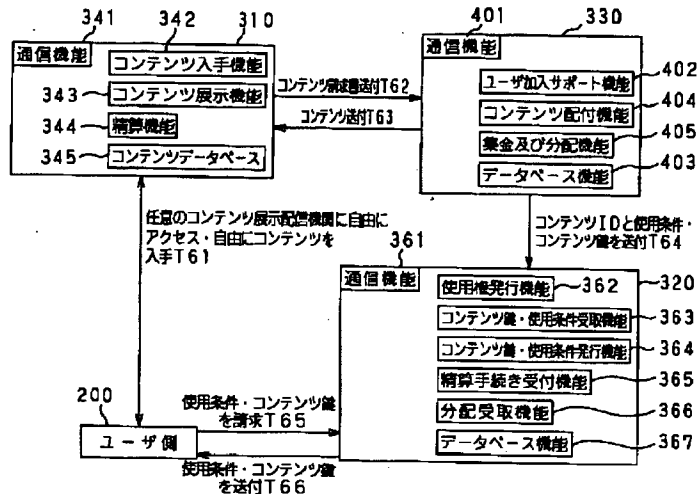
【図25】



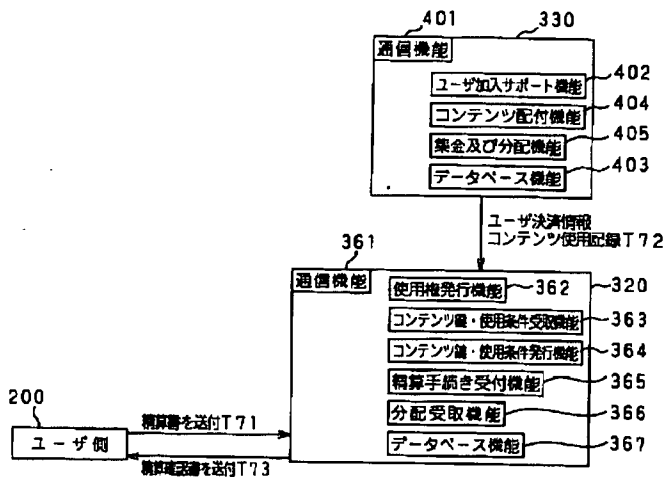
【図31】



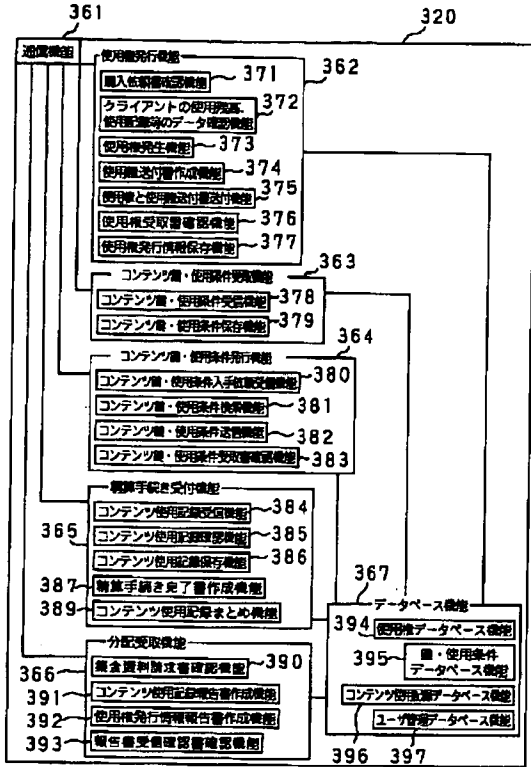
【図33】



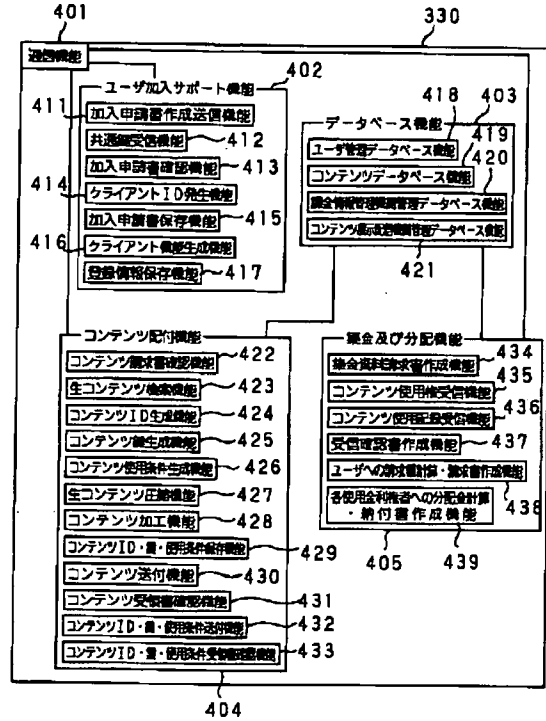
【図34】



【図36】



【図37】



フロントページの続き

(51) Int. Cl. 6

識別記号

H04L 9/08  
 12/14  
 H04M 15/00

F I

H04M 15/00  
 G06F 15/21  
 H04L 9/00

Z

Z

601E

601A

11/02

F



concerned and compresses digital contents. <BR> A contents transmission process which transmits digital contents which processed [ above-mentioned ] it according to a digital contents Request to Send from the communications-partner side. <BR> The Cong Teng key transmission process which enciphers a contents key used for decryption of digital contents processed [ above-mentioned ] and transmits according to a contents key Request to Send from the communications-partner side. <BR> An accounting information transmission process which enciphers accounting information reduced whenever it decrypts digital contents processed [ above-mentioned ] and transmits according to an accounting information Request to Send from the communications-partner side. A contents usage information receiving process which receives and decrypts enciphered contents usage information which has been transmitted from the communications-partner side and a use gold distribution process of distributing use gold collected based on the above-mentioned contents usage information to a right holder of the above-mentioned digital contents. <BR> <BR> [Claim 2] The digital contents distribution controlling method according to claim 1 wherein the above-mentioned contents key is a common key. <BR> [Claim 3] The digital contents distribution controlling method according to claim 1 enciphering the above-mentioned contents key using a public key by the side of a communications partner. <BR> [Claim 4] The digital contents distribution controlling method according to claim 1 having the common key decryption process of receiving and decrypting an enciphered common key which has been transmitted from the communications-partner side. <BR> [Claim 5] The digital contents distribution controlling method according to claim 4 wherein the above-mentioned common key is a session key. <BR> [Claim 6] The digital contents distribution controlling method according to claim 4 characterized by enciphering accounting information using the above-mentioned common key in the above-mentioned accounting information transmission process. <BR> [Claim 7] The digital contents distribution controlling method according to claim 4 using the above-mentioned common key for decryption of contents usage information enciphered [ above-mentioned ] in the above-mentioned contents usage information receiving process. <BR> [Claim 8] The digital contents distribution controlling method according to claim 1 receiving contents usage information which is transmitted from the communications-partner side concerned in connection with a Request to Send of the above-mentioned accounting information from the above-mentioned communications-partner side and which was enciphered [ above-mentioned ] in the above-mentioned contents usage information receiving process. <BR> [Claim 9] The digital contents distribution controlling method according to claim 1 transmitting information which shows a service condition of contents with the above-mentioned accounting information in the above-mentioned accounting information transmission process. <BR> [Claim 10] A <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> digital contents reproduction method comprising: <BR> A content reception process of receiving and storing digital contents processed by encryption and compression processing. <BR> A contents key demand information generation process of generating contents key demand information for requiring a contents key required for decryption of digital contents processed [ above-mentioned ]. <BR> A contents key demand transmitting information process of enciphering the above-mentioned contents key demand information and transmitting. <BR> A contents key receiving process which receives a contents key transmitted according to a demand of the above-mentioned contents key. A contents key decryption process of decrypting encryption given to the above-mentioned contents key. A contents key storage process of keeping a contents key enciphered [ above-mentioned ] or a contents key after the above-mentioned decryption. A contents decryption process of decrypting digital contents processed [ above-mentioned ] using the above-mentioned contents key. An accounting information demand information generation process of generating accounting information demand information for requiring accounting information reduced whenever it decrypts digital contents processed [ above-mentioned ]. An accounting information demand transmitting information process of enciphering the above-mentioned accounting information demand information and transmitting. An accounting information receiving process which accounting information transmitted according to a demand of the above-mentioned accounting information is received and decrypts and stores encryption given to the accounting information concerned. A contents extension process of elongating digital contents processed [ above-mentioned ]. A contents usage information storing process which generates and stores contents usage information according to decryption of digital contents processed [ above-mentioned ] and a contents usage information

transmission process which enciphers the above-mentioned contents usage information and transmits.<BR><BR>[Claim 11]In a contents usage information storing process the balance of accounting information stored [ above-mentioned ] is checkedThe digital contents reproduction method according to claim 10 generating contents usage information which reduces accounting information stored [ above-mentioned ] according to decryption of digital contents processed [ above-mentioned ] and contains the amount of cuts of the above-mentioned accounting information at least.<BR>[Claim 12]The digital contents reproduction method according to claim 10 having the digital to analog process of carrying out the digital to analog of the digital contents by which the above-mentioned decryption and extension were made.<BR>[Claim 13]The digital contents reproduction method according to claim 10 storing in external storage digital contents processed [ above-mentioned ] in the above-mentioned content reception process.<BR>[Claim 14]The digital contents reproduction method according to claim 10 wherein the above-mentioned contents key is a common key.<BR>[Claim 15]The <DP N=0003><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>digital contents reproduction method according to claim 10 characterized by decrypting the above-mentioned contents key using a peculiar secret key in the above-mentioned contents key decryption process.<BR>[Claim 16]The digital contents reproduction method according to claim 10 having a common key transmission process which generates a common key enciphers the common key concerned and transmits.<BR>[Claim 17]The digital contents reproduction method according to claim 16 characterized by generating a session key as the above-mentioned common key in the above-mentioned common key transmission process.<BR>[Claim 18]The digital contents reproduction method according to claim 16 characterized by enciphering the above-mentioned accounting information demand information using the above-mentioned common key in the above-mentioned accounting information demand transmitting information process.<BR>[Claim 19]The digital contents reproduction method according to claim 16 characterized by using the above-mentioned common key for encryption of the above-mentioned contents usage information in the above-mentioned contents usage information transmission process.<BR>[Claim 20]The digital contents reproduction method according to claim 10 transmitting contents usage information which enciphered [ above-mentioned ] in the above-mentioned contents usage information transmission process with a demand of the above-mentioned accounting information by the above-mentioned accounting information demand information generation process.<BR>[Claim 21]The digital contents reproduction method according to claim 10 also receiving information which shows a service condition of contents enciphered and transmitted with the above-mentioned accounting information in the above-mentioned accounting information receiving process.<BR>[Claim 22]A digital <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>contents playback device comprising:<BR>Data communication devices which perform data communications.<BR>A contents storage control means which receives digital contents processed by encryption and compression processing and is stored in a storage.<BR>A contents key decoding means which decrypts an enciphered contents key.<BR>A contents key storage means which keeps a contents key enciphered [ above-mentioned ] or a contents key after the above-mentioned decryptionA contents decoding means which decrypts digital contents processed [ above-mentioned ] using the above-mentioned contents keyAn accounting information decoding means which decrypts encryption given to accounting information reduced whenever it decrypts digital contents processed [ above-mentioned ]An accounting information storing means which stores accounting information decrypted [ above-mentioned ] and a contents expansion means which elongates digital contents processed [ above-mentioned ]A contents usage information creating means which generates contents usage information according to decryption of digital contents processed [ above-mentioned ]a contents usage information storing means which stores the above-mentioned contents usage information and a contents usage information encoding means which enciphers the above-mentioned contents usage information.<BR><BR>[Claim 23]The digital contents playback device comprising according to claim 22:<BR>A contents key demand information encoding means which enciphers contents key demand information for requiring a contents key required for decryption of digital contents processed [ above-mentioned ].<BR>An accounting information demand information encoding means which enciphers accounting information demand information for requiring accounting information reduced whenever it decrypts digital contents processed [ above-mentioned ].<BR><BR>[Claim 24]A contents usage information creating means checks the balance of accounting information stored in

the above-mentioned accounting information storing meansThe digital contents playback device according to claim 22 generating contents usage information which reduces accounting information stored [ above-mentioned ] according to decryption of digital contents processed [ above-mentioned ]and contains the amount of cuts of the above-mentioned accounting information at least.<BR>[Claim 25]The digital contents playback device according to claim 22 having a digital to analog means which carries out the digital to analog of the digital contents by which the above-mentioned decryption and extension were made.<BR>[Claim 26]The digital contents playback device according to claim 22wherein the above-mentioned contents storage control means stores in external storage digital contents processed [ above-mentioned ].<BR>[Claim 27]The digital contents playback device according to claim 22wherein the above-mentioned contents key is a common key.<BR>[Claim 28]The digital contents playback device according to claim 22 having an inherent key rank storage stage which keeps a key peculiar to a deviceand decrypting a contents key enciphered [ above-mentioned ] in the above-mentioned contents key decoding means using a secret key peculiar to a device currently kept to the above-mentioned peculiar key storage means.<BR>[Claim 29]The digital contents playback device comprising according to claim 22:<BR>A common key generating means which generates a common key.<BR>A common key cryptosystem-sized means to encipher the above-mentioned common key.<BR><BR>[Claim 30]The digital contents playback device according to claim 29wherein the above-mentioned common key generating means generates a session key as the above-mentioned common key.<BR>[Claim 31]The digital contents playback device according to claim 29wherein the above-mentioned accounting information decoding means decrypts the above-mentioned accounting information using the above-mentioned common key.<BR>[Claim 32]The digital contents playback device according to claim 29wherein the above-mentioned contents usage information encoding means enciphers the above-mentioned contents usage information using the above-mentioned common key.<BR>[Claim 33]The <DP N=0004><TXF FR=0001 HE=070 WI=080 LX=0200 LY=0300>digital contents playback device according to claim 22wherein the above-mentioned contents usage information encoding means has \*\*\*\* for encryption of the above-mentioned information usage information with encryption of the above-mentioned accounting information demand information by the above-mentioned accounting information demand information encoding means.<BR>[Claim 34]The digital contents playback device according to claim 22 also decrypting information which shows a service condition of contents enciphered with the above-mentioned accounting information in the above-mentioned accounting information decryption process.<BR>[Claim 35]The digital contents playback device according to claim 22 characterized by coming to be constituted so that a cellular phone is possible.<BR>[Claim 36]The digital contents playback device according to claim 22 having a case of card shape.<BR>[Claim 37]The digital contents playback device according to claim 22 which integrated-circuit-izes and is characterized by things.<BR></SDO><BR><HR><B>DETAILED DESCRIPTION</B><BR><HR><SDO DEJ><TXF FR=0002 HE=180 WI=080 LX=0200 LY=1000>[Detailed Description of the Invention]<BR>[0001]<BR>[Field of the Invention]This invention distributes digital contentssuch as audio information and a video datafor exampleand relates to the suitable digital contents distribution controlling method for the system charged according to the utilization quantity of these digital contentsa digital contents reproduction methodand a device.<BR>[0002]<BR>[Description of the Prior Art]Facilitate circulation of digital contentssuch as a computer programaudio informationa video datadelve into a latent demandand as a technique advantageous to a market expansionFor examplea technique like the software management method indicated to JP6-19707Bthe software use managing system indicated to JP6-28030Band the software management method indicated to JP6-95302B exists. The software management method indicated to above-mentioned JP6-19707B enables it to grasp the using state of software according to a software right holder etc. when using softwaresuch as a computer program which is intangible propertyand a video data. The software use managing system indicated to JP6-28030Buse of softwaresuch as a computer program which is intangible propertyand a video datais facedBuy an onerous program (after buyingit can be used for free)attach a priceprovide the data in which the amount of money which can be purchased is shown in the computer systemand in the case of onerous program purchase. Register with a table as a name of the available software in a same systemand, when reducing the data in which the amount of money concerned which can be purchased is shown by a software price and erasing registered software from this tableit is made to carry out renewal of an increase of the data



in which the amount of money in which this purchase is possible is shown according to a situation. The software management method indicated to above-mentioned JP6-95302B<TXF FR=0003 HE=250 WI=080 LX=1100 LY=0300>In order to collect a utilization charge when using softwaresuch as a computer program which is intangible propertyand a video dataaccording to actual utilization quantity (using frequency or utilization time) per onerous programIt is effective in the system in the case of carrying out "recording a user identification signal and a fee" with discernment of the used programand a program right holder being able to grasp the utilization charge of a program which he owns by collecting these recordsand collecting the program utilization charges according to the utilization quantity of the program.<BR>[0003]<BR>[Problem(s) to be solved by the Invention]Howeverthe system which distributes the digital contents mentioned above using a networkThe employment only on a personal computer is taken into considerationtherefore carrying can be done simplyand the system of enjoying the above-mentioned digital contents anywhere again never exists.<BR>[0004]On the other handthe technique given [ each ] in a gazette mentioned above delves into a latent demandand although it is advantageous to a market expansionit cannot say it as an economical system easily insufficiently as the copy of digital contentsor defense to unjust use.<BR>[0005]Thenthis invention is made in view of such a situationand is a thing.<BR>The purpose makes it possible to be able to \*\* and to enjoy digital contents anywhere alwaysIt is providing the digital contents distribution controlling method which also makes it possible to be equal to employment enough as the copy of digital contentsor defense to unjust useand to build an economical systema digital contents reproduction methodand a device.<BR><BR>[0006]<BR>[Means for Solving the Problem]According to this inventionin the distribution side of digital contents. A contents key which enciphered and compressedprocessed digital contents and was enciphered as these processed digital contentsHe is trying to distribute use gold collected based on contents usage information which transmitted accounting information furthermore enciphered to the communications-partner sideand has been transmitted from the communications-partner side to a right holderOn the other handby the reproduction side of digital contentsdecode the processed digital contents with a contents keyand it elongates and reproducesA technical problem mentioned above is solved by that a digital contents playback device of this invention is portableand performing a cut of accounting informationand generation of contents usage information according to use of contents simultaneouslyand transmitting this contents usage information to the distribution sideand being made.<BR>[0007]<BR>[Embodiment of the Invention]Hereafterthe desirable embodiment of this invention is describedreferring to drawings.<BR>[0008]Firstbefore giving the concrete contents of the digital contents distribution method of this inventiona digital contents reproduction methodand the deviceand explanation of compositionin order to make these understanding easyThe outline composition of the whole system and the operation method of a system with which this invention is applied are briefly explained using each figure from <A HREF="JP-A-H10-269289.files/000003.gif">drawing 1 </A>to <A HREF="JP-A-H10-269289.files/000009.gif">drawing 7</A>.<BR><DP N=0005><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>[0009]The rough composition of the whole system is shown in <A HREF="JP-A-H10-269289.files/000003.gif">drawing 1</A>.<BR>[0010]In this <A HREF="JP-A-H10-269289.files/000003.gif">drawing 1</A>user side 200 assumes that the digital contents playback device (it will be hereafter called the player 1) and what is called a personal computer (it will be hereafter called the user terminal 50) of this invention are held.<BR>[0011]Although the user terminal 50 is the usual personal computerThe various software which is used for this invention and which is mentioned later is stored as application softwareand whileit comes to connect the loudspeaker which is the display device and sound emission means which are displaying meansa keyboarda mouse which are information input meansetc. Via a networkthe system management company 210 and connection are possible for the user terminal 50 concernedand it has an interface means between the players 1and data transmission and reception are possible for it.<BR>[0012]The player 1 has composition as shown in <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2</A>.<BR>[0013]Although detailed explanation of the composition of this <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A>is mentioned laterThe player 1 concerned as the main components of the processing route of digital contentsIt has the common key cryptosystem decoder circuit 24 which decrypts the digital contents enciphered using a contents keythe expansion circuit 26 which is the expansion means

JPA\_1998-269289\_translation

which elongate the digital contents compressed and the D/A conversion circuit 27 which changes digital data into an analog signal at least. The decryption told to below is solving encryption. <BR>[0014]The information which shows the right information data and the operating condition of digital contents which this player 1 uses. (These information is hereafter called point usage information) The possession money data which is needed when using digital contents namely as the main components treating the billing data (it is hereafter called point information) etc. which are reduced whenever it uses digital contents It has at least the point usage information storing memory 29 which stores the above-mentioned point usage information and the point information storing memory 28 which stores the above-mentioned point information. <BR>[0015]This player 1 as composition for storing the various keys used for encryption and decryption which are mentioned later The common key storage memory 22 and the key storage memory 21 for communication It has the common code decoder circuit 24 and the open code decoder circuit 20 as composition for performing encryption and decryption using the key stored in these. This player 1 as composition relevant to the above-mentioned encryption and decryption It also has the security ID generating circuit 19 and the timer 18 which generate the random number interlocked with the host computer of the system management company 210 and generate security ID and the hash function circuit 25 grade which generates what is called a hash value mentioned later. <BR>[0016]In addition the player 1 concerned is <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> provided with the controller 16 which is a control means which performs digital contents various kinds of data in addition to this and control of each component based on the program stored in ROM 17 and the cell 5 as operation power at the time of carrying. <BR>[0017]Hereas for each main components of the player 1 of <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2</A> it is desirable on security to comprise one chip of IC (integrated circuit) or LSI (large scale integration circuit). In this <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2</A> 1 chip making of each main components is carried out into the integrated circuit 10. The player 1 concerned is equipped with three terminals (the analog output terminal 2 the interface terminal 3 for PC and the I/O terminal 4 for archive media) as an object for an interface with the exterior and these each terminal is connected to the terminals 13 12 and 11 in which the integrated circuit 10 corresponds respectively. These each terminal is possible also for also unifying and newly providing another terminal and is not scrupulous in particular. <BR>[0018]The system management company 210 consists of the control center 211 which manages the whole system and the store 212 which sells the above-mentioned player land via the virtual online shop 230 between the user terminals 50 of user side 200 transmission and reception of the information about supply of digital contents which is mentioned later processing of the digital contents which compress and encipher the contents which the content provider 240 holds the supply of digital contents processed [above-mentioned] the information transmission and reception between the financial institutions 220 etc. are performed. Between the system management company 210 and the financial institution 220 the exchange of the check of the account number of user side 200 a credit number a name a contact etc. the information on the ability to trade between user side 200 etc. etc. are performed. Processing of actual price transfer etc. is performed between the financial institution 220 and user side 200. The store 212 does not necessarily need to be included in the system management company 210 and may be a sales agent. <BR>[0019]The control center 211 of the above-mentioned system management company 210 has composition as shown for example in <A HREF="JP-A-H10-269289.files/000005.gif">drawing 3</A>. Although detailed explanation of the composition of this <A HREF="JP-A-H10-269289.files/000005.gif">drawing 3</A> is mentioned later As the main components manage digital contents and Processing treatments such as the exhibition encryption and compression The contents managing functional block 100 which has each function which is the key information used for encryption and decryption of digital contents such as a contents key and generating of ID Manage User Information and Encryption and decryption of correspondence (a message point information etc.) The user management functional block 110 provided also with the user subscription processing function part 118 which performs user subscription processing besides each functions such as generating of a confirmation message generating of security ID a settlement-of-accounts application between the financial institutions 230 generating of the point etc. It has at least the usage information controlling-function block 120 which manages point usage information

etc.and the controlling-function block 130 which manages the whole system and has a communication function.<BR>[0020]An <DP N=0006><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>example of the actual operation method of the system constituted like <A HREF="JP-A-H10-269289.files/000003.gif">drawing 1 </A>mentioned above is explained using <A HREF="JP-A-H10-269289.files/000006.gif">drawing 4 </A>- <A HREF="JP-A-H10-269289.files/000009.gif">drawing 7</A>. The following operation methods are procedures which user side 200the system management company 210the financial institution 220and content provider 240 grade actually follow.<BR>[0021]The procedure of the purchase of the player 1 in explanation of the operation method of this systemthe procedure from search of digital contents to installation of the digital contents to the memory medium for player 1The procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making the digital contents concerned usable and the procedure of distribution of the fee collection price collected from the user with appreciation of digital contents are explained in order.<BR>[0022]Firstas a procedure at the time of the purchase of the player 1as shown in (1) of <A HREF="JP-A-H10-269289.files/000006.gif">drawing 4</A>and (5)user side 200 actually purchases the above-mentioned player 1 from the above-mentioned store 212 by the shop front or mail order.<BR>[0023]Personal information (a namea contactetc.) and settlement information (a bank accounta credit numberetc.) which were provided from above-mentioned user side 200 at the time of sale of the above-mentioned player 1 at this time as the above-mentioned store 212 was shown in (2) of <A HREF="JP-A-H10-269289.files/000006.gif">drawing 4</A>The number (a player inherent key etc. are included) peculiar to the player 1 which sold [ above-mentioned ] is registered into the control center 211 of the system management company 210.<BR>[0024]As shown in (3) of <A HREF="JP-A-H10-269289.files/000006.gif">drawing 4</A>the control center 211 checks an account numbera credit numberetc. which were provided from above-mentioned user side 200 to the financial institution 220and as shown in (4) of <A HREF="JP-A-H10-269289.files/000006.gif">drawing 4</A>it acquires the information on the purport that it can trade from the financial institution 220.<BR>[0025]User side 200 [ next ] which purchased the above-mentioned player 1 as a procedure to installation of the digital contents from search of digital contents to the memory medium for player 1Using the user terminal 50 provided with the interface means with the player 1 concernedas shown in (1) of <A HREF="JP-A-H10-269289.files/000007.gif">drawing 5</A>search of the digital contents of hopeselectioneditan orderetc. are performed. Processing from the search at this time to an order is performed to the virtual online shop 230 where the user terminal 50 was connected via the network using the retrieval software stored as application software.<BR>[0026]The virtual online shop 230 is a store which the control center 211 has provided virtually on a networkfor exampleand the information which shows the contents of two or more contentsfor example is exhibited by this virtual online shop 230. User side 200 will place an order for desired contents based on these information provided in the virtual online shop 230. As information which shows the contents of the contents exhibited by the virtual online shop 230when contents are video datassuch as a moviefor exampleitles and advertisementssuch as the movie concernedImagessuch as one scene in the movie concernedetc. can be consideredand <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>when contents are audio informationa track namean artist namethe number phrase (what is called an intro) of the beginning of the music concernedetc. can be considered. Thereforewhen the above-mentioned virtual online shop 230 is accessed with the user terminal 50 of user side 200. The order of contents will be performed because the contents of two or more contents of the above-mentioned virtual online shop 230 are exhibited virtually and choose a desired thing out of these display objects on the user terminal 50 concerned.<BR>[0027]when there are an order of digital contentsetc. from the user terminal 50 of above-mentioned user side 200the above-mentioned virtual online shop 230 performs the supply request of digital contents to the control center 211as shown in (2) of <A HREF="JP-A-H10-269289.files/000007.gif">drawing 5</A>.<BR>[0028]The control center 211 which received the supply request of the digital contents concerned performs the distribution request of the digital contents which had the above-mentioned supply request to the content provider 240. Therebythe content provider 240 concerned supplies the digital contents which had the above-mentioned distribution request as shown in (4) of <A

HREF="JP-A-H10-269289.files/000007.gif">drawing 5 </A>to the control center 211.<BR>[0029]The control center 211 performs encryption and compression using predetermined compression technology to the digital contents rationed by the above-mentioned content provider 240and. The virtual-online-shop name etc. which supply charge amount and contents when right holder information and the contents concernedsuch as ID (content ID) of the contents concerned and an owner of a copyright of these contentsare used to user side 200 are added to these digital contents compressed and enciphered. The charge amount to contents is determined a priori by the content provider 240.<BR>[0030]The contents processed in the above-mentioned control center 211 are sent to the virtual online shop 230and as shown in (5) of <A HREF="JP-A-H10-269289.files/000007.gif">drawing 5</A>as shown in (6) of <A HREF="JP-A-H10-269289.files/000007.gif">drawing 5</A>they are further supplied to the user terminal 50 of user side 200 via this virtual online shop 230. By thiscontents will be supplied to the player 1 from the above-mentioned user terminal 50and these contents will be stored in the player 1 concerned.<BR>[0031]It is also possible to carry out to this <A

HREF="JP-A-H10-269289.files/000007.gif">drawing 5 </A>a priori about flowing to (2) - (5). That isit not only may exhibit the information which shows the contents of two or more above-mentioned contentsbut it may prepare beforehand for the virtual online shop 230 the digital contents corresponding to these exhibitions processed [ above-mentioned ].<BR>[0032]Nextin the procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making usable the digital contents installed in the player 1 as mentioned above. Firstwith the user terminal 50shortage of the point information stored in the player 1 is checkedand a supplement demand of point information is made from the user terminal 50 concerned.<BR>[0033]At this timeas shown in (1) of <A HREF="JP-A-H10-269289.files/000008.gif">drawing 6</A>from the <DP N=0007><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>user terminal 50 concernedthe supplement request of the point information enciphered by the player 1 is transmitted to the control center 211. Simultaneouslyit is read from the player 1is enciphered and is sent to the control center 211 via the user terminal 50a right holder's informationi.e.point usage informationcorresponding to the already used digital contentssuch as an owner of a copyright. Thustransmission of point usage information was made to be performed simultaneously with the supplement request of point informationin order that user side 200 might save the time and effort which accesses the control center 211 only for transmission to the control center 211 of the point usage information concerned. Of courseit is not necessary to necessarily perform transmission of this point usage information simultaneously with the purchase of point informationand may carry out independently.<BR>[0034]The control center 211 which received the supplement request and point usage information of point information which were enciphered [ above-mentioned ] recognizes the replenishing amount of point information and the contents of point usage information which user side 200 is demanding by decoding the code concerned. The control center 211 concerned checks [ of <A HREF="JP-A-H10-269289.files/000008.gif">drawing 6 </A>] whether as shown in (2)the settlement of accounts for the point supplement concerned is possible to the financial institution 220. From the financial institution 220 concerneda check accounts can be settled by investigating the account of user side 200 in the financial institution 220 will send directions of the settlement of accounts O.K. to the control center 211as shown in (3) of <A

HREF="JP-A-H10-269289.files/000008.gif">drawing 6</A>.<BR>[0035]The control center 211 at this time connects the point usage number which will be paid to right holderssuch as an owner of a copyrightto the content provider 240i.e.the amount of moneyas shown in (4) of <A HREF="JP-A-H10-269289.files/000008.gif">drawing 6</A>.<BR>[0036]Thenin the control center 211the letter missive of point supplementary information is encipheredand with security IDby making this into point supplement directions informationas shown in (5) of <A

HREF="JP-A-H10-269289.files/000008.gif">drawing 6</A>it sends to the user terminal 50. The above-mentioned point supplement directions information sent to the player 1 from this user terminal 50It is decrypted in the player 1 concerned and supplement of the point information on the point information storing memory 28 and deletion of right holder informationincluding the copyright information etc. which were connected to the above place from the point usage information storing memory 29are further performed after the check of security ID.<BR>[0037]Nextthe fee collection

JPA\_1998-269289\_translation

price collected from the user with appreciation of digital contentsThat is in the procedure of distribution of the price which will be charged directly to a user's account according to the usage information of a pointfirstas shown in (1) of <A HREF="JP-A-H10-269289.files/000009.gif">drawing 7</A>a price transfer request is made from the financial institution 220 to user side 200. When a price transfer request in particular is not made when there is sufficient balance for the account of user side 200 at this timeand there is not sufficient balance for an accountas shown in (2) of <A HREF="JP-A-H10-269289.files/000009.gif">drawing 7</A>transfer of a price is made from user side 200 to the financial institution 220.<BR>[0038]The financial institution 220 deducts a prescribed feeand as shown in (3) of <A HREF="JP-A-H10-269289.files/000009.gif">drawing 7</A>it <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>remits the price received from user side 200 to the control center 211. That is in the control center 211the charge of contents processinga financial feesystem management expenseetc. are collected from the above-mentioned price remitted from the financial institution 220. The control center 211 concerned pays the content provider 240 the royalty according to the point used previouslyas shown in (4) of <A HREF="JP-A-H10-269289.files/000009.gif">drawing 7</A>and as shown in (5) of <A HREF="JP-A-H10-269289.files/000009.gif">drawing 7</A>it pays a store fee to the virtual online shop 230. The content provider 240 who received the above-mentioned royalty pays each owner of a copyright a royaltyand the virtual online shop 230 which received the above-mentioned store fee pays the fee for every virtual online shop to each virtual online shop.<BR>[0039]Thus the price paid from user side 200Based on said point usage informationit is distributed to a royaltya store feea contents processing feea settlement-of-accounts feead a system management feethe above-mentioned royalty -- the content provider 240 -- the above-mentioned store fee -- the above-mentioned virtual online shop 230 -- pay the system management company 210 a contents processing feea settlement-of-accounts fee is paid to a system management company and the financial institution 220and a system management fee is paid to the system management company 210.<BR>[0040]Herein the case of the data transmission and reception between the systems of this embodimenti.e.the data transmission and reception between the control center 211 and the player 1 in order to secure the safety of data communicationsthe data encryption and decryption which communicate are performed. According to this invention embodimentit can respond as a method of encryption and decryption to both a common key encryption system and a public-key crypto system.<BR>[0041]In the embodiment of the inventionthe common key encryption system is adopted from a point of processing speed as a cipher system in the case of transmission of the variety of information of the above-mentioned digital contentssthe above-mentioned point usage informationpoint informationa message and security IDand others. The common keys used for encryption and decryption of these varieties of information differ corresponding to each informationrespectively. The common key used for decryption of the enciphered information which is transmitted from the control center 211 in the player 1 of said <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A>is kept by said common key storage memory 22said common code decoder circuit 24 decrypts the information enciphered from the above-mentioned control center 211 using the common key currently kept in this common key storage memory 22.<BR>[0042]The cipher system adopted by whether the player inherent key which is a peculiar key of said player 1 deals with which method as a cipher system in the case of transmission of the above-mentioned common key used for encryption and decryption of the above-mentioned variety of information on the other hand changes. That iswhen the above-mentioned player inherent key supports the common key encryption systemthe above-mentioned common key will be enciphered using the player inherent key concernedand the enciphered common key concerned will be decrypted using the above-mentioned player inherent key. On the other handwhen the above-mentioned player inherent key supports the public-key crypto systemthe <DP N=0008><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>public key of the partner point is used for encryption of the above-mentioned common keyand the secret key of the side which decryptsrespectively is used for decryption of the enciphered above-mentioned common key.<BR>[0043]For examplein the case where the above-mentioned common key (for examplesession key mentioned later) is sent to the control center 211 from the above-mentioned player 1when the above-mentioned player inherent key supports the common key encryption systemIn the above-mentioned player 1the above-mentioned common key encryptosystem decoder circuit 24 enciphers the above-mentioned common key using the player

inherent key which the key storage memory 21 for communication is keeping and the common key enciphered [ above-mentioned ] is decrypted in the control center 211 using the player inherent key which the control center 211 concerned is keeping. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the control center 211 from the above-mentioned player 1 for example. The above-mentioned public-key-encryption decoder circuit 20 enciphers the above-mentioned common key in the public key of the control center 211 which the \*\* key storage memory 21 for communication of the above-mentioned player 1 is keeping and the common key enciphered [ above-mentioned ] is decrypted in the control center 211 using the secret key which the control center 211 concerned is keeping. [0044] On the contrary when the above-mentioned common key (for example contents key) is sent to the player 1 for example from the above-mentioned control center 211 and the above-mentioned player inherent key supports the common key encryption system. The above-mentioned common key is enciphered with the player inherent key which the above-mentioned control center 211 is keeping and said common code decoder circuit 24 decrypts the common key enciphered [ above-mentioned ] using the player inherent key currently kept by the above-mentioned key storage memory 21 for communication in the player 1. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the player 1 from the above-mentioned control center 211 for example. The above-mentioned common key is enciphered in the public key of the player 1 which the above-mentioned control center 211 is keeping and said open code decoder circuit 20 decrypts the common key enciphered [ above-mentioned ] using the player inherent key i.e. the secret key which are kept by the above-mentioned key storage memory 21 for communication in the player 1. [0045] The cipher system of the player inherent key itself [ which was mentioned above ] is determined by whether delivery (delivery to the player 1 from the system management company 210) of the player inherent key concerned is easy. That is since the common key encryption system is more advantageous in cost if delivery of a player inherent key is easy a common key encryption system will be adopted but when delivery of the player inherent key concerned is difficult it is a high cost but a public-key crypto system is adopted. In mounting a player inherent key in hardware and mounting a common key encryption system in software it adopts a public-key crypto system. [0046] Hereafter in an embodiment of the invention the example which adopts the above-mentioned public-key crypto system will be given and explained in consideration of the compatibility in the case of mounting in software as a cipher system of a player inherent key itself. Namely <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> in the case where transmission of said common key is performed between the above-mentioned control center 211 and the player 1 when a common key (session key) is enciphered by the above-mentioned player 1 side encryption is made using the public key of the control center 211 and the common key enciphered [ above-mentioned ] using the above-mentioned player inherent key (namely secret key) is decrypted in the control center 211. On the contrary when a common key (contents key) is enciphered by the above-mentioned control center 211 side encryption is made in the public key of a player and the common key enciphered [ above-mentioned ] using the above-mentioned player inherent key (namely secret key) is decrypted in the player 1. [0047] Actual operation of the above-mentioned player 1 the user terminal 50 and the control center 211 which constitute the system employed using each procedure and a cipher system which were mentioned above is explained in order below. [0048] First it explains referring to said <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A> and <A HREF="JP-A-H10-269289.files/000005.gif">drawing 3 </A> for flowing into the processing in the player 1 at the time of the point supplement i.e. point purchase which were mentioned above the user terminal 50 and the control center 10 using <A HREF="JP-A-H10-269289.files/000013.gif">drawing 11 </A> from <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8 </A>. [0049] The flow of the processing in the player 1 at the time of purchasing the point is shown in <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8 </A>. [0050] In this <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8 </A> starting of the software for point purchase beforehand installed in the user terminal 50 i.e. a personal computer is performed by step ST11 it is waiting for the controller 16 of the player 1 in the meantime until the software for the point purchase concerned rises. [0051] If the software for the above-mentioned point purchase rises the controller 16 of the player

1 will receive the information inputted into the above-mentioned user terminal 50 from the user terminal 50 concerned in step ST2. An input request is made from the user terminal 50 concerned to the user who operates the above-mentioned user terminal 50 according to the software for the above-mentioned point purchase and the information inputted into the user terminal 50 at this time is information including a password a point information number to purchase etc. [0052] The information from these user terminals 50 is received by the controller 16 via the terminal 12 of the integrated circuit 10 by which 1 chip making was carried out into the interface terminal 3 for PC of the player 1 and the player 1 concerned. The controller 16 which received the information from the user terminal 50 concerned in step ST3 comparison with the password which the password storing memory 14 in the integrated circuit 10 of the player 1 concerned stores and the password in the information which received [above-mentioned] is performed and the above-mentioned receiving password checks that it is the right. [0053] The above-mentioned password the right and the checked controller 16 at the same time it generates the information on the purport that he would like to purchase the point in step ST4 (main point of point purchase) and a point information number to purchase and other information Security ID is generated from the security ID generating circuit 19 and these information is made to encipher by the common code decoder circuit 24 in the following step ST5. The controller 16 <DP N=0009><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> reads user ID from the user ID storing memory 23 in step ST6 next It adds to the information which enciphered [above-mentioned] the user ID concerned and the data which added and created the user ID concerned in step ST7 is further transmitted to the user terminal 50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50 the above-mentioned prepared data will be sent to the control center 211. [0054] Since the common key encryption system is adopted as encryption of the above-mentioned prepared data at this time as mentioned above generation of a common key is performed in advance of transmission of the prepared data concerned. For this reason in the above-mentioned controller 16 a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation means for example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto system herein the above-mentioned controller 16. The public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken out and it sends to the above-mentioned open code decoder circuit 20 at the same time it sends the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concerned encryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus with user ID the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data. [0055] As mentioned above when also performing transmission of point usage information with a demand of point information the controller 16 reads point usage information including said right holder information from the point usage information storing memory 29 and these also make the above-mentioned common code decoder circuit 26 send and encipher it. This enciphered point usage information is transmitted with the above-mentioned prepared data. Simultaneously with transmission of point usage information it is also possible to transmit the balance of point information similarly. [0056] Then the controller 16 receives the data which has been sent from the control center 211 through the user terminal 50 in step ST8 and which is enciphered. The data sent from this control center 211 is the data in which the point information and information including security ID etc. according to the above-mentioned point information number previously transmitted from the player 1 concerned to purchase were enciphered using the same common key as the above-mentioned session key. [0057] If the data from the above-mentioned control center 211 is received in step ST9 it sends the data concerned to the above-mentioned common code decoder circuit 24 and the controller 16 will read said common key which was generated previously and kept in the common key storage memory 22 and similarly will send it to the common code decoder circuit 24. In the common code decoder circuit 24 concerned the data enciphered from the above-mentioned control center 211 using the above-mentioned common key is <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> decrypted. [0058] Next security ID of the data in which the above-mentioned

controller 16 was decrypted [ above-mentioned ] in step ST10the point information which checked by comparison with security ID from the above-mentioned security ID generating circuit 19and was stored in the above-mentioned point information storing memory 28 in step ST11 after the check -- the above -- it corrects for the newly sent point information.<BR>[0059]After processing of correction of the above-mentioned point informationetc. is completedthe controller 16 generates the sign of processing completionsends it to the above-mentioned common code decoder circuit 24 with the common key read from the above-mentioned common key storage memory 22and is made to encipher by the common code decoder circuit 24 concerned in step ST12. Then the controller 16 transmits the sign of the enciphered processing completion concerned to the user terminal 50 via the terminals 12 and 3 in step ST13and sends it to the control center 211.<BR>[0060]By the abovethe flow of the processing in the player 1 in the case of point purchase is completed.<BR>[0061]Nextthe flow of the processing in the user terminal 50 at the time of the above-mentioned point purchase is explained using <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>.<BR>[0062]In this <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>the user terminal 50 starts the software for point purchase in step ST21. When the software for point purchase concerned risesin this user terminal 50. The input request of informationincluding the password mentioned above to the user who operates the user terminal 50 concerned in step ST22 according to the software for the above-mentioned point purchasea point size to purchaseetc.is performedIf these information is inputted from a userthe inputted information concerned will be transmitted to the above-mentioned player 1 like step ST2 of said <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8</A>.<BR>[0063]Nextthe user terminal 50 will transmit the data transmitted from the player 1 concerned in step ST24if the data created like step ST7 of said <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8 </A>from the above-mentioned player 1 in step ST23 is receivedthe address 211i.e.the control centerwhich are registered beforehand.<BR>[0064]If the user terminal 50 after performing the above-mentioned data transfer has the data return from waiting and the control center 211 in the return from the control center 211it will transmit the data from the control center 211 concerned to the player 1 as it is in step ST25.<BR>[0065]If the sign of processing completion is received like step ST13 of said <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8 </A>from the above-mentioned player 1 in step ST26in order to tell a user about processing of the point purchase concerned etc. having been completedthe user terminal 50 concernedThe sign of processing completion is displayed on a display in step ST27and a user is made to check.<BR>[0066]Then the user terminal 50 concerned <DP N=0010><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>transmits the cryptogram of the sign of the processing completion sent from the above-mentioned player 1 to the control center 211.<BR>[0067]By the abovethe flow of the processing in the user terminal 50 in the case of point purchase is completed.<BR>[0068]Nextthe flow of the processing in the control center 211 at the time of point purchase is explained using <A HREF="JP-A-H10-269289.files/000012.gif">drawing 10</A>.<BR>[0069]In this <A HREF="JP-A-H10-269289.files/000012.gif">drawing 10</A>the control center 211 like step ST31The data enciphered [ above-mentioned ] from the player 1 transmitted via the user terminal 50 by the communication function section 133 of the controlling-function block 130 by which the whole is controlled like step ST7 of said <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8 </A>and step ST24 of <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9 </A>in the control function part 131 is received. When this data is receivedthe user management functional block 110 of the control center 211Based on the user ID attached to the received data concerneda common key comes to hand from the database section 112 under control of the control function part 111 like step ST32and security ID comes to hand from the security ID generating function part 116.<BR>[0070]The common key at this time is said session key beforehand sent from said player 1and this session key is enciphered and sent with a public-key crypto system as mentioned above. Thereforeat the time of decoding of this session key enciphered. In the user management functional block 110 of the control center 211 concernedthe secret key of the public-key crypto system of the above-mentioned control center 211 is taken outand the session key enciphered [ above-mentioned ] with this secret key is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerneddecryption of a session key enciphered [



above-mentioned ] using the public key of the above-mentioned control center 211 is performed. Thus the obtained session key (common key) is stored in the above-mentioned database section 112. <BR>[0071] If the common key corresponding to the above-mentioned user ID comes to hand from the above-mentioned database section 112 and security ID comes to hand from the security ID generating function part 116 as shown in step ST33 in the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211. Further in [ decrypt the data enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common key and ] the control function part 111 comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned security ID generating function part 116 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed. <BR>[0072] In the control center 211 which checked the justification of the above-mentioned access origin. Like step ST34 by the point generating function part 113 of the user management functional block 110. The point information according to the contents of the data sent from the above-mentioned user terminal 50 is published and the <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> claim preparations to a user's settlement-of-accounts organization (financial institution 220) are made by the settlement-of-accounts claim function part 117. <BR>[0073] Like step ST35 in the control function part 111 the control center 211 checks that there is no injustice in the balance and point usage information of point information from the player land performs the conclusion of information for next processing. That is a check and conclusion of whether there is any unjust use are performed from the balance of point information and the number of the actually used point information. It is better to perform this check and conclusion desirably although it must not carry out. <BR>[0074] In the user management functional block 110 of the control center 211 like step ST36 after processing of above-mentioned step ST35 again in the security ID generating function part 115 new security ID to the above-mentioned player 1 (user) is computed based on a random number generation and above-mentioned security ID is enciphered with the above-mentioned point information in the control function part 110 further for example. Encryption at this time is also performed using said session key (common key) sent beforehand from said player 1. <BR>[0075] An end of the above-mentioned encryption will transmit the data which enciphered [ above-mentioned ] to the player 1 via the user terminal 50 under control of the control function part 131 like step ST25 of said <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A> and step ST8 of <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8</A> in the communication function section 133 of the controlling-function block 130 of the control center 211. <BR>[0076] Then in the communication function section 133 of the control center 211 like step ST38 when the processing completion sign from the user terminal 50 shown in step ST28 of said <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A> is received and decrypted in the settlement-of-accounts claim function part 117 of the user management functional block 110 of the control center 211 like step ST39 the financial institution 220 is asked for settlement of accounts based on the processing completion sign concerned. The settlement-of-accounts claim to this financial institution 220 is performed from the communication function section 132 of the controlling-function block 130. <BR>[0077] By the above the flow of the processing in the control center 211 in the case of point purchase is completed. <BR>[0078] From <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8</A> mentioned above the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of <A HREF="JP-A-H10-269289.files/000012.gif">drawing 10</A> and the control center 211 can be expressed as shown in <A HREF="JP-A-H10-269289.files/000013.gif">drawing 11</A>. <BR>[0079] That is in this <A HREF="JP-A-H10-269289.files/000013.gif">drawing 11</A> inputs such as said password and a point size is transmitted from the user terminal 50 to the player 1 by the input transmission T1 like step ST2 of said <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8</A> and step ST22 of <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>. <BR>[0080] In the prepared data transmission T2 the data created from the player 1 by said player 1 to the user terminal 50 is transmitted like step ST7 of said <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8</A> and step ST23 of <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>. In data transfer T3 the <DP N=0011><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> data which said player 1 created

JPA\_1998-269289\_translation

from the user terminal 50 to the control center 211 is transmitted like step ST24 of said <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>and step ST31 of <A HREF="JP-A-H10-269289.files/000012.gif">drawing 10</A>. <BR>[0081]In the data transfer T4the data enciphered from the control center 211 to the user terminal 50 in the control center 211 is transmitted like step ST37 of said <A HREF="JP-A-H10-269289.files/000012.gif">drawing 10</A>and step ST25 of <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>. In the transmission T5the data from the control center 211 is transmitted to the user terminal 50 by the player 1 as it is like step ST25 of said <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>and step ST8 of <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8</A>. <BR>[0082]In the processing completion sign transmission T6the processing completion sign from the player 1 is transmitted to the user terminal 50 like step ST13 of said <A HREF="JP-A-H10-269289.files/000010.gif">drawing 8</A>and step ST26 of <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>. In processing completion sign cryptogram transmissionthe processing completion sign enciphered from the player 1 is transmitted to the control center 211 like step ST28 of said <A HREF="JP-A-H10-269289.files/000011.gif">drawing 9</A>and step ST38 of <A HREF="JP-A-H10-269289.files/000012.gif">drawing 10</A>. <BR>[0083]Nextit explains from <A HREF="JP-A-H10-269289.files/000014.gif">drawing 12 </A>flowing into the processing in the player 1 at the time of acquisition of the digital contents mentioned abovethe user terminal 50and the control center 211 using <A HREF="JP-A-H10-269289.files/000017.gif">drawing 15</A>referring to <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A>and <A HREF="JP-A-H10-269289.files/000005.gif">drawing 3</A>. <BR>[0084]The flow of the processing in the player 1 at the time of acquisition of digital contents is shown in <A HREF="JP-A-H10-269289.files/000014.gif">drawing 12</A>. <BR>[0085]In this <A HREF="JP-A-H10-269289.files/000014.gif">drawing 12</A>it is waiting for the controller 16 until starting of the software for digital contents acquisition beforehand installed in the user terminal 50i.e.a personal computeris performed like step ST41.<BR>[0086]If the software for the above-mentioned digital contents acquisition rises the controller 16 will receive the data which contains digital contents from the control center 211 via the user terminal 50 like step ST42. It has at least the digital contents enciphered with the contents key (a different common key for every contents) as having mentioned above the data received via the terminals 3 and 12 from the user terminal 50 at this timeand the content ID corresponding to the digital contents concerned. thereforein order to use these enciphered digital contentsa contents key comes to hand from the control center 211 -- if it kicksit will not become. The method of acquisition of this contents key is mentioned later.<BR>[0087]The controller 16 which received the data from this user terminal 50 stores this datai.e.the enciphered digital contentsin the memory medium connected to the I/O terminal 4 for memory media via the terminal 11 of the integrated circuit 10. Although various kinds of storagessuch as a rewritable optical disc and semiconductor memorycan be considered as this memory mediumthe thing in which random access is possible is desirable.<BR><TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>[0088]By the abovethe flow of the processing in the player 1 at the time of acquisition of digital contents is completed.<BR>[0089]Nextthe flow of the processing in the user terminal 50 at the time of acquisition of digital contents is explained using <A HREF="JP-A-H10-269289.files/000015.gif">drawing 13</A>. <BR>[0090]In this <A HREF="JP-A-H10-269289.files/000015.gif">drawing 13</A>the user terminal 50 starts the software for digital contents acquisition in step ST51. If the software concerned risesin this user terminal 50the control center 211 of the address beforehand registered in step ST52 according to the software for the above-mentioned digital contents acquisition will be accessed.<BR>[0091]At this timethe control center 211 concerned is exhibiting two or more digital contents using said virtual online shop 230. From the user terminal 50the digital contents of the request according to the selection operation of the user out of two or more digital contents currently exhibited by this virtual online shop 230 in step ST53 are specified. That isthe user terminal 50 transmits the specification information on the contents for specifying the digital contents of the request in the digital contents exhibited by the virtual online shop 230 like step ST54 to the control center 211.<BR>[0092]If the data which consists of data returned from the control center 211 according to the above-mentioned contents designation informationi.e.said

enciphered digital contents and content ID like step ST55 is received. The user terminal 50 concerned once stores the above-mentioned data in storing means such as an inside for example a hard disk and a memory like step ST56. [0093] Then the user terminal 50 transmits the stored data (digital contents and content ID which were enciphered) concerned to the player 1 like step ST42 of said <A HREF="JP-A-H10-269289.files/000014.gif">drawing 12</A>. [0094] By the above the flow of the processing in the user terminal 50 at the time of acquisition of digital contents is completed. [0095] Next the flow of the processing in the control center 211 at the time of digital contents acquisition is explained using <A HREF="JP-A-H10-269289.files/000016.gif">drawing 14</A>. [0096] The control center 211 shown in <A HREF="JP-A-H10-269289.files/000005.gif">drawing 3 </A> is making the virtual online shop 230 mentioned above exhibit two or more contents here. In the contents managing functional block 100 of control center 211 \*\*said virtual online shop 230 is generated and specifically two or more above-mentioned digital contents are exhibited to this virtual online shop 230. [0097] Thus in the state where digital contents are exhibited to the virtual online shop 230 contents designation information is received from the user terminal 50 like step ST61 of <A HREF="JP-A-H10-269289.files/000016.gif">drawing 14 </A> step ST54 of said <A HREF="JP-A-H10-269289.files/000015.gif">drawing 13</A>. [0098] If the above-mentioned contents designation information is received from the user terminal 50 concerned the <DP N=0012><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> control function part 101 of the contents managing functional block 100 will send this contents designation information to the controlling-function block 130. The control function part 131 of the controlling-function block 130 lets the communication function section 134 for right holders pass and transmits the contents designation information received from the above-mentioned control controlling-function block 100 to said content provider 240. Thereby from the content provider 240 concerned the digital contents demanded in the above-mentioned contents designation information are transmitted. The digital contents which came to hand from the above-mentioned content provider 240 are sent to the contents managing functional block 100 from the controlling-function block 130 and are inputted into this contents code and compression-ized function part 104. At this time the control function part 101 sends the contents key which is generated in a contents key and the ID generating function part 103 and is stored in the database 102 to above-mentioned contents code and compression-ized function part 104. In this contents code and compression-ized function part 104 encryption using the above-mentioned contents key is given to the above-mentioned digital contents and further predetermined compression processing is performed. The control function part 101 adds the content ID taken out from the database 102 to the digital contents by which above encryption and compression processing were carried out and sends it to the controlling-function block 130. As predetermined compression processing in case digital contents are audio signals for example like what is called ATRAC (Adaptive Transform Acoustic Coding) that is the art currently used in what is called MD (mini disc: trademark) produced commercially in recent years processing which carries out highly efficient compression of the audio information in consideration of human being's aural characteristic was made into an example -- it can mention. [0099] Then as shown in step ST62 of <A HREF="JP-A-H10-269289.files/000016.gif">drawing 14</A> the control section 131 of the controlling-function block 130 transmits the digital contents to which it let the communication function section 133 with a user terminal pass and it enciphered [above-] and processed [compression-] and content ID was added to the above-mentioned user terminal 50. [0100] The flow of the processing in the control center 211 at the time of digital contents acquisition is above. [0101] From <A HREF="JP-A-H10-269289.files/000014.gif">drawing 12 </A> mentioned above the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of <A HREF="JP-A-H10-269289.files/000016.gif">drawing 14</A> and the control center 211 can be expressed as shown in <A HREF="JP-A-H10-269289.files/000017.gif">drawing 15</A>. [0102] That is in this <A HREF="JP-A-H10-269289.files/000017.gif">drawing 15</A> said contents designation information is transmitted from the user terminal 50 to the control center 211 like step ST54 of said <A HREF="JP-A-H10-269289.files/000015.gif">drawing 13 </A> by the input transmission T11. In the contents transfer T12 the digital contents and content ID which were enciphered are transmitted to the user terminal 50 like step ST62 of said <A

JPA\_1998-269289\_translation

href="JP-A-H10-269289.files/000016.gif">drawing 14 </A>from the control center 211.<br>[0103]In the contents transfer T13the <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>digital contents and content ID which were once stored in the user terminal 50 and which were enciphered [ above-mentioned ] are transmitted to the player 1 like step ST57 of said <A href="JP-A-H10-269289.files/000015.gif">drawing 13</A>and step ST42 of <A href="JP-A-H10-269289.files/000014.gif">drawing 12</A>.<br>[0104]Nextit explains from <A href="JP-A-H10-269289.files/000018.gif">drawing 16 </A>flowing into the processing in the contents key which is needed when using the digital contents mentioned above the player 1 at the time of acquisition of the service condition and the user terminal 50and the control center 211 using <A href="JP-A-H10-269289.files/000021.gif">drawing 19</A>referring to <A href="JP-A-H10-269289.files/000004.gif">drawing 2 </A>and <A href="JP-A-H10-269289.files/000005.gif">drawing 3</A>.<br>[0105]The flow of the processing in the player 1 at the time of acquisition of a contents key and a service condition is shown in <A href="JP-A-H10-269289.files/000018.gif">drawing 16</A>.<br>[0106]In step ST71 of this <A href="JP-A-H10-269289.files/000018.gif">drawing 16</A>in the controller 16 of the player 1it is waiting until starting of the software the contents key beforehand installed in the user terminal 50 and for service-condition acquisition is performed.<br>[0107]If the above-mentioned contents key of the above-mentioned user terminal 50 and the software for service-condition acquisition risethe information inputted into the user terminal 50 according to the software concerned will be received like step ST72 via said interface terminal 3 for PCand the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is information for requiring a contents key required to solve encryption of digital contents to appreciate. In this examplethe specification information on the digital contents which use this contents key is used as demand information on the above-mentioned contents key.<br>[0108]The controller 16 which received this contents designation information from the above-mentioned user terminal 50ID of the digital contents specified in the contents designation information concerned and security ID from the security ID generating circuit 19 are createdand this created data is made to encipher by the common code decoder circuit 24 in step ST73. The controller 16 adds the user ID read from the user ID storing memory 23 to the created data concernedand transmits it to the user terminal 50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50the above-mentioned prepared data will be sent to the control center 211.<br>[0109]Since the common key encryption system is adopted also as encryption of the prepared data at this time as mentioned abovein advance of transmission of the prepared data concernedgeneration of a common key is performed to it. For this reasonin the above-mentioned controller 16a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation meansfor example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto systemin the above-mentioned controller 16. The <DP N=0013><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken outand it sends to the above-mentioned open code decoder circuit 20 at the same time it sends the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concernedencryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data.<br>[0110]Then the controller 16 receives the enciphered data which has been sent from the control center 211 via the user terminal 50 in step ST75 so that it may mention later. The above-mentioned contents keya service conditionsecurity IDetc. are enciphered as mentioning later the data sent from the control center 211 at this time.<br>[0111]If the data enciphered from the above-mentioned control center 211 is receivedin the player 1the data enciphered [ above-mentioned ] will be decrypted like step ST76and the justification of the data will be checked. That is the controller 16 evaluates the justification by checking security ID of the data decrypted [ above-mentioned ]

by comparison with security ID from the above-mentioned security ID generating circuit 19. <BR>[0112] Here encryption is made with a public-key crypto system so that a contents key may be mentioned later and about a service condition and security ID encryption is made with the common key encryption system. Therefore in order to decrypt the contents key concerned enciphered the secret key of a public-key crypto system is required and since the player inherent key is used as a secret key as mentioned above in the player 1 of this embodiment the player inherent key concerned is taken out from the key storage memory 21 for communication. This player inherent key is sent to the open code decoder circuit 20 with the contents key enciphered [ above-mentioned ]. In this open code decoder circuit 20 the contents key enciphered [ above-mentioned ] is decrypted using the above-mentioned player inherent key. The contents key decrypted in this way is kept by the common key storage memory 22. On the other hand in decrypting the service condition and security ID which are enciphered with the above-mentioned common key encryption system these data is sent to the above-mentioned common code decoder circuit 24 and said common key which was generated previously and kept in the common key storage memory 22 is read and similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned the above-mentioned service condition and security ID are decrypted using the above-mentioned common key. The service condition decrypted in this way is stored in the point usage information storing memory 29. It is important here that the decrypted contents key and the service condition concerned are not taken out from the exterior of the player 1 concerned the controller 16 specifically formed in the integrated circuit 10 of <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A> or the common key storage memory 22 and the point usage information storing memory 29 outside. <BR>[0113] The controller 16 <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> makes the contents key which decoded [ above-mentioned ] store in the above-mentioned common key storage memory 22 with the above-mentioned content ID like step ST77 after the check of the above-mentioned justification. <BR>[0114] Then the controller 16 creates the message which shows that the above-mentioned contents key came to hand in step ST78. This message is sent to the common key encryption system decoder circuit 24 like the above-mentioned and said common key which was generated beforehand and kept in the common key storage memory 22 is read and similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned a message is enciphered using the above-mentioned common key. <BR>[0115] After encryption of the message concerned is completed the controller 16 transmits this enciphered message to the user terminal 50 via the terminals 12 and 3 like step ST79. This enciphered message is made to transmit to the control center 211 after that. <BR>[0116] By the above the flow of the processing in the player 1 at the time of a contents key and service-condition acquisition is completed. <BR>[0117] Next the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is explained using <A HREF="JP-A-H10-269289.files/000019.gif">drawing 17 </A>. <BR>[0118] In this <A HREF="JP-A-H10-269289.files/000019.gif">drawing 17 </A> the user terminal 50 starts the software for a contents key and service-condition acquisition in step ST81. If the designation input demand of the contents of hope is performed and specification of contents is made from a user to the user who will operate the user terminal 50 concerned in step ST82 with this user terminal 50 according to the above-mentioned software if the software concerned rises that specification information will be generated. The user terminal 50 transmits the specification information on the above-mentioned contents to the player 1 in the above-mentioned step ST83. <BR>[0119] Next if the data created and transmitted by the above-mentioned player 1 like step ST74 of said <A HREF="JP-A-H10-269289.files/000018.gif">drawing 16 </A> in step ST84 is received the user terminal 50 the data transmitted from the player 1 concerned in step ST85 is transmitted to the control center 211 where the address is registered beforehand. <BR>[0120] The user terminal 50 after performing a data transfer to the above-mentioned control center 211 if there is return of the data in which the contents key and service condition specified by the above-mentioned content ID from the control center 211 in waiting and step ST86 security ID etc. were enciphered the return from the control center 211 the data from the control center 211 concerned is transmitted to the player 1 as it is in step ST87. <BR>[0121] The user terminal 50 after performing a data transfer to the above-mentioned player 1 the return from the player 1 in waiting and step ST88 like step ST79 of said <A

JPA\_1998-269289\_translation

HREF="JP-A-H10-269289.files/000018.gif">drawing 16 </A>from the player 1 if there is return of the message as which it was enciphered that the above-mentioned contents key came to hand it will indicate that the above-mentioned contents key acquisition was completed to the display device connected to the user terminal 50 concerned in step ST89 and a user will be told.<BR><DP N=0014><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>[0122]Then the message which was returned from the above-mentioned player 1 and which was enciphered [ above-mentioned ] is sent to the control center 211 in step ST90.<BR>[0123]By the above the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is completed.<BR>[0124]Next the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is explained using <A HREF="JP-A-H10-269289.files/000020.gif">drawing 18</A>.<BR>[0125]In this <A HREF="JP-A-H10-269289.files/000020.gif">drawing 18</A>the communication function section 133 with the user terminal of the control center 211The encryption data of the content ID transmitted to the user terminal 50 from the player 1 via \*\* in step ST91 like step ST74 of said <A HREF="JP-A-H10-269289.files/000018.gif">drawing 16</A>and step ST85 of <A HREF="JP-A-H10-269289.files/000019.gif">drawing 17</A>user ID a message and security ID is received. This received data is sent to the user management functional block 110.<BR>[0126]The control function part 111 of the user management functional block 110 concerned based on the user ID added to the encryption data which received [ above-mentioned ] the common key for solving the encryption concerned is taken out from the database section 112 and the above-mentioned encryption data is decoded using this common key in a correspondence code and the function decoding part 114. The control function part 111 checks the justification of the data which was received [ above-mentioned ] and decrypted using the user ID and security ID from the security ID generating function part 116 which were read from the database section 112.<BR>[0127]The common key at this time is said session key beforehand sent from said player 1 and this session key is enciphered and sent with a public-key crypto system as mentioned above. Therefore at the time of decoding of this session key enciphered. Like the above-mentioned in the control center 211 concerned the secret key of the public-key crypto system of the above-mentioned control center 211 is taken out and the session key enciphered [ above-mentioned ] is decrypted using the secret key concerned in a correspondence code / the function decoding part 114 concerned. Thus the obtained session key (common key) is stored in the above-mentioned database section 112.<BR>[0128]When the justification of the data which received [ above-mentioned ] is checked the control function part 111The contents key and service condition which were specified in the above-mentioned content ID to the contents managing functional block 100 are requiredThe control function part 101 of the contents managing functional block 100 which received the demand concerned reads the contents key and service condition which were specified in the above-mentioned content ID from the database section 102 and transmits them to the user management functional block 110. The control function part 111 sends these contents keys and a service condition to a correspondence code / function decoding part 114 with security ID as shown in step ST93.<BR>[0129]Here encryption is made with the public-key crypto system mentioned above about the contents key and <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>encryption is made with the common key encryption system mentioned above about a service condition and security ID. Therefore when enciphering the contents key concerned the public key (public key beforehand stored corresponding to the player 1) of user side 200 is taken out from said database section 112 based on the above-mentioned user ID and it is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerned the above-mentioned contents key is enciphered using the above-mentioned public key. On the other hand when enciphering the above-mentioned service condition and security ID the common key (session key) specified by the above-mentioned user ID is taken out from the above-mentioned database section 112 and it is sent to a correspondence code / function decoding part 114. In the correspondence code / function decoding part 114 at this time the above-mentioned service condition and security ID are enciphered using the above-mentioned common key.<BR>[0130]The contents key the service condition and security ID which were enciphered [ above-mentioned ] are sent to the controlling-function block 130 and are transmitted to the user terminal 50 from the communication function section 133 with a user terminal like step ST94. The data transmitted to this user terminal 50 will be sent to the player 1 via the user

terminal 50 like step ST87 of said <A HREF="JP-A-H10-269289.files/000019.gif">drawing 17</A> and step ST75 of <A HREF="JP-A-H10-269289.files/000018.gif">drawing 16</A>. <BR>[0131] Reception of the encryption message which the control center 211 was generated by the player 1 like step ST79 of said <A HREF="JP-A-H10-269289.files/000018.gif">drawing 16</A> and step ST90 of <A HREF="JP-A-H10-269289.files/000019.gif">drawing 17</A> and was transmitted via the user terminal 50. Then waiting when the above-mentioned communication function section 133 receives the encryption message which the above-mentioned player 1 generated like step ST95 the control center 211 concerned. Like step ST96 the encryption message concerned is decrypted with a common key and it checks that the above-mentioned player 1 has obtained the contents key and the service condition from the decoding message. <BR>[0132] By the above the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is completed. <BR>[0133] From <A HREF="JP-A-H10-269289.files/000018.gif">drawing 16</A> mentioned above the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of <A HREF="JP-A-H10-269289.files/000020.gif">drawing 18</A> and the control center 211 can be expressed as shown in <A HREF="JP-A-H10-269289.files/000021.gif">drawing 19</A>. <BR>[0134] That is in this <A HREF="JP-A-H10-269289.files/000021.gif">drawing 19</A> said contents designation information is transmitted from the user terminal 50 to the player 1 like step ST83 of said <A HREF="JP-A-H10-269289.files/000019.gif">drawing 17</A> by the contents-designation-information transmission T21. In the prepared data transmission T22 the data created by the player 1 is transmitted to the user terminal 50 like above step ST74. In the prepared data transmission T23 the data created by the above-mentioned player 1 from the user terminal 50 concerned is transmitted to the control center 211. In the enciphered data sending T24 the data enciphered in the control center 211 is sent to the user terminal 50 like step ST94 of said <A HREF="JP-A-H10-269289.files/000020.gif">drawing 18</A> and the <DP N=0015><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> enciphered data concerned is further sent to the player 1 by the enciphered data sending T25. <BR>[0135] In the message transfer T26 like step ST79 of said <A HREF="JP-A-H10-269289.files/000018.gif">drawing 16</A> in the data sending T27 as which the data which enciphered the message which shows the completion of contents key acquisition was transmitted to the user terminal 50 from the player 1 and was enciphered further the message enciphered from the above-mentioned player 1 is sent to the control center 211 from the user terminal 50. <BR>[0136] Next in the player 1 which received point information digital contents and a contents key as mentioned above it explains flowing into the processing at the time of actually appreciating digital contents using the user terminal 50 using <A HREF="JP-A-H10-269289.files/000022.gif">drawing 20</A> referring to <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2</A>. <BR>[0137] Here it is assumed that the memory medium said digital contents were remembered to be is connected to the terminal 4 of the player 1. <BR>[0138] In this state the digital contents which wish to appreciate from the user terminal 50 are specified to the player 1 concerned like step ST101. At this time the specification concerned is made when a user operates the user terminal 50 for example. <BR>[0139] Like step ST102 according to the contents designation information from the above-mentioned user terminal 50 the controller 16 of the player 1 performs access to the above-mentioned memory medium and reads ID of contents at this time. <BR>[0140] Based on the content ID read in the above-mentioned memory medium the above-mentioned controller 16 like step ST103 it accesses to said common key storage memory 22 and it checks whether the contents key is stored and accesses to said point usage information storing memory 29 and it is checked whether the service condition is stored. <BR>[0141] When it checks here that the above-mentioned contents key and the service condition are not stored in the above-mentioned common key storage memory 22 or the point usage information storing memory 29 the controller 16 the information on the purport that the contents key concerned etc. do not exist to the user terminal 50 is sent and this displays the message which stimulates acquisition of the above-mentioned contents key etc. on said display device from the user terminal 50. In this case it carries out like the flow chart for contents key acquisition mentioned above and a contents key etc. come to hand. Thus when a contents key etc. newly come to hand as mentioned above in step ST104 the contents key which are enciphered is decrypted. <BR>[0142] Next the controller 16 checks whether there is any enough balance of the point information stored in the

point information storing memory 28 based on the service condition decrypted [ above-mentioned ] as shown in step ST105. <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>when the balance of the above-mentioned point information stored in the above-mentioned point information storing memory 28 is insufficientThe information on the purport that the balance of the point information concerned is insufficient is sent from the controller 16 to the user terminal 50andtherebythe user terminal 50 displays the message which stimulates acquisition of the above-mentioned point information on said display device. In this caseit carries out like a flow chart for point access to information which was mentioned aboveand point information comes to hand.<BR>[0143]when actually appreciating digital contentshere the controller 16According to the digital contents concerned to appreciatea point information number is reduced from the above-mentioned point information storing memory 28 like step ST106Furthermorethe new point usage information according to the condition of use of the point information concerned is stored in the point usage information storing memory 29 (point usage information is updated). Thusas point usage information newly stored to the point usage information storing memory 29they are the right holder information corresponding to the digital contents which appreciated [ above-mentioned ]including owner of a copyright etc.informationother information on the reduced point information numberetc.<BR>[0144]Then the controller 16 will read digital contents from a memory mediumif it checks that the processing for fee collection of the cut of these point informationnew storing of point usage informationetc. has been completed like step ST107.<BR>[0145]since the digital contents read from this memory medium are encipheredthe controller 16 transmits the digital contents enciphered [ above-mentioned ] to the common code decoder circuit 24 like step ST109.<BR>[0146]In this common code decoder circuit 24the digital contents enciphered [ above-mentioned ] are decrypted like step ST110 using the contents key which decrypts previously and is kept by the common key storage memory 22 based on the directions from the controller 16.<BR>[0147]Since predetermined compression processing is made as mentioned abovethese digital contents the controller 16The digital contents by which the above-mentioned code was decrypted and by which compression processing is carried out [ above-mentioned ] are made to transmit to the expansion circuit 26 from the above-mentioned common code decoder circuit 24 like step ST111and the elongation processing corresponding to the above-mentioned predetermined compression processing is made to perform here.<BR>[0148]Then the elongated digital contents concernedLike step ST112it is changed into an analog signal in the D/A conversion circuit 27and is outputted outside (for exampleuser terminal 50 grade) like step ST113 via the terminal 13 of the integrated circuit 10and the analog output terminal 2 of the player 1 concerned.<BR>[0149]By the abovethe flow of the processing in the player 1 at the time of contents appreciation is completedand the appreciation of digital contents of a user is attained.<BR><DP N=0016><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>[0150]Nextthe point usage information newly stored in the point usage information storing media 29 of said player 1 with appreciation of digital contents which were mentioned aboveIt explains flowing into the processing in the player 1 at the time of returning to the control center 21the user terminal 50and the pipe center 310 using <A HREF="JP-A-H10-269289.files/000026.gif">drawing 24 </A>from <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21</A>referring to <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A>and <A HREF="JP-A-H10-269289.files/000005.gif">drawing 3</A>.<BR>[0151]The flow of the processing in the player 1 at the time of point usage information return is shown in <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21</A>.<BR>[0152]In this <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21</A>it waits for the controller 16 until starting of the software for point usage information return beforehand installed in the user terminal 50 is performedas shown in step ST121.<BR>[0153]If the software for the above-mentioned point usage information return of the above-mentioned user terminal 50 risesthe information inputted into the user terminal 50 according to the software concerned will be received like step ST122 via said interface terminal 3 for PCand the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is a password etc. which are entered by the user.<BR>[0154]The controller 16 which received this contents designation information from the above-mentioned user terminal 50The password supplied from the user terminal 50 concerned in step ST123 is compared with the password stored in the password storing memory 14and the



password concerned carries out the right check of how.<BR>[0155]when it is checked that it is a right password in the check of the above-mentioned passwordthe controller 16The balance of the point information stored in the point information storing memory 28 and the point usage information stored in the point usage information storing memory 29 are read like step ST124respectivelyand these information is enciphered.<BR>[0156]After the balance of the above-mentioned point information and encryption of point usage information are completedthe controller 16 is attached to the data which read user ID from the user ID storing memory 23and enciphered [ above-mentioned ] like step ST125.<BR>[0157]The data in which this user ID was attached is transmitted to the user terminal 50 via the terminal 12 and the interface terminal 3 for PC like step ST126 from the controller 16. This data is transmitted to the control center 211 after that.<BR>[0158]As mentioned above also in the encryption at this timethe common key encryption system is adopted. That isin advance of transmission of the data concernedgeneration of a common key is performed like the above-mentionedit is enciphered with said public-key crypto system (encryption using the public key of the control center 211)and this generated common key is sent to the control center 211 with user ID.<BR>[0159]<TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>After transmitting data to the user terminal 50 as mentioned abovethe controller 16 waits to transmit the data later mentioned from the above-mentioned control center 211 via the user terminal 50.<BR>[0160]when the data from the above-mentioned control center 211 is received like step ST127here in the player 1. The received data enciphered using the common key encryption system are decrypted like step ST127 using a common key like the above-mentionedand the justification of the data is checked. That isthe controller 16 evaluates the justification by checking security ID of the data decrypted [ above-mentioned ] by comparison with security ID from the above-mentioned security ID generating circuit 19.<BR>[0161]The message of the processing completion enciphered using the above-mentioned common key is also contained in the data transmitted from the above-mentioned control center 211. Thereforethe controller 16 after the check of above-mentioned security ID is completedSend the processing completion message enciphered [ above-mentioned ] to the common code decoder circuit 24the decryption using a common key is made to perform hereand it is checked that processing in the above-mentioned control center 211 has been completed by receiving this decrypted processing completion message.<BR>[0162]By the abovethe flow of the processing in the player 1 at the time of point usage information return is completed.<BR>[0163]Nextthe flow of the processing in the user terminal 50 at the time of point usage information return is explained using <A HREF="JP-A-H10-269289.files/000024.gif">drawing 22</A>.<BR>[0164]In this <A HREF="JP-A-H10-269289.files/000024.gif">drawing 22</A>the user terminal 50 starts the software for point usage information return in step ST131. when the software concerned risesin this user terminal 50. If input requestssuch as a passwordare performed and the input of a password is made from a user to the user who operates the user terminal 50 concerned in step ST132 according to the above-mentioned softwarethe password will be transmitted to the player 1.<BR>[0165]Nextif the data created and transmitted by the above-mentioned player 1 like step ST126 of said <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21 </A>in step ST133 is receivedthe user terminal 50The data transmitted from the player 1 concerned in step ST134 is transmitted to the control center 211 where the address is registered beforehand.<BR>[0166]The user terminal 50 after performing a data transfer to the above-mentioned control center 211 will transmit the data concerned to the player 1 as it isif the data in which the return from the control center 211 is sent from the control center 211 to the player 1 in waiting and step ST135 is received.<BR>[0167]The user terminal 50 after performing a data transfer to the above-mentioned player 1 performs the display for making a user know that processing was completed to a display deviceand receives the check from a user.<BR>[0168]By the abovethe <DP N=0017><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>flow of the processing in the user terminal 50 at the time of point usage information return is completed.<BR>[0169]Nextthe flow of the processing in the control center 211 at the time of point usage information return is explained using <A HREF="JP-A-H10-269289.files/000025.gif">drawing 23</A>.<BR>[0170]In the communication function section 133 with the user terminal of the control center 211the data of the point usage information etc. which have been transmitted by step ST126 of said <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21 </A>and step

ST134 of <A HREF="JP-A-H10-269289.files/000024.gif">drawing 22 </A>from the player 1 via said user terminal 50 is received like step ST141.<BR>[0171]when this data is receivedthe user management functional block 110 of the control center 211The common key which is beforehand received from the database section 112 like the above-mentionedand is stored under control of the control function part 111 like step ST142 based on the user ID attached to the received data concerned comes to handand security ID comes to hand.<BR>[0172]If the common key and security ID corresponding to the above-mentioned user ID come to hand from the above-mentioned database section 112as shown in step ST143In the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211Further in [ decrypt the data of the point usage information etc. which were enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common keyand ] the control function part 111Comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned database section 112 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed.<BR>[0173]The data after the check of the above-mentioned justification and the contents is transmitted to the usage information controlling-function block 120. The control function part 121 of this usage information controlling-function block 120As shown in step ST144it is checked whether there is any injustice in use of above-mentioned user side 200 using the information stored in the database section 122 using the balance and point usage information of point information which have been sent from the above-mentioned player 1. Simultaneouslywhen [ concerned / unjust ] it comes and things are checkedthe operation which summarizes the balance and point usage information of point information in the usage information calculation function part 123 is performed.<BR>[0174]Then the control function part 111 of the user management functional block 110 controls the security ID generating function part 116makes security ID computecontrols the confirmation message generating function part 115 furtherand makes the message of processing completion generateas shown in step ST145. These security ID and a processing completion message are enciphered using said common key in the correspondence code / function decoding part 114 of the user management functional block 110.<BR>[0175]The data which was enciphered [ above-mentioned ] and generated will be <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>sent to the user terminal 50 from the communication function section 133 with a user terminalas shown in step ST146and it will be transmitted to the player 1 from the user terminal 50 concerned like step ST135 of said <A HREF="JP-A-H10-269289.files/000024.gif">drawing 22</A>and step ST127 of <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21</A>.<BR>[0176]By the above the flow of the processing in the control center 211 at the time of point usage information return is completed.<BR>[0177]From <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21 </A>mentioned above the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of <A HREF="JP-A-H10-269289.files/000025.gif">drawing 23</A>and the control center 211 can be expressedas shown in <A HREF="JP-A-H10-269289.files/000026.gif">drawing 24</A>.<BR>[0178]That is in this <A HREF="JP-A-H10-269289.files/000026.gif">drawing 24</A>the input of said password is transmitted from the user terminal 50 to the player 1 like step ST132 of said <A HREF="JP-A-H10-269289.files/000024.gif">drawing 22 </A>by the input transmission T31. In the prepared data transmission T32the data which the player 1 created is transmitted to the user terminal 50 like step ST126 of said <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21</A>. In the prepared data transmission T33the data created by the above-mentioned player 1 is transmitted to the control center 211 from the above-mentioned user terminal 50 like step ST134 of said <A HREF="JP-A-H10-269289.files/000024.gif">drawing 22</A>. In the data transfer T34the data created in the control center 211 is transmitted to the user terminal 50 like step ST146 of said <A HREF="JP-A-H10-269289.files/000025.gif">drawing 23</A>. In the data transfer T35the data created in the control center 211 is transmitted to the player 1 via the user terminal 50 like step ST127 of said <A HREF="JP-A-H10-269289.files/000023.gif">drawing 21</A>.<BR>[0179]Actual operation of the player 1 of the system of this embodimentthe user terminal 50and the control center 211 serves as a flow which was mentioned above.<BR>[0180]so far although the flow of processing of the whole in the system of this embodiment has been explainedoperation of each of the principal part of the system of this embodiment is

explained in detail after this.<BR>[0181]First explanation about operation of the encryption and compression in this invention embodiment and extension and decryption is given.<BR>[0182]Like the system of an embodiment mentioned above when distributing digital contents using a network in order to stop the data volume compression/extension art is used and encryption/compression technology is used for anti-copying or fee collection. That is compressing digital contents and carrying out encryption processing further by the distribution side (an above-mentioned example the control center 211 side) is performed. When distributing the digital contents (encryption/compressed data) generated at the transmitting side (control center 211 side) like an above-mentioned example using a network in a receiver (an above-mentioned example player 1) decrypting after receiving the digital contents which were above-enciphered and were compressed elongating further and restoring digital contents is performed. The turn of processing of the above-mentioned encryption/compression and decryption and extension may interchange.<TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300><DP N=0018><BR>[0183]When copyright etc. exist in the above-mentioned digital contents when the above-mentioned receiver elongates the above-mentioned digital contents with the above-mentioned decryption it will be charged according to intention of the above-mentioned owner of a copyright etc. Although this fee collection is performed by mainly purchasing the key i.e. the contents key of decryption it is in the method of purchasing this contents key variously.<BR>[0184]Hereas mentioned above when procedure which compresses digital contents is enciphered is decrypted and is elongated is followed the user who had bad faith for example can obtain comparatively easily the compressed data decrypted [ above-mentioned ]. Namely the compressed data of digital contents generally capacity is large therefore for example since not an internal memory but the \*\* value of a common contents playback device of a receiver are accumulated in external memory in many cases it is because it is easy to take out unjustly the digital contents compressed [ above-mentioned ] by the connection section with direct or external memory from this external memory.<BR>[0185]What cannot be processed if the algorithm of the expansion system to compression is hidden like the key of a code general to the algorithm of an expansion system respectively being opened to the public in many cases does not exist. And as compared with the digital contents by which the encryption distributed from the above-mentioned transmitting side and compression were made\*\*\*\* which distributes the compression digital contents which did not change in data volume therefore were decrypted [ above-mentioned ] with bad faith is also easy for the compression digital contents decrypted [ above-mentioned ]. Namely according to the method which is enciphered and distributes digital contents after compressing [ above-mentioned ]. The danger that the compression digital contents which can elongate anyone easily will be distributed further in the place which a theft is easily carried out to a user with bad faith and intention of an owner of a copyright etc. does not reach for this reason or will be elongated is large.<BR>[0186]So in the embodiment of the invention in order to make it possible to raise the safety of the digital contents distributed using a network in view of such a situation in the player 1 of above-mentioned <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2</A> processing as shown in the flow chart of the following <A HREF="JP-A-H10-269289.files/000027.gif">drawing 25 </A> is performed.<BR>[0187]Namely in the decoding processing in the common code decoder circuit 24 of the player 1 of <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2</A> and the elongation processing in the above-mentioned expansion circuit 26. The data of the digital contents by which compression processing was carried out with the encryption read from said memory medium like step ST151 first it divides into the unit of the least common multiple lcm (XY) of the batch X bit of the algorithm of decoding processing and the algorithm batch Y bit of elongation processing.<BR>[0188]Next<TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> as the data of digital contents in which the above-mentioned encryption divided into the unit of the above-mentioned least common multiple lcm (XY) and compression processing are made is shown in step ST152 decoding processing is performed by the above-mentioned common code decoder circuit 24 for every unit of the least common multiple lcm (XY) concerned.<BR>[0189]As the data of digital contents in which the unit of the least common multiple lcm (XY) obtained by the decoding processing concerned is compressed is shown in step ST154 elongation processing is performed to all the compressed data for the unit concerned in the above-mentioned expansion circuit 26.<BR>[0190]Then the decryption and elongation processing for every unit of this least common multiple

lcm (XY) are continued until the processing about all the data of digital contents by which compression processing was carried out with the above-mentioned encryption is completed. . Namely judgment whether the decryption and elongation processing for every unit of the least common multiple lcm (XY) were completed to all the data of digital contents should do to be shown in step ST155. When not having completed and it returned and completes to step ST152 the flow chart of the processing concerned is completed. <BR>[0191]The digital contents by which all the data was decrypted and elongated by this will be obtained. <BR>[0192]Although the decoding data of the above-mentioned least-common-multiple lcm (XY) unit will exist the data volume of the decoding data concerned also has little processing of the flow chart of <A HREF="JP-A-H10-269289.files/000027.gif">drawing 25 </A> in the player 1 concerned. For this reason a possibility of being stolen like [ in the case of saving at external memory which can be saved at an internal memory with high safety even if comparatively expensive therefore was mentioned above ] will become very low. <BR>[0193]In the above-mentioned player 1 in this embodiment the buffer memory 25 of <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A> is formed as an internal memory for securing the above-mentioned safety between the above-mentioned common code decoder circuit 24 and the expansion circuit 26. That is this buffer memory 25 is formed in the integrated circuit 10 of one chip and it is hard to be accessed from the outside therefore data is not taken out outside. <BR>[0194]In an above-mentioned flow chart are made to perform decryption and elongation processing to all the data for the unit of the least common multiple lcm (XY) and as concrete composition for it for example the data of digital contents is first divided into the batch X bit of the algorithm of decoding processing like composition of being shown in <A HREF="JP-A-H10-269289.files/000028.gif">drawing 26 </A> By performing decoding processing to the data of this X bit gathering the data in which the X bit concerned by which decoding processing was carried out is compressed after that by the algorithm batch Y bit of elongation processing and elongating the compressed data of the Y bit concerned. It is made to realize the decryption and elongation processing in the unit of the least common multiple lcm (XY) as mentioned above. <BR>[0195]The common code decoder circuit 24 of the player 1 which realizes this consists of the input part 30 and the code decoding part 31 and the above-mentioned expansion circuit 26 consists of the expanding part 32 and the outputting part 33. <DP N=0019><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> Said buffer memory 25 is formed between these common code decoder circuit 24 and the expansion circuit 26. <BR>[0196]If encryption processing to the above-mentioned digital contents is performed as a more concrete example here for example using the DES (Data Encryption Standard) code the encryption processing concerned and decoding processing corresponding to it will be performed by 64 bit wise. <BR>[0197]In the case of the elongation processing to the compressed digital contents it changes also with the compression ratios and sampling frequencies but under the present circumstances it is processed per 1K - 2 K bits/channel in many cases. Here it is assumed that it is processed for every 1.28K bit for convenience. <BR>[0198]Therefore in the case of the system using the above-mentioned DES cipher system and the compression expansion system for every above-mentioned 1.28K bit the above-mentioned least common multiple lcm is set to 1.28K. <BR>[0199]Said digital contents enciphered and compressed are inputted into the input part 30 of the basis of such conditions and the common code decoder circuit 24 of <A HREF="JP-A-H10-269289.files/000028.gif">drawing 26 </A>. In the input part 31 concerned the digital contents which were enciphered [ above-mentioned ] and compressed are divided into [ every batch X bit of the algorithm of the above-mentioned decoding processing ] i.e. 64 bits data and are outputted to the code decoding part 31. <BR>[0200]In this code decoding part 32 decoding processing of the above-mentioned X bit i.e. 64 bits data is carried out concerned every 64 bits. The 64 bits [ which was obtained by the decryption in this every 64 bits ] data compressed is sent to the buffer memory 25. <BR>[0201]When the compressed data for the algorithm batch Y bit of elongation processing i.e. a 1.28K bit accumulates according to the directions from said controller 16 the buffer memory 25 concerned The compressed data for the 1.28K bit concerned is outputted collectively and this compressed data is sent to the expanding part 32 of the above-mentioned expansion circuit 26. <BR>[0202]The above-mentioned expanding part 26 elongates the compressed data for the 1.28K bit inputted [ above-mentioned ] and outputs it to the outputting part 33. <BR>[0203]The controller 16 controls processing of the decoding section 31 and processing of the expanding part 32 monitoring the data volume which accumulated in

the buffer memory 25.<BR>[0204]If 20 pieces (= 1280/64) are parallel in decoding processing if it is this case and it processes it will become a more nearly high-speed processing system.<BR>[0205]In addition when performing not hardware constitutions like said <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2 </A> or <A HREF="JP-A-H10-269289.files/000028.gif">drawing 26 </A> but processing mentioned above with the programmable device the controller 16 will process based on a decoded program or an extension program corresponding to the situation of the buffer memory 25.<BR>[0206]Although the digital contents enciphered after compressing were supplied to the player 1 and the example elongated after decrypting these digital contents compressed and enciphered was given by the player 1 by above-mentioned explanation<TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>Even if it is a case where the compressed digital contents are elongated and decrypted after enciphering the same effect as \*\*\*\* can be acquired.<BR>[0207]The algorithm of compression / extension and encryption/decryption is not limited and this invention is effective to any methods.<BR>[0208]Thus according to this invention the safety of the digital contents distributed using a network improves.<BR>[0209]Next explanation about generating operation of said security ID is given.<BR>[0210]As point information comes to hand beforehand and being mentioned above like this embodiment in the case of a method which reduces the point information concerned according to appreciation of digital contents After the control center 211 on a network performs checks as arbitrary after receiving communication of a purchase request of the point information from the user terminal 50 of user side 200 as financial institution 220 and others it enciphers the point information and sends it to the player 1 of user side 200 via a network.<BR>[0211]In the case of a method which obtains point information beforehand and reduces the point information concerned like this embodiment according to appreciation of digital contents between the control center 211 and the player 1 (user terminal 50) an exchange of the data same each time as the degree of the purchase of point information -- carrying out (for example the information of "the point information on 3000 cyclotomies" corresponding to "3000 supplement demand of the point information on a cyclotomy" and it which were enciphered is exchanged) -- it is based on those who have bad faith for example. The amount-of-money supplement depended for what is called "impersonating" to the financial institution 220 serves as a problem. "Impersonating" to the financial institution which says here means what a person with the above-mentioned bad faith impersonates an original user (this embodiment user side 200) and obtains point information unjustly.<BR>[0212]Namely if the data same each time as the degree of the purchase of point information is exchanged For example a person with bad faith robs a communication line of the data concerned and the same data is generated In the case as the destination is made into itself (person with bad faith) to the control center 211 and acquisition of point information was requested. A person with the bad faith concerned can obtain point information and the claim of the purchase price of this point information has further a possibility that the problem that it will be made by original user side 200 may occur.<BR>[0213]Then in order to prevent such injustice in the system of this invention embodiment the random number generated by the random number generation function which has interlocked beforehand by both a receiver (player 1 side) and the distribution side (control center 211 side) is used for the improvement in safety. According to this embodiment said security ID is generated as the above-mentioned random number. what is necessary <DP N=0020><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> is to initialize the timer 18 for example and just to synchronize operation between both for example in the case such as a user's registration procedure in order to interlock a random number generation among both.<BR>[0214]That is the operation at the time of the player 1 for example point access to information from the control center 211 at the time of using this random number (security ID) serves as the following flows.<BR>[0215]The data sent from the control center 211 to the player 1 is made with the data which consists of security ID generated [above-mentioned] with the point information enciphered using the common key (session key) which came to hand beforehand from the player 1 as mentioned above at the time of the purchase of point information.<BR>[0216]The controller 16 of the player 1 is sent to the common code decoder circuit 24 as the data received from the control center 211 concerned was mentioned above and it performs decoding processing here using said common key. By this the point information and security ID which have been sent from the control center 211 will be obtained.<BR>[0217]Then the controller 16 of the player 1 compares security ID sent from the above-mentioned control center 211 with

security ID generated in the own security ID generating circuit 19. In this comparison the controller 16 stores in said point information storing memory 28 the point information sent from the above-mentioned control center 21 only when security ID from the control center 21 and security ID which the above itself generated are in agreement. [0218] By this only the player 1 of valid-user side 200 can obtain point information. the malicious person who in other words has the player 1 of valid-user side 200 and the same player -- said -- impersonating even if it is going to obtain point information unjustly since security ID of the player which the person of the bad faith concerned has and security ID sent from the above-mentioned control center 21 are not in agreement the person with this bad faith will not get said inaccurate point access to information depended for impersonating. [0219] Of course security ID generated in the player 1 of user side 200 The security ID generating circuit 19 provided in the integrated circuit 10 of the player 1 concerned occurs and since it is what cannot be taken out outside a person with bad faith cannot steal the security ID concerned. [0220] Although some are various in the composition which generates the random number as above-mentioned security ID the example is shown in [drawing 27](JP-A-H10-269289.files/000029.gif). The composition of this [drawing 27](JP-A-H10-269289.files/000029.gif) is one example of the security ID generating circuit 19 of said [drawing 2](JP-A-H10-269289.files/000004.gif). [0221] In this [drawing 27](JP-A-H10-269289.files/000029.gif) the one-way function generating part 40 generates what is called a one-way nature function. The inverse function is far difficult for calculation with a function with the above-mentioned one-way nature function comparatively easy to calculate. It receives by secret communication etc. beforehand and this one-way function can also be [drawing 2](JP-A-H10-269289.files/000004.gif) saved at the one-way function generating part 40 concerned. The one-way function generating part 40 can also be made to generate the above-mentioned one-way function by making into an input function the hour entry from the timer 18 established in the integrated circuit 10 of said [drawing 2](JP-A-H10-269289.files/000004.gif). The above-mentioned one-way function is sent to the random number deciding part 43. [0222] The number generating part 41 of users generates the predetermined number of users defined for every user. This number of users is beforehand sent by secret communication etc. and is saved at the number generating part 41 of users concerned. The user ID which said user ID storing memory 23 stores for example can also be used for this number of users. [0223] The random number database 42 stores a random number and stores 99 random numbers. [0224] The time communication storage parts store 44 memorizes the time communication information sent for example from the controller 16. This time communication information is information which shows the time communication between the player 1 and the control center 21. [0225] These one-way functions the number of users and time communication information are sent to the random number deciding part 43. The random number deciding part 43 concerned generates the random number of the range beforehand memorized by the random number database section 42 from the above-mentioned one-way function and the number of users for example based on the hour entry from said timer 18 (for example 99 pieces). [0226] Namely if the above-mentioned time communication information is the communication which is the 1st time in this random number deciding part 43 the 99th random number is taken out from the above-mentioned random number database section 42 and if for example time communication information is the communication which is the n-th time the 100-n-th random numbers will be picked out from the above-mentioned random number database 42 and this taken-out random number is outputted as said security ID. [0227] The composition of this security ID generating has the same thing in the player 1 and the control center 21. [0228] When finishing using all the random numbers stored in the random number database section 42 in the above-mentioned random number deciding part 42 100 pieces - the 199th random number are calculated or secret communication of a new random number and unidirectional function is carried out and it re-stores in the random number database section 42 or on the other hand reconstructs to the tropism function generation part 40. [0229] Although a random number (security ID) is generated and he is trying to improve the safety for every communication in the explanation mentioned above according to this embodiment since he is also trying to generate programmably a common key (session key) different each time whenever it communicates between user side 200 and the control center 21 side as mentioned above safety is improved further. [0230] Here the above-mentioned

JPA\_1998-269289\_translation

random number is inserted about the transmission sentences (for example message etc.) actually transmitted and signs that encryption by a session key is made and signs that a random number is taken out from a receiving sentence and the check of justification is made are explained using <A HREF="JP-A-H10-269289.files/000030.gif">drawing 28 </A> and <A HREF="JP-A-H10-269289.files/000031.gif">drawing 29</A>. He is also <DP N=0021><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> trying to add a signature (digital signature) to a transmission sentence in the example of these <A HREF="JP-A-H10-269289.files/000030.gif">drawing 28 </A> and <A HREF="JP-A-H10-269289.files/000031.gif">drawing 29</A>. <BR>[0231] In this <A HREF="JP-A-H10-269289.files/000030.gif">drawing 28</A> first as a flow which enciphers said common key with a public-key crypto system and transmits it generates as a common key which uses said session key for communication and this common key is enciphered by the public key of a receiver to the public-key-encryption chemically-modified degree P8 by the common key generating process P7 for communication. This enciphered common key is sent to a receiver. <BR>[0232] On the other hand as a flow in the case of enciphering the message as a transmission sentence with a common key encryption system and transmitting in the message generation distance P1 the message M is generated and a random number (said security ID) is generated at the random number generation process P5 for example. These messages M and a random number are sent to the common key encryption system chemically-modified degree P6. In the common key encryption system chemically-modified [ this ] degree P6 the above-mentioned message M and a random number are enciphered using the common key by which it was generated at the above-mentioned common key generating process P7 for communication. <BR>[0233] When adding the above-mentioned digital signature the above-mentioned message M is sent to the hash value calculation process P2. In the hash value calculation process P2 concerned what is called a hash value is calculated from the above-mentioned message M. A hash value is address information called for by a hash method and a hash method performs a predetermined operation to some contents (keyword) of data (in this case the message M) and uses that result for it as an address. The hash value (M) generated from this message is sent to the secret key cryptosystem chemically-modified degree P4 as a digital signature. In the secret key cryptosystem chemically-modified [ this ] degree P4 the above-mentioned digital signature is enciphered with the secret key of the transmitting side. This enciphered digital signature is sent to the common key encryption system chemically-modified degree P6. This enciphers the above-mentioned digital signature in the common key encryption system chemically-modified degree P6 using the common key by which it was generated at the above-mentioned common key generating process P7 for communication. <BR>[0234] These messages M a digital signature and a random number are transmitted to a receiver. <BR>[0235] Next the flow of processing by the receiver corresponding to <A HREF="JP-A-H10-269289.files/000030.gif">drawing 28 </A> is explained using <A HREF="JP-A-H10-269289.files/000031.gif">drawing 29</A>. <BR>[0236] In this <A HREF="JP-A-H10-269289.files/000031.gif">drawing 29</A> the common key transmitted from the above-mentioned transmitting side is first decrypted with the secret key of the receiver concerned at the secret key decryption process P11 as a flow which decrypts said common key with a public-key crypto system. <BR>[0237] At the common key decoding process 13 the message M transmitted [ above-mentioned ] is decrypted using the common key decrypted at the above-mentioned secret key decryption process P11 as a flow which on the other hand decrypts the message M enciphered with said common key encryption system. This decrypted message M will be sent to other processes by the other functional transmission processes P20. <BR>[0238] The hash value which decodes a digital signature and which flowed and was decrypted at the above-mentioned common key decryption process P13 is <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> decrypted using the public key of the transmitting side at the public key decryption process P14. Simultaneously in the hash value calculation process P17 a hash value is calculated from the above-mentioned message M. The check of the hash value decrypted by these public key decryption process P14 and the hash value calculated by the above-mentioned hash value calculation process P17 being compared and not being altered by the comparison process P19 is performed. <BR>[0239] About the transmitted random number the random number decrypted at the above-mentioned common key decryption process P13 and the random number generated at the random number generation process P21 of the receiver concerned are compared by the just exact private seal process P22 and the check of

justification is performed. [0240] By the way in the system of this embodiment shown in [drawing 1](JP-A-H10-269289.files/000003.gif) mentioned above the system management company 210, the virtual online shop 230 and the content provider 240 are formed as a system side to user side 200. The financial institution 220 of [drawing 1](JP-A-H10-269289.files/000003.gif) is an external bank etc. for example. [0241] The control center 210 of the above-mentioned system management company 210, exhibition of digital contents and management of distribution in the virtual online shop 230 between the financial institutions 220 -- the main work by the side of systems such as collection of the accounting information of user side 200 or a variety of information distribution and those management, encryption of the digital contents from the content provider 240 and a security management of the information to treat -- all are performed mostly. [0242] However in the system which distributes digital contents using a network which was mentioned above in the time of the user side obtaining digital contents from the system side and the case of the fee collection accompanying use of digital contents, communication will concentrate on the system side and there is a possibility that a satisfying response may no longer be obtained to the user side. [0243] So in other embodiments of this invention it makes it possible to prevent concentration of communication which was mentioned above and to raise a communicative response by the function of the system management company 210 and more specifically dividing the function of the control center 211 as follows. [0244] Namely the content exhibiting distributing institution 310 which has a function which exhibits digital contents and distributes the composition by the side of the system to user side 200 in other embodiments of this invention as shown in [drawing 30](JP-A-H10-269289.files/000032.gif). Accounting information control machine Seki 320 which has the function to manage the accounting information of the user of a fixed area, it divides into the data generation of enciphering digital contents, distribution of generated data to the above-mentioned content exhibiting distributing institution 310, the information gathering from above-mentioned accounting information control machine Seki 320, division of earnings and the system management organization 330 that has the function to perform the security management and others of the whole system, user side 200 and communication are independently attained for each organization 310, 320, 330 respectively. [0245] In composition like this [drawing 30](JP-A-H10-269289.files/000032.gif) the content exhibiting distributing institution 310 is scattered on the network in the world, two or more arrangement is possible for it and if even communication charges are paid it can access user side 200 to the content exhibiting distributing institution 310 of every area. For example when user side 200 wants for digital contents to come to hand, the above-mentioned content exhibiting distributing institution 310 is accessed from user side 200 and digital contents come to hand. Digital contents [which were enciphered by the system management organization 330] i.e. user side 200 will be the digital contents at this time in the state which can be transmitted directly using a network. [0246] Holding not much many users installs accounting information control machine Seki 320 for a moderate number of every users undesirably therefore on safety management in order to treat accounting information. However since the attack point (accounting information control machine Seki 320) from the 3rd person with bad faith will be increased and it will be traded off if it installs not much mostly optimizing is desirable. For example when user side 200 performs communication about fee collection it accesses from user side 200 to above-mentioned accounting information control machine Seki 320. [0247] The above-mentioned system management organization 330, subscription to a user's system and registration of means of settlement, profits distribution to the profits beneficiary of the collection of money from a user said right holder, the content exhibiting distributing institution 310 and accounting information control machine Seki 320 grade etc. raise security by carrying out by summarizing management of important information on security. However as for the system management organization 330 concerned it is desirable not to necessarily establish one place in the world and to install in a certain settled unit for example the unit of a country etc. For example when user side 200 performs important communication on [such as subscription to this system and registration of means of settlement] security it carries out by accessing from user side 200 to the above-mentioned system management organization 330. The system management organization 330 concerned which obtained information performs profits distribution



to the collection of money and the profits beneficiary from the user concerned collectively from above-mentioned accounting information control machine Seki 320. It is supplied to the system management organization 330 concerned the source data i.e. the contents which an owner of a copyright etc. have they are changed into the digital contents by which encryption etc. were made here and are distributed to the above-mentioned content exhibiting distributing institution 310. <BR>[0248] As mentioned above by distributing the function by the side of a system to the three organizations 310 320 330 and making direct access of it possible between user side 200 and each organization 310 320 330 communicative concentration is prevented and it becomes possible to raise a communicative response. According to the content exhibiting distributing institution 310 it can respond also to a thing like what is called an existing virtual Mall and it is effective also in sales promotion and attractive for a user. By dividing accounting information control machine Seki 320 independently it is useful for the dishonesty prevention which conspired with exhibition and the selling function of contents. In order that a fixed number may obstruct the user who manages the controlling function who receives unjustly is also more effective. <BR><TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>[0249] In the system of other embodiments of this invention shown in <A HREF="JP-A-H10-269289.files/000032.gif">drawing 30 </A> mentioned above below it explains that the accounting information accompanying the information flow at the time of acquisition of the contents key subscription to a user's system the purchase of point information and for decoding of the enciphered digital contents etc. the flow in the case of circulation of the information for contents and contents appreciation and use of contents flows. <BR>[0250] First the principal part of the flow of the time of subscription to a user's system is explained using <A HREF="JP-A-H10-269289.files/000033.gif">drawing 31 </A>. <BR>[0251] In the case of the subscription registration to a user's system the following procedures depended on the user subscription support functional block 402 of the system management organization 330 followed and registering operation is performed at it. <BR>[0252] From user side 200 [1] i.e. said player and the user terminal 50 the information which shows the intention of subscription to a system is first sent via a network like the subscription intention sending T41 to the system management organization 330. The information on the above-mentioned subscription intention of having been inputted into the communication function block 401 of the system management organization 330 is sent to the user subscription support functional block 402. <BR>[0253] Reception of the above-mentioned subscription intention information of the user subscription support functional block 402 concerned will send the information on a file required for subscription to user side 200 via the communication function block 401 like the subscription required file sending T42. <BR>[0254] In user side 200 creation of the subscription request according to a predetermined format is performed based on the subscription required file sent from the above-mentioned system management organization 330. The drawn-up subscription request concerned is sent to the system management organization 330 like the subscription request sending T43. <BR>[0255] The user subscription support functional block 402 which received the above-mentioned subscription request sends the information which explains the function of a client to user side 200 like the client function sending T44. <BR>[0256] From user side who received information on client function concerned 200 User Information such as users' information for example an account number and a credit number which were mentioned above a name and a contact is sent to the system management organization 330 like the User Information sending T45. <BR>[0257] The user subscription support functional block 402 which received sending of the User Information concerned notifies the information on the purport that the registration procedure of subscription was completed to user side 200 like the registration procedure completion notification T46. <BR>[0258] The user subscription support functional block 402 of the system management organization 330 transmits User Information to accounting information control machine Seki 320 via the communication function block 401 like the User Information sending T47 after the completion of procedure of this user subscription registration. Accounting information control machine Seki 320 which received this User Information <DP N=0023><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> saves the User Information concerned at the database function block 367. <BR>[0259] By the above the main flows of the time of subscription to a user's system are completed. The explanation about other composition currently mentioned to this <A HREF="JP-A-H10-269289.files/000033.gif">drawing 31 </A> is mentioned

later.<BR>[0260]Nextthe principal part of the flow of the information at the time of acquisition of the key the purchase of point information and for decoding of the enciphered digital contentsetc. is explained using <A HREF="JP-A-H10-269289.files/000034.gif">drawing 32</A>. Since the information on the contents key the purchase of the above-mentioned point information and for decoding of the enciphered digital contents is information for using contentsit is made to simplify these and to call it royalty information by the following explanation.<BR>[0261]When a user obtains the important information (here royalty of contents) used by a systemaccess is made from user side 200 to accounting information control machine Seki 320 where the assignment in its duty is beforehand made for every user side 200. To access of an acquisition demand of the contents royalty information sent from above-mentioned user side 200the royalty issuing function block 362 of accounting information control machine Seki 320 correspondsand issue of a royalty is performed according to the following procedures.<BR>[0262]Firstfrom user side 200the information on the purport that he would like to purchase a royalty is sent to accounting information control machine Seki 320 like the purchase written request sending T51. The information on the purport that he would like to purchase a royalty is information on the purchase written request which followed the predetermined format by user side 200. Thus the information on the above-mentioned purchase written request inputted into the communication function block 361 of this accounting information control machine Seki 320 is sent to the royalty issuing function block 362 via a network.<BR>[0263]In the royalty issuing function block 362 concernedif the information on the above-mentioned purchase written request is receivedit will carry out based on User Information saved at the database function block 367the information on a new royalty will be generatedand the information on the royalty concerned will be sent to user side 200 like the new royalty sending T52.<BR>[0264]If the receipt of the information on the above-mentioned new royalty is checkeduser side 200 will draw up the receipt written confirmation according to a predetermined formatand will send it to the royalty issuing function block 362 of accounting information control machine Seki 320 like the receipt written confirmation sending T53.<BR>[0265]By the abovethe main flows of the time of the purchase of a royalty are completed. The explanation about other composition currently mentioned to this <A HREF="JP-A-H10-269289.files/000034.gif">drawing 32 </A>is mentioned later.<BR>[0266]Nextthe principal part of the flow in the case of circulation of the information for contents and contents appreciation (herethey are a service condition and a contents key) is explained using <A HREF="JP-A-H10-269289.files/000035.gif">drawing 33</A>.<BR>[0267]Firstthe contents acquisition functional block 342 of the content exhibiting distributing institution 310 charges digital contents to the system management organization 330 like the contents bill sending T62.<BR>[0268]<TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>In the contents distribution functional block 404the system management organization 330 which received the contents bill concerned is processed so that the demanded contents can be circulated. That isin this contents distribution functional block 404the digital contents (enciphered digital contents) of the state which can be sent to user side 200 are generated. These processed digital contents are sent to the content exhibiting distributing institution 310 like the contents sending 63.<BR>[0269]In the content exhibiting distributing institution 310 concernedthe digital contents processed [ above-mentioned ] are saved at the contents database functional block 345.<BR>[0270]In the contents distribution functional block 404 of the system management organization 330. The contents key for decoding the contents enciphered as content ID and a service condition as information for contents appreciation is sent to accounting information control machine Seki 320 like the information sending T64 for contents appreciation.<BR>[0271]In accounting information control machine Seki 320a contents key and the service-condition receipt functional block 363 receive the information for the above-mentioned contents appreciationand it is saved at the database function block 367.<BR>[0272]Nextlike the contents acquisition request T61user side 200 is accessed to the content exhibiting distributing institution 310and obtains contents. Namelythe content exhibiting distributing institution 310reading the enciphered digital contents which are saved at the contents database functional block 354if the demand of acquisition of contents is made from above-mentioned user side 200 via the communication function block 341 -- the read digital contents concerned -- user side 200 --

sending .<BR>[0273]Then user side 200 is accessed to accounting information control machine Seki 320 by the information claim T65 for contents appreciation and obtains the information for contents appreciation like the information sending T66 for contents appreciation. Namely via the communication function block 361 in accounting information control machine Seki 320. If the request for a service condition and a contents key is made as information for contents appreciation from above-mentioned user side 200, a contents key and a service condition will be published from a contents key and the service-condition issuing function block 364, and these will be sent to user side 200 via the communication function block 361.<BR>[0274]By the above flow in the case of circulation of the information for contents and contents appreciation is completed. The explanation about other composition currently mentioned to this <A HREF="JP-A-H10-269289.files/000035.gif">drawing 33 </A> is mentioned later.<BR>[0275]Next the principal part of the flow of balancing account, i.e. balancing account of a contents usage fee when contents are actually appreciated is explained using <A HREF="JP-A-H10-269289.files/000036.gif">drawing 34 </A>.<BR>[0276]First after appreciation of contents is performed in user side 200, from concerned user side 200, point usage information, i.e. use record of contents, is sent to accounting information control machine Seki 320 like the statement-of-accounts sending T71 as mentioned above. Thus if sending of the above-mentioned contents use record is received from above-mentioned user side 200 via the communication function block 361, the contents use record concerned will be received with the balancing account procedure reception functional block 365 of accounting information control machine Seki 320, and the balancing account written confirmation corresponding to this will be published. Similarly the balancing account written confirmation concerned is sent to user side 200 via the communication function block 361 like the balancing account written confirmation sending T73. Thereby user side 200 can know that balancing account was performed.<BR>[0277]Next the balancing account procedure reception functional block 365 of accounting information control machine Seki 320 makes royalty issuing information publish from the royalty issuing function block 362. This royalty issuing information is sent to the system management organization 330 via the communication function block 361 as user settlement of accounts and the contents use record sending T74 with the contents use record sent from above-mentioned user side 200.<BR>[0278]The system management organization 330 summarizes the information sent from accounting information control machine Seki 320 currently distributed in various places with collection of money and the distribution frame block 405, totals the amount of collection of money and a collection-of-money place, and the distribution destination of money and settles them through a actual financial institution.<BR>[0279]By the above flow of balancing account of a contents usage fee is completed. The explanation about other composition currently mentioned to this <A HREF="JP-A-H10-269289.files/000036.gif">drawing 34 </A> is mentioned later.<BR>[0280]In explanation to <A HREF="JP-A-H10-269289.files/000036.gif">drawing 34 </A> from above-mentioned <A HREF="JP-A-H10-269289.files/000032.gif">drawing 30 </A> the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, the system management organization 330, and user side 200. In the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, and the system management organization 330, it cannot be overemphasized that a data encryption and decryption are performed like the above-mentioned. Also in this encryption and decryption, any of a public-key crypto system and a common key encryption system may be used as mentioned above. A public-key crypto system can be used as a cipher system of a contents key or a common key, and a common key encryption system can be used as cipher systems such as a message and various kinds of documents. It is also possible to use the technique of the improvement in security using said random number, the encryption at the time of treating contents, and least-common-multiple-ization of a compressive batch with these encryption.<BR>[0281]Next the concrete composition of each organizations 310, 320, and 330 mentioned above is explained briefly.<BR>[0282]First the composition of the content exhibiting distributing institution 310 is explained using <A HREF="JP-A-H10-269289.files/000037.gif">drawing 35 </A>.<BR>[0283]In this <A HREF="JP-A-H10-269289.files/000037.gif">drawing 35 </A> the content exhibiting distributing institution 310 concerned, the communication function block 341 which divides roughly and takes charge of the communication function between user side 200

JPA\_1998-269289\_translation

and the system management organization 330It <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>consists of the contents acquisition functional block 342 which takes charge of the acquisition function of contents,the content display functional block 343 which takes charge of the exhibition function of contents,the balancing account functional block 344 which takes charge of balancing accountand the contents database functional block 345 which saves contents.<BR>[0284]The contents bill creation function part 351 which takes charge of creation of a bill in case the above-mentioned contents acquisition functional block 342 charges contents to the system management organization 330The contents receipt creation function part 352 which takes charge of creation of a receipt when contents are received from the system management organization 330It consists of the function part 353 corresponding to a contents database which takes charge of correspondence with these \*\*\*\* and \*\* contentsand the contents saved at the contents database functional block 345.<BR>[0285]The content display function part 354 which takes charge of the function for which the above-mentioned content display functional block 343 actually exhibits contents to virtual online shopIt consists of the function part 355 corresponding to a contents database which takes charge of correspondence with the contents currently these-exhibited and the contents saved at the above-mentioned contents database functional block 345.<BR>[0286]The above-mentioned balancing account functional block 344 consists of the receipt issuing function part 356 which takes charge of the function to publish a receiptand the function part 357 corresponding to the financial institution which takes charge of correspondence between the financial institutions 220.<BR>[0287]Nextthe composition of accounting information control machine seki 320 is explained using <A HREF="JP-A-H10-269289.files/000038.gif">drawing 36</A>.<BR>[0288]In this <A HREF="JP-A-H10-269289.files/000038.gif">drawing 36</A>accounting information control machine Seki 320 concernedThe communication function block 361 which divides roughly and takes charge of the communication function between user side 200 and the system management organization 330The royalty issuing function block 362 which takes charge of the function to publish a royaltyA contents keyand the contents key and service-condition receipt functional block 363 which take charge of the receipt of a service conditionA contents keyand the contents key and service-condition issuing function block 364 which take charge of issue of a service conditionIt consists of the balancing account procedure reception functional block 365 which takes charge of the receptionist function of balancing account procedurethe distribution receipt functional block 366 which takes charge of the function of a receipt as distributionand the database function block 376.<BR>[0289]The purchase written request acknowledgement function part 371 in which the above-mentioned royalty issuing function block 362 takes charge of the acknowledgement function of a purchase written requestThe point-data acknowledgement function part 372 which takes charge of the check of the data of the balance (balance of point information) of the royalty of clienti.e.userside 200use record (point usage information)etc.The royalty generating function part 373 which takes charge of the function to generate a royaltyand the royalty invoice creation function part 374 which takes charge of the function which draws up the invoice of a royaltyIt consists of a royaltythe sending function part 375 which takes charge of the function to actually send a royalty invoicethe royalty receipt acknowledgement function part 376 which takes charge of the check of the receipt document of a royaltyand the royalty issuing information preservation function part 377 which takes charge of the function to save the information on the published royalty.<BR>[0290]Above-mentioned contents key and service-condition receipt functional block 363 <DP N=0025><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>consist of a contents keythe receipt function part 378 which takes charge of the receipt of a service conditionand a contents key and the preservation function part 379 which saves a service condition.<BR>[0291]Above-mentioned contents key and service-condition issuing function block 364A contents key and the receiving function part 380 which takes charge of the function to receive the acquisition request of a service conditionThe search service part 381 which takes charge of the function which searches and discovers a contents key and a service condition from the database function block 367It consists of the transmitting-function part 382 which takes charge of the function to encipher and send a contents key and a service conditionand a contents key and the acknowledgement function part 383 which takes charge of the acknowledgement function of the receipt document of a service condition.<BR>[0292]The contents use record receiving function part 384 which takes

charge of the function which the above-mentioned balancing account procedure reception functional block 365 receives the contents use record (point usage information) enciphered and is decrypted. The contents use record acknowledgement function part 385 which takes charge of the check of contents use record. The contents use record-keeping function part 386 which takes charge of the function in which the database function block 367 saves contents use record. It consists of the completion document creation function part 387 which takes charge of the function which draws up the completion document of balancing account procedure and the conclusion function part 389 which takes charge of the function to edit contents use record collectively.

[0293] The bill acknowledgement function part 390 which takes charge of the acknowledgement function of the request-for-information document which charges the data at the time of the above-mentioned distribution receipt functional block 366 collecting money. The use record report writer feature part 391 which takes charge of the function which draws up the report of the contents use record submitted to the system management organization 330. It consists of the royalty issue report writer feature part 392 which takes charge of the function which draws up the report of the royalty issuing information submitted to the system management organization 330 and the written confirmation acknowledgement function part 393 which takes charge of the acknowledgement function of the confirmation-of-receipt document of a report.

[0294] The royalty database function part 394 which takes charge of the function in which the database function block 367 saves the data of a royalty. A contents key and the contents key and royalty database function part 395 which take charge of the function to save the data of a service condition. It consists of the user management data base function part 397 which saves the information about the contents use recording data base function part 396 which saves contents use record and a user.

[0295] Next the composition of the system management organization 330 is explained using [drawing 37](JP-A-H10-269289.files/000039.gif).

[0296] In this [drawing 37](JP-A-H10-269289.files/000039.gif) the system management organization 330 concerned. The communication function block 401 which divides roughly and takes charge of the communication function between user side 200, the content exhibiting distributing institution 310 and accounting information control machine Seki 320. It consists of the user subscription support functional block 402 which performs the support in the case of user subscription, the contents distribution functional block 404 which takes charge of distribution of contents, the database function block 403 and collection of money and the collection-of-money \*\*\*\* distribution frame block 405 which takes charge of the function of distribution.

<TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> [0297] The above-mentioned user subscription support functional block 402. Creation of a subscription request and the subscription request creation transmitting-function part 411 which takes charge of transmission. The common key receiving function part 412 which takes charge of the function which receives and decrypts the enciphered common key. The subscription request acknowledgement function part 413 which takes charge of the acknowledgement function of the subscription request transmitted from user side 200. The ID generating function part 414 which takes charge of the function to generate client ID, i.e. user ID. The subscription request preservation function part 415 which takes charge of the function to save a subscription request at the database function block 403. It consists of the client function generation function part 416 which generates a client function and the registration information preservation function part 417 which takes charge of the function to save registration information at the database function block 403.

[0298] The user management data base function part 418 to which the database function block 403 carries out preservation management of a user's information. The contents database function part 419 which saves contents and the accounting information control machine Seki database function part 420 which carries out preservation management of the information on accounting information control machine Seki 320. It consists of the content-exhibiting-distributing-institution database function part 421 which carries out preservation management of the information of the content exhibiting distributing institution 310.

[0299] The bill acknowledgement function part 422 in which the contents distribution functional block 404 takes charge of the acknowledgement function of the bill of contents. The content retrieval function part 423 which takes charge of the function to search ready-mixed concrete TENTSU (source data), i.e. the contents before processing from the contents database function part 419 of the database function block 403. The content ID generation function part 424 which

generates content ID and the contents key generation function part 425 which generates a contents key. The contents service-condition generation function part 426 which generates a contents service condition. The contents compression function part 427 which compresses ready-mixed concrete TENTSUI.e.the contents before processing. The preservation function part 429 which takes charge of the function to save the contents processing function part 428 which enciphers contents and content ID a contents key and a service condition at the contents database function part 419 of the database function block 403. The contents sending function part 430 which takes charge of the function to send contents via the communication function block 401 and the contents receipt acknowledgement function part 431 which takes charge of the function to check the receipt of contents. Content ID a contents key and ID key and service-condition sending function part 432 that take charge of the function to send a service condition via the communication function block 401. It consists of content ID a contents key and ID key and service-condition receipt acknowledgement function part 433 that take charge of the function to check the receipt of a service condition. <BR>[0300] The request-for-information document creation function part 434 which makes out the bill of the data which use collection of money and the distribution frame block 405 for collection of money. The contents royalty receiving function part 435 which takes charge of the function to receive a contents royalty via the communication function block 401. The <DP N=0026><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> contents use record receiving function part 436 which takes charge of the function to receive contents use record via the communication function block 401. The confirmation-of-receipt document creation function part 437 which takes charge of the function which draws up the written confirmation of reception. It consists of the calculation and the bill creation function part 438 which makes out the bill which performs the calculation of the amount billed and the creation of a bill which are charged to a user calculation of the dividend at the time of distributing the use gold collected by use to a right holder and the calculation and the form-for-payment creation function part 439 which perform creation of a form for payment. <BR>[0301] next -- being concerned -- others -- the composition of user side 200 corresponding to the system of an embodiment is explained using <A HREF="JP-A-H10-269289.files/000040.gif">drawing 38</A>. This <A HREF="JP-A-H10-269289.files/000040.gif">drawing 38 </A> expresses each function of said player 1 and the user terminal 50 collectively. <BR>[0302] In this <A HREF="JP-A-H10-269289.files/000040.gif">drawing 38</A> the composition of concerned user side 200. The communication function block 451 which will take charge of the communication function between the system management organization 330 the content exhibiting distributing institution 310 and accounting information control machine Seki 320 if it divides roughly. The contents acquisition functional block 452 which takes charge of acquisition of contents. The royalty purchasing function block 453 which takes charge of the purchase of royalty such as point information a contents key a service condition a contents key and the contents key and service-condition acquisition functional block 454 which take charge of acquisition of a service condition. The balancing account procedure functional block 455 which takes charge of balancing account procedure and the user subscription support functional block 456 which takes charge of the function which supports subscription to a system. It consists of appreciation of contents the contents appreciation accounting function block 457 which takes charge of the function of fee collection and the database function block 458. <BR>[0303] The above-mentioned contents acquisition functional block 452 consists of the contents acquisition function part 461 which takes charge of the function which actually obtains contents and the contents preservation function part 462 which takes charge of the function in which contents are made to save at a memory medium. <BR>[0304] The purchase written request creation function part 463 in which the royalty purchasing function block 453 draws up the purchase written request of a royalty. The conclusion function part 464 which takes charge of the conclusion of the data of the balance (point balance) of the royalty of a client (user) use record (point usage information) etc. It consists of the royalty installation function part 465 which takes charge of the function which installs each information as a royalty and the royalty receipt document creation function part 467 which draws up a royalty receipt document. <BR>[0305] A contents key and the service-condition acquisition functional block 454. It consists of a contents key the acquisition written request creation function part 468 which draws up the acquisition written request of a service condition a contents key and the receiving

function part 469 which takes charge of reception of a service condition and a contents key and the receipt document creation function part 470 which draws up the receipt document of a service condition. <BR> [0306] The balancing account procedure functional block 455 consists of the conclusion function part 471 which performs the conclusion of contents use record (point usage information) and the completion document receiving function part 472 which takes charge of reception of the completion document of balancing account procedure. <BR> <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300> [0307] The above-mentioned user subscription support functional block 456 It consists of the subscription request creation function part 473 which takes charge of creation of a subscription request the client function installation function part 474 which takes charge of installation of a client function i.e. initialization of a user's player land the registration information creation function part 475 which takes charge of the function which creates registration information. <BR> [0308] The content retrieval function part 476 which takes charge of search of the contents by which the contents appreciation accounting function block 457 was saved at the memory medium The royalty acknowledgement function part 477 which takes charge of the check of a royalty and the simple contents appreciation function part 478 which reproduces contents in [ when choosing contents for example ] simple The accounting function part 479 which manages accounting information (point information) and the contents function decoding part 480 which decrypts the contents enciphered It consists of the contents extension function part 481 which elongates the contents compressed and the contents viewer function part 482 for enabling recognition of the contents of the contents saved at the memory medium for example. <BR> [0309] The royalty database function part 483 where the database function block 458 saves the data of a royalty It consists of a contents key the contents key and service-condition database function part 484 which save a service condition the contents use recording data base function part 485 which saves contents use record and the user information data base function part 486 which saves User Information. <BR> [0310] Next the player 1 of each embodiment which was mentioned above and the concrete using form of the user terminal 50 are explained using <A HREF="JP-A-H10-269289.files/000041.gif">drawing 39 </A> and <A HREF="JP-A-H10-269289.files/000042.gif">drawing 40 </A>. <BR> [0311] As shown in <A HREF="JP-A-H10-269289.files/000041.gif">drawing 39 </A> the player 1 is arranged after said analog output terminal 2 the interface terminal 3 for PC and the I/O terminal 4 for memory media have projected out of the case of the player land the memory medium 61 is connected to the above-mentioned I/O terminal 4 for memory media. For example in the case 60 these players 1 and the memory medium 61 are formed so that storage is possible and they are made as [ arrange / for example at the end side of this case 60 / the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC ]. <BR> [0312] The case 60 where this player 1 and memory medium 61 were stored From the side by which the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC are arranged it is formed in the input/output port 53 of the personal computer 50 as the above-mentioned user terminal 50 so that insertion connecting may be possible. <BR> [0313] Although the personal computer 50 concerned has the general composition which equipped the computer body with the display device 52 the keyboard 54 and the mouse 55 In the above-mentioned input/output port 53 the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC and the corresponding interface are formed. <DP N=0027> <TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300> Therefore only by inserting in the input/output port 53 of the above-mentioned personal computer 50 the case 60 where the above-mentioned player 1 and the memory medium 61 were stored The analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC come to be connected with the above-mentioned personal computer 50. <BR> [0314] Although he is trying to form an interface [ in the input/output port 53 of the personal computer 50 / terminal / 3 / for PC / the analog output terminal 2 of the above-mentioned player land / interface ] in the example of above-mentioned <A HREF="JP-A-H10-269289.files/000041.gif">drawing 39 </A> For example as shown in <A HREF="JP-A-H10-269289.files/000042.gif">drawing 40 </A> it is also possible to arrange the adapter 62 which can respond to the interface of the general-purpose input/output port of the personal computer 50 between the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC. <BR> [0315] In the system of an embodiment of the invention since it has stated above since digital

contents are enciphered with the contents key which is a common key of a system. If it is the user (player 1) who registered with the system of this embodiment, if only it can copy these enciphered contents freely and a contents key comes to hand, appreciation of these contents is also possible. Therefore, installation to this contents memory medium (enciphered contents) can also be performed easily. On the other hand, since the enciphered digital contents cannot be decoded, the right of the copyright of contents or the right holder of the contents concerned is protected by the terminal unit which is not based on this embodiment system. <BR>[0316] an embodiment of the invention while according to the system filling up point information with a prepaid system (charge advance payment method) and reducing point information at the time of contents appreciation. Since he is trying to collect the usage information of the point, recovery of an appreciation price is possible for right holders (owner of a copyright etc.) a contents selling store etc. with the right about a used point. <BR>[0317] Since encryption is given in the case of an exchange of the data of point information or point usage information as mentioned above, security nature is improving. For example, since it shall trade after checking that use the random number (security ID) which interlocked by the system and player side and both are in agreement as mentioned above even if the completely same thing as the last data is forged and it tries to steal the point information for fee collection, it is safe. <BR>[0318] 1 chip making of the main components of a player is carried out and it is difficult to take out key information and the decrypted digital contents outside. This player 1 equips player 1 the very thing with the tamper resistance function in order to prevent the data usurpation by destruction of the player 1 concerned. <BR>[0319] As mentioned above according to the embodiment of the invention, the digital contents distributing system with high security top intensity is built. <BR><TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>[0320] As above-mentioned digital contents, various kinds of things other than digital audio informations such as a digital video data can be mentioned. When dynamic-image-data (audio information is also included) use is carried out as the above-mentioned digital video data as the technique of said compression compression method such as MPEG (Moving Picture Image Coding Experts Group) can be used for example. The above-mentioned MPEG in WG (Working Group) 11 of SC (Sub Committee) 29 of JTC (Joint Technical Committee) 1 of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). It is a common name of the packed video coding mode and there are MPEG1 MPEG2 MPEG4 etc. <BR>[0321] As the technique of the above-mentioned encryption as mentioned above, the enciphering method currently called what is called DES (Data Encryption Standard) can be used. DES is the standard cipher system (cryptographic algorithm) which NIST (National Institute of Standards and Technology) in the U.S. announced in 1976. Data conversion is performed for every 64-bit data block and specifically the conversion using a function is repeated 16 times. The above-mentioned digital contents point information etc. are enciphered with what is called a common key system using the DES concerned. It is a method which becomes the same [ the key (decode key data) for decrypting with the key data (encryption key data) for enciphering ] as that of the above-mentioned common key system. <BR>[0322] what is called an EEPROM (electrically eliminable ROM) can be used for the common key storage memory 22 of the player 1 of said <A HREF="JP-A-H10-269289.files/000003.gif">drawing 1</A> the key storage memory 21 for communication, the point usage information storing memory 29 and point information storing memory 28 grade for example. <BR>[0323] As a memory medium, the memory medium of recording media such as a hard disk, a floppy disk, a magneto-optical disc and a phase-change optical disk or semiconductor memory (IC card etc.) can be used for others for example. <BR>[0324] In addition, although selection check etc. were performed in the above-mentioned embodiment using the keyboard 54 of the user terminal 50 and the mouse 55 and the display device 52 on the occasion such as content confirmation etc. of the contents exhibited by selection and the virtual online shop 230 of contents, it is also possible to simplify a function to these keyboards or a mouse and a display device and to give the player 1, namely, Like <A HREF="JP-A-H10-269289.files/000004.gif">drawing 2</A> it is also possible to form the input key part 6 and the indicator 7 in the player 1. <BR>[0325] <BR>[Effect of the Invention] It is possible to be able to do carrying simply in the above explanation according to this invention so that clearly and to enjoy digital contents anywhere always. It is <DP N=0028><TXF FR=0001 HE=005 WI=080 LX=0200 LY=0300> possible also in it being equal to employment enough as the copy of digital contents or



defense to unjust use and building an economical system.

</SDO><BR><HR><B>DESCRIPTION OF DRAWINGS</B><BR><HR><SDO EDJ><TXF FR=0002 HE=245 WI=080 LX=0200 LY=0350>[Brief Description of the Drawings]<BR><A HREF="JP-A-H10-269289.files/000003.gif">[Drawing 1]</A>It is a system configuration figure showing the entire configuration of the digital contents distribution system of an embodiment of the invention.<BR><A HREF="JP-A-H10-269289.files/000004.gif">[Drawing 2]</A>It is a block circuit diagram showing the concrete composition of the player corresponding to the system of an embodiment of the invention.<BR><A HREF="JP-A-H10-269289.files/000005.gif">[Drawing 3]</A>It is a block circuit diagram showing the concrete composition of the control center corresponding to the system of an embodiment of the invention.<BR><A HREF="JP-A-H10-269289.files/000006.gif">[Drawing 4]</A>It is a figure used for explanation of the procedure at the time of the purchase of a player in the system of this embodiment.<BR><A HREF="JP-A-H10-269289.files/000007.gif">[Drawing 5]</A>It is a figure used for explanation of the procedure to installation of the digital contents from search of digital contents to the memory medium for players in the system of this embodiment.<BR><A HREF="JP-A-H10-269289.files/000008.gif">[Drawing 6]</A>It is a figure used for explanation of the procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for fee collection in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000009.gif">[Drawing 7]</A>It is a figure used for explanation of the procedure of distribution of a fee collection price in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000010.gif">[Drawing 8]</A>It is a flow chart which shows the flow of the processing in the player at the time of point purchase in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000011.gif">[Drawing 9]</A>It is a flow chart which shows the flow of the processing in the user terminal at the time of point purchase in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000012.gif">[Drawing 10]</A>It is a flow chart which shows the flow of the processing in the control center at the time of point purchase in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000013.gif">[Drawing 11]</A>It is a figure showing the sequence of the information transmission and reception at the time of point purchase in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000014.gif">[Drawing 12]</A>It is a flow chart which shows the flow of the processing in the player at the time of acquisition of digital contents in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000015.gif">[Drawing 13]</A>It is a flow chart which shows the flow of the processing in the user terminal at the time of acquisition of digital contents in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000016.gif">[Drawing 14]</A>It is a flow chart which shows the flow of the processing in the control center at the time of acquisition of digital contents in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000017.gif">[Drawing 15]</A>It is a figure showing the sequence of the information transmission and reception at the time of acquisition of digital contents in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000018.gif">[Drawing 16]</A>It is a flow chart which shows the flow of the processing in the player at the time of acquisition of a contents key and a service condition in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000019.gif">[Drawing 17]</A>It is a flow chart which shows the flow of the processing in a contents key and the user terminal at the time of acquisition of a service condition in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000020.gif">[Drawing 18]</A>It <TXF FR=0003 HE=250 WI=080 LX=1100 LY=0300>is a flow chart which shows the flow of the processing in the control center at the time of acquisition of a contents key and a service condition in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000021.gif">[Drawing 19]</A>It is a figure showing the sequence of the information transmission and reception at the time of acquisition of a contents key and a service condition in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000022.gif">[Drawing 20]</A>It is a flow chart which shows the flow of the processing at the time of actually appreciating digital contents using a player and a user terminal in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000023.gif">[Drawing 21]</A>It is a flow chart which

JPA\_1998-269289\_translation

shows the flow of the processing in the player at the time of point usage information return in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000024.gif">[Drawing 22]</A>It is a flow chart which shows the flow of the processing in the user terminal at the time of point usage information return in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000025.gif">[Drawing 23]</A>It is a flow chart which shows the flow of the processing in the control center at the time of point usage information return in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000026.gif">[Drawing 24]</A>It is a figure showing the sequence of the information transmission and reception at the time of point usage information return in the system of an embodiment.<BR><A HREF="JP-A-H10-269289.files/000027.gif">[Drawing 25]</A>It is a flow chart which shows the flow of the processing at the time of performing decryption and extension in the least common multiple of the batch of encryption and compression.<BR><A HREF="JP-A-H10-269289.files/000028.gif">[Drawing 26]</A>It is a block circuit diagram showing the composition which performs encryption/decryption for every unit of the least common multiple of a compressive batch and elongation processing.<BR><A HREF="JP-A-H10-269289.files/000029.gif">[Drawing 27]</A>It is a block circuit diagram showing the concrete composition which generates the random number as security ID.<BR><A HREF="JP-A-H10-269289.files/000030.gif">[Drawing 28]</A>when enciphering a common key with a public-key crypto system and transmitting it is a figure for explaining signs that a random number is inserted.<BR><A HREF="JP-A-H10-269289.files/000031.gif">[Drawing 29]</A>It is a figure for explaining signs that a random number is taken out from a receiving sentence and the check of justification is made.<BR><A HREF="JP-A-H10-269289.files/000032.gif">[Drawing 30]</A>It is a figure used for explanation of each organization when the function by the side of a system is divided.<BR><A HREF="JP-A-H10-269289.files/000033.gif">[Drawing 31]</A>In the embodiment which divided the function by the side of a system it is a figure for explaining the principal part of the flow of the time of subscription to a user's system.<BR><A HREF="JP-A-H10-269289.files/000034.gif">[Drawing 32]</A>In the embodiment which divided the function by the side of a system it is a figure for explaining the principal part of the information flow at the time of acquisition of the key the purchase of point information and for decoding of the enciphered digital content setc.<BR><A HREF="JP-A-H10-269289.files/000035.gif">[Drawing 33]</A>In the embodiment which divided the function by the side of a system it is a figure for explaining the principal part of the flow in the case of circulation of the information for contents and contents appreciation.<BR><A HREF="JP-A-H10-269289.files/000036.gif">[Drawing 34]</A>In the embodiment which divided the function by the side of a system it is a figure for explaining the principal part of the flow of balancing account when contents are actually appreciated.<BR><A HREF="JP-A-H10-269289.files/000037.gif">[Drawing 35]</A>In the embodiment which divided the function by the side of a system it is a block diagram showing the composition of content exhibiting distributing institution.<BR><A HREF="JP-A-H10-269289.files/000038.gif">[Drawing 36]</A><DP N=0029><TXF FR=0001 HE=065 WI=080 LX=0200 LY=0300>In the embodiment which divided the function by the side of a system it is a block diagram showing the composition of accounting information control machine Seki.<BR><A HREF="JP-A-H10-269289.files/000039.gif">[Drawing 37]</A>In the embodiment which divided the function by the side of a system it is a block diagram showing the composition of a system management organization.<BR><A HREF="JP-A-H10-269289.files/000040.gif">[Drawing 38]</A>In the embodiment which divided the function by the side of a system it is a block diagram showing users' composition.<BR><A HREF="JP-A-H10-269289.files/000041.gif">[Drawing 39]</A>It is a figure used for explanation of an example of the concrete using form of a player and a user terminal.<BR><A HREF="JP-A-H10-269289.files/000042.gif">[Drawing 40]</A>It is a figure used for explanation of other examples of the concrete using form of a player and a user terminal.<BR>[Description of Notations]<BR>1 A player 2 analog output terminal the <TXF FR=0002 HE=065 WI=080 LX=1100 LY=0300> interface terminal for 3 PCThe I/O terminal for 4 memory media and 16 A controller and 19 Security ID generating circuit 20 An open code decoder circuit and 21 The key storage memory for communication and 22 Common key storage memory 23 A user ID storing memory and 24 A common code decoder circuit and 25 buffer memories 26 An expansion circuit 27 D/A

JPA\_1998-269289\_translation

conversion circuits50 user terminalsand a 100 contents-managing functional blockA  
110 user-management functional block and 120 [ A financial institution and 230 /  
Virtual online shop and 240 / Content provider ] A usage information  
controlling-function block and 130 A controlling-function block and 200 The user  
side210 system management companies211 control centersand  
220<BR></SDO><BR><HR></BODY></HTML>

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number  
**WO 01/31599 A1**

(51) International Patent Classification?: G07F 17/16, 7/08

Hulst [NL/GB]; 23 Tanza Road, Hampstead, London NW3 2UA (GB). RACZ, Patrick, Sandor [GB/—]; 19 Royal Square, St. Helier, Jersey JE1 4WA (GB).

(21) International Application Number: PCT/GB00/04110

(22) International Filing Date: 25 October 2000 (25.10.2000)

(74) Agent: LUCKHURST, Anthony, Henry, William; Marks & Clerk, 57-60 Lincolns Inn Fields, London WC2A 3LS (GB).

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
9925227.2 25 October 1999 (25.10.1999) GB

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(71) Applicant (for all designated States except US): SMART-FLASH LIMITED [GB/GB]; Upper Nordens, High Hurst Wood, Uckfield, East Sussex TN22 4AN (GB).

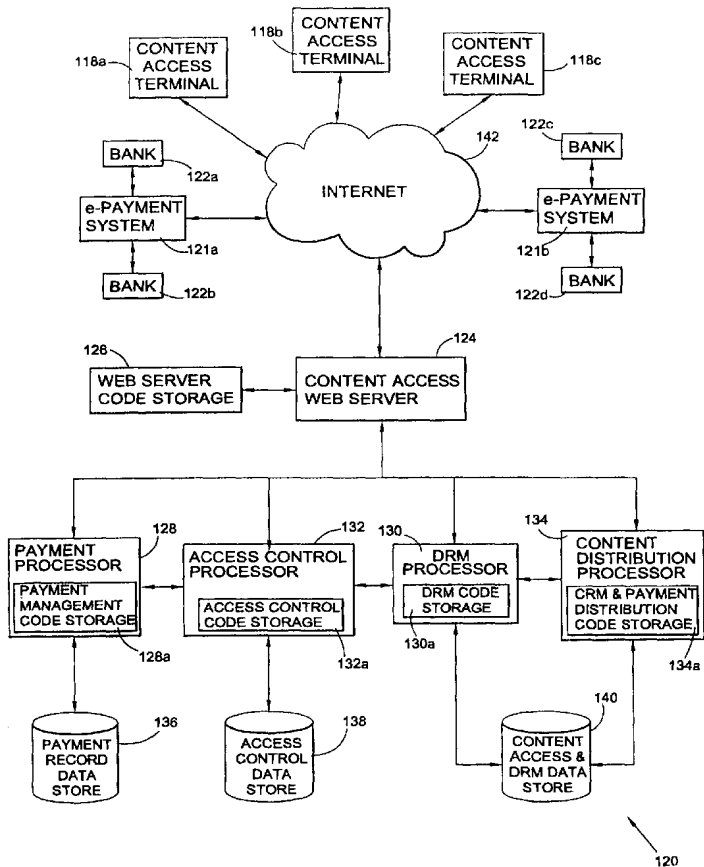
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

(72) Inventors; and

(75) Inventors/Applicants (for US only): HERMEN-ARD,

[Continued on next page]

(54) Title: DATA STORAGE AND ACCESS SYSTEMS



(57) Abstract: Data storage and access systems are described for downloading and paying for data such as audio and video data, text, software, games and other types of data. A portable data carrier has an interface for sending and receiving data, non-volatile data memory for storing received content data and non-volatile payment validation memory for providing payment validation data to an external device. The carrier may also store a record of access made to the stored content, and content use rules for controlling access to the stored content. Preferred embodiments store further access control data and supplementary data such as hot links to web sites and/or advertising data. A complementary data access terminal, data supply computer system and data access device are also described. The combination of payment data and stored content data and, in preferred embodiments, use rule data, helps reduce the risk of unauthorised access to data such as compressed music and video data, especially over the internet.

WO 01/31599 A1



IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

— *With international search report.*

### DATA STORAGE AND ACCESS SYSTEMS

This invention is generally concerned with data storage and access systems. More particularly, it relates to a portable data carrier for storing and paying for data and to computer systems for providing access to data to be stored. The invention also includes corresponding methods and computer programs. The invention is particularly useful for managing stored audio and video data, but may also be applied to storage and access of text and software, including games, as well as other types of data.

Once problem associated with the increasingly wide use of the internet is the growing prevalence of so-called data pirates. Such pirates obtain data either by unauthorised or legitimate means and then make this data available essentially world-wide over the internet without authorisation. Data can be a very valuable commodity, but once it has been published on the Internet it is difficult to police access to and use of it by Internet users who may not even realise that it is pirated. This is a particular problem with audio recordings, and, once the bandwidth becomes available, is also likely to be evident with video.

Over the past three or four years compressed audio sources have become increasingly widely available on web pages. One widely used audio data compression format is MP3 (MPEG3) which is an internationally defined standard including a definition of compressed audio information such as speech or music. It relies on psycho-acoustic properties of human hearing to achieve very large data compression factors. It is thus feasible to download usefully long passages of music in a practically convenient short time. Pirate data suppliers have not been slow to realise the potential of this and many unauthorised websites have sprung up offering popular music including recent releases by world famous bands. This has caused the recording industry considerable concern and there is an urgent need to find a way to address the problem of data piracy.

The invention described below addresses this and related problems.

According to the present invention there is therefore provided a method of providing portable data comprising providing a portable data storage device comprising downloaded data storage means and payment validation means; providing a terminal for internet access; coupling the portable data storage device to the terminal; reading payment information from the payment validation means using the terminal; validating the payment information; and downloading data into the portable storage device from a data supplier.

Another aspect of the invention provides a corresponding mobile data retrieval device for retrieving and outputting data such as stored music and/or noise from the data storage device.

The payment validation means is, for example, means to validate payment with an external authority such as a bank or building society. The combination of the payment validation means with the data storage means allows the access to the downloaded data which is to be stored by the data storage means, to be made conditional upon checked and validated payment being made for the data. Binding the data access and payment together allows the legitimate owners of the data to make the data available themselves over the internet without fear of loss of revenue, thus undermining the position of data pirates.

A further advantage of the system is that it allows users under the age of 18 to make internet purchases. Currently internet users pay for goods and/or services by credit card. Since credit cards cannot be legitimately be used by persons under the age of 18 (at least in the UK), a significant fraction of adventurous internet users are excluded from e-commerce, one of the most significant predicted uses of the internet. In one embodiment of the invention however, the payment validation means comprises e-cash - that is the payment validation means stores transaction value information on a cash

value of transactions validatable by the data storage means. In simple terms, the data storage means can be a card which is charged up to a desired cash value (if necessary limited to a maximum value) at a suitable terminal. This might be an internet access terminal but could, more simply, be a device to accept the data storage card and to receive and count money deposited by the user to charge the card, writing update cash value information onto the card. More sophisticated ways of updating the cash value on the card are also possible, such as direct bank transfer. Since, with this type of embodiment, the data storage means is, essentially, precharged with cash rather than acting as a credit card it can be used by young people without the risk of their incurring large debts.

In one embodiment the data storage means is powered by the retrieval device when it is connected to the device and retains a memory of the downloaded data when it is unpowered. This can be achieved by the use of Flash RAM or, more generally, any form of programmable read-only memory. Alternatively the data storage means may incorporate a rechargeable cell or capacitor and store information in battery backed-up static RAM.

The downloaded data maybe entered into the data storage device by means of an interface such as a magnetically or capacitatively coupled connection or an optical connection, but preferably the interface comprises contacts for direct electrical connection to the storage means. The payment validation means may likewise have one of a variety of interfaces but again preferably comprises a set of electrical contacts. The payment validation means could, however comprise a magnetic or holographic data-strip such as is known for use with credit cards and phone cards. The interface to receive the downloaded data may be separate from the interface to the payment validation means, to facilitate separate and simultaneous access to both these systems. In other embodiments a single interface may serve for both data storage and payment. Advantageously the payment validation means includes a memory storing information to identify the person who is paying for the downloaded data.



For additional security the downloaded data may be encrypted. In this case data decryption may be necessary at some stage, either in the data storage means or in the retrieval device or in an information delivering apparatus such as a data access terminal. Alternatively the data decryption function can be shared amongst one or more of these devices. The skilled person will be aware of a range of suitable encryption/decryption techniques including Pretty Good Privacy (Registered Trade Mark) and PKI (Public Key Infrastructure). Normally when the downloaded data is encrypted a decryption key must be supplied. This can be generated automatically by the data access terminal or data access service provider or it can be entered by the user into the data access terminal or into the mobile data retrieval device.

The data storage means and/or the retrieval device can be provided with access control means to prevent unauthorised access to the downloaded data. Additionally or alternatively, use control means can be provided to stop or provide only limited access of the user to the downloaded data in accordance with the amount paid. These access and use control functions may in some embodiments be combined, permitted use controlling access or permitted access controlling use. Thus, for example, a complete set of data information relating to a particular topic, a particular music track, or a particular software package might be downloaded, although access to part of the data set might thereafter be controlled by payments made by a user at a later stage. In this way, a user could pay to enable an extra level on a game or to enable further tracks of an album.

In embodiments where the access or use control means is responsive to the payment validation means, access or use control information may be stored with the downloaded data or in a separate storage area, for example in the payment validation means. The user's access to the downloaded data could advantageously be responsive to the payment validation means, for example, by means of a control line coupling the payment validation means with a memory access or decryption control element.

In one embodiment the data storage means comprises an electronic memory card or smart card and the mobile data retrieval device is provided with a slot to receive the card. Preferably the card is a push-fit within the retrieval device, and retention of the card may be effected by pressure from electrical interface connections and/or resilience of the housing, or by using a resilient retaining means. In a preferred embodiment the retrieval device includes an audio output and a display, to play a downloaded track and to show information about the track and/or an accompanying video.

To download data onto the data storage means the user can employ a data access terminal coupled to the internet. The terminal can directly validate payment - for example in the case of a smart card charged with electronic cash it can deduct a cash value from the card. Alternatively it can communicate with a bank or other financial services provider to control payment. In a preferred embodiment, however, the terminal connects to a data access service provider which provides a portal to other sites and which validates payment and then forwards data from a data supplier to the user's local access terminal. The data access service provider may alternatively forward payment validation information and/or information from the payment validation authority to the data supplier for control by the supplier of the data supplied. Thus, access to the payment validation system and/or data for downloading may be entirely controlled by the data supplier.

Data held on the data storage means may advantageously include data relating to the user's or payer's usage of the system. This information may include, for example, information on a user's spending pattern, information on data suppliers used and information on the downloaded data. This information may be accessed by the data supplier and/or data access service provider and can be used for targeted marketing or loyalty-based incentive schemes such as air miles or the like.

The data access terminal may be a conventional computer or, alternatively, it may be a mobile phone. Wireless Application Protocol (WAP) and i-mode allow mobile phones to efficiently access the internet and this allows a mobile phone to be used to download

data to the data storage means, advantageously, directly. The data storage means can, if desired, incorporate the functionality of a mobile phone SIM (Subscriber Identity Module) card, which cards already include a user identification means, to allow user billing through the phone network operator.

In preferred embodiment the downloaded data is MP3 or other encoded audio data, but the system finds more general application for other data types. For example, download data can include software, and particularly games, share price information, current news information, transport timetable information, weather information and catalogue shopping information. The downloaded information may also include compressed video data. The storage capacity of the data storage means is adaptable to suit the type of data intended to be downloaded - for example, 32 megabytes is sufficient for CD quality music, but for video it is preferable that the data storage means has a capacity of 128 megabytes or greater.

In another aspect, the invention provides a portable data carrier comprising an interface for reading and writing data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; non-volatile payment data memory, coupled to the interface, for providing payment data to an external device.

These features allow the data carrier to store both payment data and content data thus providing the advantages outlined above. Depending upon the payment system used, the payment data memory may also store code for validating or confirming a payment to an external payment system. The payment data will normally be linked to card or card holder identification data for payment by the card holder. The non-volatile memory ensures that stored content and payment data is retained in the data carrier when the data carrier is not receiving power from an external source. Thus "non-volatile" encompasses, for example, low-power memory whose contents are retained by a battery back-up system. In one embodiment the payment data memory comprises EEPROM and the content data memory comprises Flash memory, but other types of content data memory, such as optical, for example, holographic, data memory can also be used. The

data carrier may also be integrated into other apparatus, such as a mobile communications device.

Preferably, the portable data carrier further comprises a program store storing code implementable by a processor; and a processor, coupled to the content data memory, the payment data memory, the interface and to the program store for implementing code in the program store, wherein the code comprises code to output payment data from the payment data memory to the interface and code to provide external access to the data memory.

Normally, the (content) data memory allows both write and read access for both storing and retrieving data, but in some embodiments the content data memory may be read only memory. In such embodiments, content may be pre-loaded onto the carrier and payment may then be made for permission to access the pre-loaded data.

Preferably, the data carrier also stores a record of access made to the content data and updates this in response to external access, preferably read access, made to the data memory. The carrier may also store content use rules pertaining to allowed use of stored data items. These use rules may be linked to payments made from the card to provide payment options such as access to buy content data outright; rental access to content data for a time period or for a specified number of access events; and/or rental/purchase, for example where rental use is provided together with an option to purchase content data at the reduced price after rental access has expired.

Thus where the data carrier stores, for example, music the purchase outright option may be equivalent to the purchase of a compact disc (CD), preferably with some form of content copy protection such as digital watermarking. In this example, the rental or subscription payment option may be a pay-per-play option, and with this option payment may either be before or after access to the stored data so that the carrier may operate in either a debit or credit payment mode.

The portability of the data carrier potentially allows it to be used to access content or, in the example, play music without the need to be linked to a communications system or to be on-line to the internet. By providing a use record memory on the data carrier, use of the stored data can be tracked whilst off-line and then any necessary payment can be made when the data carrier is next coupled to a communication system. This allows the data carrier to operate in a credit mode. In a debit mode, the additional storage of use rules facilitates the regulation of access to content data stored on the carrier without the need for further exchange of payment/use data with an external system to validate the use.

By combining digital rights management with content data storage using a single carrier the stored content data becomes mobile and can be accessed anywhere whilst retaining control over the stored data for the data content provider or data copyright owner. Preferably, the data carrier also stores access control data, such as a user ID and a password, as the stored data may be valuable. The access control data may be combined with access control to the payment data, which is typically by means of a PIN (Personal Identification Number) to simplify access to valued content stored on the carrier.

In one embodiment the stored content data is encrypted and a unique password or PIN and/or biometric data is required for decryption. The data carrier may be arranged so that the content is erased after a predetermined number of incorrect access attempts. Additionally or alternatively, a permanently stored flag may be set and/or a hardware modification (such as a fusible link) may be made to prevent the data carrier from functioning for further data storage/retrieval. Preferably, however, access to any stored value/payment data is nevertheless retained.

Supplementary data may also be stored on the carrier in association with stored content data. This supplementary data may comprise customer reward management data and/or advertising data. The supplementary data may comprise a pointer to an external data source from which data is downloaded either to the data carrier or to a data access

device or content player, so that advertising or other data can be displayed when reviewing or accessing the stored content.

Additional data security and/or a mechanism for rewarding operators at different levels in the data supply chain may be provided using a content synthesis function. The content synthesis function combines partial content information from two or more sources to provide content data items for storage and/or output. Thus, for example, a first percentage of a content data item could be provided by a content retailer whilst a remaining percentage could be provided by an on-line data supplier. This would provide an incentive for a user to register with a content retailer or distributor as well as with an on-line scheme owner and so could encourage the use of existing retailers and could provide a mechanism for paying commission to such retailers. The two portions of data combined to provide a content data item could comprise encryption data and a key but preferably comprise separate parts of a complete data item, for example, least significant bits and most significant bits or high frequencies and low frequencies (for audio). This arrangement also facilitates customer reward and loyalty management.

In one embodiment the data carrier further comprises memory for storing data for accessing a mobile communications network, for example to receive content data over the network. For such an embodiment, the data carrier may replace a SIM (Subscriber Identity Module) card in a mobile communications device, thus providing a single card for both network access and valued content retrieval and storage. Additionally or alternatively the card may also store the web address of a data supplier from whom data may be downloaded onto the carrier.

The data memory for storing content data may be optic, magnetic or semiconductor memory, but preferably comprises Flash memory. Preferably, the data memory has a large capacity for storing large data files such as compressed video data. Preferably, the data memory is partitioned for lock access, that is for read and/or write access to blocks of, for example, 1K, 4K, 16K or 64K databytes for faster data access, particularly where the stored content data will normally be accessed serially, as is normally the case with

audio and video data. Preferably the card is configured as an IC card or smart card and has a credit card-type format, although other formats such as the "memory stick" format may also be used. This provides a small and convenient portable format and facilitates removable interfacing with a variety of devices.

The invention also provides a related method of controlling access to data on a data carrier, the data carrier comprising non-volatile data memory and non-volatile parameter memory storing use status data and use rules, the method comprising receiving a data access request; reading the use status data and use rules from memory; and evaluating the use status data using the use rules to determine whether access to the stored data is permitted.

According to another aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a pointer to a data provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item from the requester; code to receive from the communications interface payment data comprising data relating to payment for the requested data item; code responsive to the request and to the received payment data, to read data for the requested data item from a content provider; and code to transmit the read data to the requester over the communications interface.

The computer system is operated by a data supplier or data supply "scheme owner" for providing content data to the data carrier described above. The payment data received may either be data relating to an actual payment made to the data supplier, or it may be a record of a payment made to an e-payment system relating either to a payment to the data supplier, or to a payment to a third party. The data from the content provider, preferably without permanent (local) storage of the forwarded data. This improves data

security as the content provider retains control over a content data item and the data supplier, a copy of a data item, is unable to supply data for the item without the content provider's assistance. The computer system may provide temporary storage for a requested data item, for example, using a disk cache, but preferably the computer system does not store a complete data item, even temporarily.

Preferably, the computer system includes payment distribution information so that when payment is made for a data item, the payment can be distributed for reimbursing royalties and making other payments. Typically a large fraction of the payment for a data item will be transferred to a copyright owner or "content provider" for the item whilst smaller payments will go to the artist and/or publisher and/or retailer/distributor. Payment may be made directly by the computer system to the computer systems of other relevant parties using, for example, a signature-transporting type E-payment system. Alternatively, the computer system can issue appropriate instructions to a third party E-payment system for making the transfers. The computer system allows automatic distribution of payments either before, during or after content data download, or after content data access by a user. Instructions for distributing the payments may be issued substantially simultaneously, thereby avoiding long delays in the payment of some parties - for example, it can presently take a year or more for an artist generating content to be paid by conventional methods.

Preferably, the computer system also stores content data item access rule data, for downloading in association with a content data item. The rule data may be stored by a content provider but is preferably held by the computer system, and links a content identifier with an access rule, typically based upon a required payment value, as outlined above in the context of the data carrier. Normally, each content data item will have an associated access rule, but a single rule may apply to a large number of data items. The computer system also, preferably, stores requester reward data for customer reward/loyalty management. This data may again comprise one or more rules linking a payment value and/or content data item type to a specified reward, such as a number of air miles or retailer value points. The computer system preferably also keeps a record of



an identified user's or data's carriers content item downloads and payments for market research purposes.

The computer system, in one embodiment, also stores access control data, such as an access request identity and password which can be employed, for example, to create an extranet of system users, which again can be linked to stored access record data for marketing purposes. When further linked to content item type data, such an arrangement can be used to construct a club of users of content data items of a particular type, for example, country and western or rock and roll music. As described in connection with the portable data carrier, the computer system may also comprise content synthesis code for additional data security and for more secure management of payment distributions.

The invention also provides a related method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; reading the requested data from a content provider responsive to the received payment data; and transmitting the read data to the requester.

According to a further aspect of the present invention, there is provided a data access terminal for retrieving data from a data supplier and providing the retrieved data to a data carrier, the terminal comprising a first interface for communicating with the data supplier; a data carrier interface for interfacing with the data carrier; a program store storing code implementable by a processor; and a processor, coupled to the first interface, the data carrier interface and to the program store for implementing the stored code, the code comprising: code to read payment data from the data carrier and to forward the payment data to a payment validation system; code to receive payment validation data from the payment validation system; code responsive to the payment validation data to retrieve data from the data supplier and to write the retrieved data into the data carrier.

This terminal can be used for retrieving data from the above described computer system and for downloading the retrieved data to the above described portable data carrier. As with the data supply computer system, it is preferable that there is no (local) storage of content item data forwarded from the data supplier to the data carrier. The data access terminal is not restricted to use with the above described status supplier and could, for example, retrieve data for downloading to the data carrier from a local data source, such as a CD (Compact Disc) or DVD (Digital Versatile Disc), or from a third party such as a cable TV company.

The terminal reads payment data from the data carrier and transmits this to a payment validation system for validating the data and authorising the payment. This may be part of the data supplier's computer system or it may be a separate system such as an e-payment system. Thus, the terminal operates with a data carrier storing payment (validation) data and, in some embodiments, additional payment validation code for validating payment to the payment validation system. Again, the terminal is preferably configured to provide a data item use rule to the carrier in conjunction with a data item. As before, the data item use rule will normally be dependent upon payment value information embodied in the payment data read from the data carrier. The terminal is preferably also configured for user input of access control data. This access control data may be forwarded to the data carrier for access permission verification and/or it may be passed to the data supplier computer system for a similar purpose. The terminal may be configured to warn a user of content access or data carrier function inhibition after a predetermined number of access requests have been refused. The terminal may also incorporate content synthesis code as described above.

The terminal may comprise code to output supplementary data when downloading data to the data carrier. Identity data on the data carrier can be used to retrieve the supplementary data, or a pointer to the supplementary data, from the data supplier computer system, or the supplementary data or a pointer thereto can be retrieved directly from the data carrier. Preferably, however, identification data on the card is used to retrieve characterising data such as card user preference data from the data supplier

computer system, and this characterising data is then used by the terminal to retrieve and output supplementary data to a terminal user. When the terminal is associated with a contact distributor or retailer, the supplementary data may be retrieved over a network associated with the retailer/distributor such as a local area network (LAN), wide area network (WAN) or extranet.

The invention also provides a method of providing data from a data supplier to a data carrier, the method comprising reading payment data from the data carrier; forwarding the payment data to a payment validation system; retrieving data from the data supplier; and writing the retrieved data into the data carrier.

The payment validation system may be part of the data supplier's computer systems or it may be a separate e-payment system. In one embodiment the method further comprises receiving payment validation data from the payment validation system; and transmitting at least a portion of the payment validation data to the data supplier. Alternatively the payment validation system may comprise a payment processor at the data supplier or at a destination retrieved from the data supplier. The payment processor may also provide payment distribution data for distributing a payment represented by the payment data.

In a further aspect, the invention provides a data access device for retrieving stored data from a data carrier, the device comprising a user interface; a data carrier interface; a program store storing code implementable by a processor; and a processor coupled to the user interface, to the data carrier interface and to the program store for implementing the stored code, the code comprising code to retrieve use status data indicating a use status of data stored on the carrier, and use rules data indicating permissible use of data stored on the carrier; code to evaluate the use status data using the use rules data to determine whether access is permitted to the stored data; and code to access the stored data when access is permitted.

The data access device uses the use status data and use rules to determine what access is permitted to data stored on the data carrier. As described above, the use rules will

normally be dependent upon payments made for data stored on the data carrier, but may also comprise access control employing a user identification and password. Since a single data carrier may have more than one user, the use status and use rules may be selected dependent upon a user identity. The data access device may also be configured to present supplementary data when presenting the content data, retrieved as described above, from the card, from a remote computer system or from some other source such as a cable TV network or off-air.

The invention also provides a related method of controlling access to data from a data carrier, comprising retrieving use status data from the data carrier indicating past use of the stored data; retrieving use rules from the data carrier; evaluating the use status data using the use rules to determine whether access to data stored on the carrier is permitted; and permitting access to the data on the data carrier dependent on the result of said evaluating.

According to a further aspect of the invention there is provided a data access system comprising a data supply computer system for forwarding data from a data provider to a data access terminal; a electronic payment system for confirming an electronic payment; a data access terminal for communicating with the data supply system to write data from the data supply system onto a data carrier; and a data carrier for storing data from the data supply system and payment data; wherein data is forwarded from the data provider to the data carrier on validation of payment data provided from the data carrier to the electronic payment system.

In a further aspect of the invention, there is provided a portable data carrier comprising an interface for sending and receiving data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; and a digital rights management processor for controlling access to the stored data.

In a further aspect of the invention, there is provided a portable data carrier comprising an interface for sending and receiving data from and to the carrier; non-volatile data

memory, coupled to the interface, for storing data on the carrier; and an access control processor; wherein the data memory is partitioned as data blocks and the access control processor controls external access to the data blocks.

In a further aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a resource locator a data provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item; code, responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

In a further aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a printer location data identifying an electronic address for a provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item; code responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein said data access data store further comprises data item access rule data for output to the

requester with a said data item; and further comprising code to select access rule data for output with a data item in response to said payment data.

In a yet further aspect of the invention, there is provided a method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; transmitting the requested data to the requester; reading payment distribution information from a data store; and outputting payment data to a payment system for distributing the payment for the requested data.

In a still further aspect of the invention, there is provided a method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; transmitting the requested data to the requester; and transmitting data access rule data to requester with the read data.

These and other aspects of the invention will now be further described, by way of example, only, with reference to the accompanying figures in which:-

Figure 1 shows a data access device a) from the top; b) from the front; and c) from the side;

Figure 2 shows, conceptually, a portable data carrier;

Figures 3a and b show exemplary data access terminals;

Figure 4a and b show, respectively, a logical signal path between elements of a conceptual data access system; and a physical representation of a conceptual data access system;

Figure 5 shows a content provision system;

Figure 6 shows a data supply computer system;

Figure 7 shows a variety of data access terminals;

Figure 8 shows a schematic diagram of components of a data access terminal;

Figure 9 shows a schematic diagram of components of a data carrier;

Figure 10 shows a schematic diagram of components of a data access device;

Figures 11a and 11b show a flow diagrams of a data carrier registration process;

Figures 12a-c and 12d-e show, respectively, a flow diagram of data access using a data access terminal; and a flow diagram of data supply using a data supply computer system; and

Figure 13 shows a flow diagram of data retrieval using a data access device.

Referring to Figure 1, this shows a data access device for playing MP3 audio (10) with operator controls (12) and LCD display (14). The outline of a smart card data storage device is shown at (16). The operator controls allow a user to select and play tracks, whilst track information and still or video images are provided on display (14). A slot (18) is provided in the front of the device to receive a smart card-type data storage means. This smart card occupies space (20) and interfaces with resilient contacts (24); it is held in the data retrieval device against the contacts, by resilient housing element (22).

Referring now to Figure 2, this shows a portable data carrier (30) suitable for use with the device of Figure 1. The data storage means is based on a standard smart card; it is plastic, about the size of a standard credit card, and has some flexibility. On the card

(30) are two sets of contacts, contacts (32) for interfacing with the payment validation means and contacts (34) for interfacing with the memory for storing downloaded data (although in other embodiments, a single set of contacts may be used for both). The surface of the card can be embellished with suitable graphics.

In one embodiment the smart card retains all its useable functionality as specified for standard Electronics Point of Sale Systems (EPOSS) and, if desired, the memory for storing the downloaded data can be electrically separate from this. However, it may be preferable to provide interaction between the standard smart card device and the data memory in order to accomplish the access control/decryption functions described above.

Referring now to Figure 3, an example of a data access terminal is shown at (40). This has a screen (42) and a slot (44) to receive the data carrier (30). Alternatively the data carrier may interface to the terminal via the data access device (10) and an interface (46) to the terminal (40). In Figure 3b a dedicated terminal (50) has a slot (52) to receive the data carrier, a display (54) and controls (56). Coins can be inserted into the terminal at (58) and notes at (60) to charge the data carrier with cash.

Referring now to Figure 4a, this illustrates conceptually the logical connections and data flow between data processing systems involved in payment validation, and data download to the carrier (30). A user connects the data carrier (30) to terminal (40) and logs on to a data web page of data supply service provider (60). Either terminal (40) or service provider (60) then communicates via data paths (62) with a payment validation authority (70) to check and authorise the user's or payer's payment. In the case of electronic cash the terminal (40) may immediately validate the payment information, updating the service provider and/or payment validation authority (70) at a later stage. The logical connection (64) between the terminal and the service provider is preferably made over the internet.

The service provider may provide a direct portal to data providers (80) or may collect information from data suppliers (80) and provide a "front end" to present data from the



suppliers to the terminal user. Alternatively data supply service provider (60) may regulate direct access between terminal (40) and data providers (80), as shown by links (66), by communicating with the terminal and the data providers to provide communication regulation information to, for example, instruct data suppliers about what information the user of terminal (40) should have access to.

In a preferred embodiment service provider (60) pays royalties at an agreed rate - for example, 10 pence per track or 10 pence per minute - to a computer system owned by a company or entity in the recording industry, such as a content provider or copyright owner, a content publisher or a content creator, and the user of terminal (40) effectively pays the service provider. Billing can also be regulated by bandwidth and/or data download time.

Preferably the service provider (60) monitors the user's access to the system and either stores or forwards to data providers (80), or downloads to the data carrier (30), usage information. In a preferred embodiment the service provider sends information via terminal (40) to data carrier (30) which can be used to determine incentives to be provided to users of the system.

Figure 4b shows a conceptual physical configuration of the system of Figure 4a in which a plurality of terminals (40), a plurality of service providers (60) and a plurality of data providers (80) all interact via the internet. The physical embodiment of the system is not critical and a skilled person will understand that the terminals, data processing systems and the like can all take a variety of forms.

Referring now to Figure 5, this shows a conceptual illustration of a content provision system 100. Content creators 104a, b generate or receive content data from artist terminals 102a-d and store content data in databases 106a, b. The content data stored in databases 106a, b may comprise audio data, such as music, video data, such as films or TV programs, text, such as literary works, software, such as games software, or other data. Content creators 104a, b are coupled to communications network 101 for

communicating created content data over the network. Also coupled to communications network 101 are content publishers 110a and 110b, each of which is coupled to an associated stored content database, 112a and 112b respectively. The content publishers make their stored content available for controlled access using communications network 101. In some instances, for example where the content data comprises computer games, the functions of content creator and content publisher may be provided by a single entity. Also although conceptually illustrated as blocks in Figure 5, the content creator and content publisher typically each comprise a client server computer network.

The communications network 101 is typically a private communications network, such as an extranet, with security controlled access to entities connected to the network. Physically the network may comprise an internet protocol network or it may comprise, or consist of, dedicated point-to-point links. Thus, for example, a content creator 104 may be directly linked to a content publisher 110 and/or to other entities shown in Figure 5 such as a content provider or content distributor.

The content provision system includes a plurality of content providers 108a-e, each coupled to the communications network 101. In the illustrated system, the content providers own copyright in stored content data accessible over communications network 101 and may, in practice, also perform a content publication function. Five content providers own the copyright in over 80% of all world-wide music sales. The content providers are coupled to stored content databases 106 and 112 via communications network 101, for supplying stored content data.

A gateway server 114 is also coupled to communications network 101 to link the communications network to other networks such as the internet and/or mobile communications networks. Gateway server 114 provides security and access control functions and firewalls. A second gateway, content distributor WAN gateway 116 is also shown attached to communications network 101. This provides similar security and firewall functions and coupled communications network 101 to distributor WAN (wide area network) 117. Gateway 116 has logical access to one or more of a content

creator, content publisher and content provider for accessing stored content data. Content distributor gateway 116 may be owned by a chain of record stores and provide content access terminals 118, coupled to WAN 117, in separate retail outlets. Content access terminals 118 have access, via gateway 116, to stored content accessible over communications network 101.

Referring now to Figure 6, this shows a data supply computer system 120. In this embodiment, three content access terminals 118a-c, e-payment systems 121a, b, and content access web server 124 are all coupled to internet 142. Data supply system 120 is coupled to the content provision system 100 illustrated in Figure 5. Where Communications network 101 of Figure 5 is an extranet, this extranet physically operates over internet 142; where communications network 101 does not partly operate via internet 142, a connection to internet 142 is established via gateway server 114 as shown in Figure 5. In this way content access terminals 118a-c are provided with controlled access to the stored content data of content provision system 100.

E-payment systems 121a and 121b are coupled to banks 122a, b and c, d respectively. These provide an e-payment system according to, for example, MONDEX, Proton, and/or Visa cash compliant standards. Preferably at least one of e-payment systems 121a, b operates a so-called "open purse" system in which the value is stored as a publicly verifiable digital signature issued by the e-payment system. In such a signature-transporting arrangement payment data may be validated using public keys and thus payment authentication need not be performed by the e-payment system but may instead be performed by, for example, a data access terminal or data supply system computer, using payment management code. The authenticated signatures, which in effect perform a similar role to cheques, are submitted to the relevant e-payment system after authentication for verification and reimbursement or transfer of monetary value. With such a system payments may be made anonymously and thus payer identification is not essential. Data carriers, such as data cards, may be issued with stored value or without value, in which latter case value (that is a publicly verifiable digital signature) may be written onto the card during an on-line transaction.

In alternative embodiments, a data carrier such as the smart flash card described below may be used to create value bearing digital signatures as is well-known to those familiar with e-money.

Content access web server 124 is also coupled to internet 142 for providing content access terminals 118a-c with access to content data. Content access web server 124 is typically owned by a content data supply "scheme owner" who acts as an intermediary between a content access terminal user and a content provider, forwarding content data provided (directly or indirectly) by a content provider to a content access terminal and thence to a stored content data carrier. Web server 124 is coupled to web server code storage 126 storing Java code for generating web pages for interpretation by web browsers on content access terminals 111a-c. The web pages provide the content download, value add, CRM (customer reward management) value cheque/spend and website link functions described below.

Web server 124 is coupled to payment processor 128, Digital Rights Management (DRM) processor 130, access control processor 132, and content distribution processor 134. Payment processor 128 includes payment management code storage 128a and is coupled to payment record data store 136. Access control processor 132 includes access control code storage 132a and is coupled to access control data store 138. DRM processor 130 includes DRM code storage 130a and is coupled to content access and DRM data store 140. Content distribution processor 134 includes CRM (customer reward management) and payment distribution management code storage 134a and is also coupled to content access and DRM data store 140. As shown in Figure 6, processors 128-134 are all in communication with one another.

Processors 128, 130, 132 and 134 may comprise separate application programs or a single computer program and may operate on a single physical computer, on which web server 124 may also be provided, or may operate on separate computers. Likewise data stores 136, 138 and 140 may comprise a single physical data store or may be distributed

over a plurality of physical devices and may even be at physically remote locations from processors 128-134 and coupled to these processors via internet 142.

Web server 124 communicates with processors 128-134 by means of a CGI (common gateway interface) script and the code associated with processors 128-134 may be written in any conventional computer language such as C, C++, or Perl. However, in other embodiments one or more of the processors may be coupled to web server 124 via internet 142 and owned and operated by a separate entity, such as a financial institution. In this case conventional secure web-based communications may be operated between web server 124 and the relevant processor. In particular, payment processor 128 may be operated by one of the e-payment system providers 128a, b.

Payment management code 128a issues and authenticates payment data and stores an audit record in payment record data store 136. Access control code 132a stores identification data (of a user or card) together with registration data provided by user when registering with the scheme owner. This data comprises a user password for accessing stored content and/or payment data; user characterising data, for example characterising user preferences, for marketing purposes; data indicating an e-payment system to use; and in some embodiments, further general user related data such as card level data for identifying the provision of "gold" level services to selected users. A copy of the password is stored with the content data on the portable data carrier, as described further below. Alternatively, one or both of the access control data store and portable data carrier may simply store data for verifying a user-entered password.

Content access and DRM data store 140 stores data related to content access and content use, but does not itself store content data items; these are instead provided via content provision system 100 described above. Data store 140 stores a plurality of records each comprising a data item identifier, a data item description, a data item type or genre, and location data comprising one or more pointers to a location or locations from where the data item can be downloaded. Associated with a data item is also a table of use rule data comprising a list of values (i.e. content data item prices) and corresponding levels

of permitted usage. Thus a value of £1 might permit ten plays of a music track, whilst the value of £10 might permit an unlimited number of plays of the track and copying of the track for personal use.

Also associated with a data item is a table of payment distribution data comprising a list of recipients and corresponding fractions of the data item value each is to receive. Typically, the main recipient will be the copyright owner of the data item and other recipients will be selected from the content creator, the artist or artists, the scheme owner, the content publisher, and the retailer/distributor. The payment distribution proportions may be dependent upon the payment value in which case a plurality of sets of payment distribution figures may be associated with each data item, each set of distribution figures corresponding to a payment value range. The payment data and distribution data is here termed DRM (Digital Rights Management) data.

Further associated with a data item is a table of CRM (Customer Reward Management) data, linked to the user rule data, comprising CRM rules to specify, for one or more data item use levels, a quantity of reward points and one or more recipients for the reward points (the recipients may include the card user and the retailer/distributor).

The CRM and payment distribution code 134a operates with content access and DRM data store 140 to inform a system user of the description and value of a data item, to access and download a data item from the content provider system to a content access terminal, to provide content use rules with the data item, and to provide instructions either to payment processor 128 or to E-payment system 121 to distribute payments for the data item to the recipients identified by the data store 140 and to distribute CRM reward points.

The access control data store 138 holds a secure key, such as a secret "public" key in a public key cryptography system, for the scheme owner to authenticate its identity to a content provider. This data is held securely with other sensitive data in the access control data store 138. As is described in more detail below, when data supply system

120 receives a request for a content data item from a content access terminal 118, it looks up a location from which the data item is available using content access and DRM data store 140 and then determines the identity of the corresponding content provider. This identity is either stored in content access and DRM data store 140 or, as there are relatively few content providers, it may be hard written in DRM code 130a. DRM code 130 then requests access control processor 132 to provide the secure scheme owner identifier from access control data store 138 to the relevant content provider and sets up a trusted connection between the content provider and content access web server 124 for downloading the data item to a content access terminal 118 and thence to a portable data carrier.

Referring now to Figure 7, this shows a variety of content access terminals for accessing data supply computer system 120 over internet 142. The terminals are provided with an interface to a portable data carrier or "smart Flash card" (SFC) as generally described with reference to Figure 2 and as described in more detail below. In most embodiments of the terminal the SFC interface allows the smart Flash card data carrier to be inserted into and removed from the terminal, but in some embodiments the data carrier may be integral with the terminal.

Referring now to the specific embodiments illustrated in Figure 7, a simple content access terminal may comprise a home personal computer 144 with SFC interface 144a. In another embodiment, a mobile communications device 152 is provided with a smart Flash card interface 152a and is coupled to internet 142 via radio tower 150, mobile communications system 148 and mobile communications internet gateway 146.

In another embodiment, a smart Flash card interface is provided to a so-called "set top box" (STB) 154. The set top box is, in effect, a receiver for television programmes received on video input 154b, which may comprise a satellite TV signal, a cable TV signal or an off-air TV signal. The video signal is provided from the set top box to television 156 or to some other home entertainment device such as a personal computer (not shown). In another embodiment content access terminals 166 and 168 each with

respective SFC interfaces 166a and 168a are coupled to a retailer local area network (LAN) 160 connected to internet 142 via retailer LAN server 158. DVD player 164 is also coupled to LAN 160. In a further embodiment a smart Flash card interface 170a is provided for a CD/DVD player 170.

In these latter three embodiments, content data for storage on the smart Flash card may be retrieved from broadcast video and/or a CD or DVD. In this case, the computer data supply system 120 illustrated in Figure 6 may be used to provide use rule data for the content data stored on the smart Flash card, and to pay for data downloaded onto the card; the content data may be captured before or after the data supply system 120 is accessed to enable use of the stored data, but in a preferred embodiment content data written to the card from a supplier other than the content data supply computer system is not accessible to a user until corresponding use rule data has been downloaded from computer system 120, which will normally be after receiving payment for the downloaded data.

Referring now to Figure 8, this shows a schematic diagram of one embodiment of a data access terminal 170. The terminal comprises a general purpose computer including an audio/visual interface 184, a keyboard 186 and a pointing device 188 for providing an interface to the user. The terminal has an internet interface 176, for example a modem, and optionally a LAN/WAN interface 174 for connecting the terminal to a retailer or distributor LAN or WAN. The terminal also has an optional video input 178 for receiving broadcast video data and a media input device 180, such as a CD or DVD drive. Further communications I/O ports 182 may also be provided. A portable data carrier or smart Flash card interface 190 is provided for interfacing to a smart Flash card. Optionally, a cash input and verification system 192, such as is conventionally used in an automatic teller machine (ATM) may also be incorporated within the content access terminal. The terminal has working memory 194 such as RAM and program memory 196 which can comprise any conventional storage device such as RAM, ROM or a disk drive. Program code in program memory 196 may also be stored on removable disk 198. A processor 200 loads and implements program code stored in program



memory 196. All the components of the terminal are linked by a data and communications bus 172.

More specifically, processor 200 loads and implements cash payment management code 200a for managing cash input data from cash input and verification system 192, for adding value to a smart Flash card. Processor 200 also implements a web browser 200b for accessing scheme owner web pages and data exchange interface 200c for exchanging data between a smart Flash card interface to the terminal and data supply system 120.

Processor 200 also implements off-line contents retrieval code 200d for retrieving data for storage on a smart Flash card from media input device 180 and/or video input 178 and/or LAN/WAN interface 174. The processor implements a content sampler 200e for outputting small extracts of content data items to a user via audio/visual interface 184. Such data item samples may be stored with the content description data in content access data store 140. The processor also implements a smart Flash card interface driver 200f, user interface code 200g and additional communication drivers 200h for driving LAN/WAN interface 174 and/or comms I/O ports 182.

Referring now to Figure 9, this shows a schematic diagram of components of a portable data carrier 202, in the embodiment shown a so-called "smart Flash card". In this context, "smart Flash card" refers to an IC card similar in size to a plastic payment card incorporating a processor and Flash data memory, preferably of large capacity. For further details on smart cards reference may be made to the ISO (International Standards Organisation) series of standards including ISO 7810, ISO 7811, ISO 7812, ISO 7813, ISO 7816, ISO 9992 and ISO 10102, which are hereby incorporated by reference.

Referring in more detail to Figure 9, a data and communications bus 204 links components of the card which include a processor 210, working memory 212, timing and control logic 208 and an external interface which may have contacts (ISO 7816) or be contactless (ISO 10536) for providing external access to a bus 204 for reading data from and writing data to the card 202. Also coupled to bus 204 are permanent program

memory 216, non-volatile data memory 218 and non-volatile (Flash) content data memory 214. Non-volatile data memory 218 may comprise EEPROM and permanent program memory 216 may comprise ROM, for example, mask-programmed ROM. All the components of Figure 9 are mounted on a single substrate, in a preferred embodiment bearing contacts for external interface 206.

Processor 200 loads and implements program code from permanent program memory 216. This code comprises operating system code for providing the card with a basic operating system for at least external communications, payment management code for supplying payment data from non-volatile data memory 218 to pay for downloaded content; DRM (Digital Rights Management) and security code including code to implement content data use rules and code for password controlled access to data and program functions; CRM code for implementing CRM-related rules; and content synthesis code for combining stored content data with additional data provided via external interface 206 for synthesising complete content item data.

Non-volatile data memory 218 stores data including card identity data, access control data, including password data for validating a user password, access record data for storing a record of access attempts and their outcomes, and content supply data such as scheme owner website addresses and retailer/distributor website addresses.

Data memory 218 further stores card value data comprising E-money such as publicly verifiable digital signatures, and payment data for storing a payment audit trail including payment amounts and data on to whom payments have been made. The memory 218 also stores RFM (Recency Frequency Monetary) data to provide a record of transactions for market research and customer reward purposes, and CRM data storing customer reward points. Data memory 218 also stores an index of content data items stored in Flash memory 214 and associated content use rules, as well as DRM and royalty data for maintaining an audit trail of use history for rights management tracking. Optionally, data memory 218 may also store supply chain data specifying a supply chain route through which data has been obtained from a content provider, which may be used for

rewarding supply chain intermediaries, for example on a commission or reward points basis.

Content data memory 214 preferably comprises at least 100 MB of data storage, partitioned as data blocks of a size selected to match the stored content type. For storing video data Flash memory 214 preferably comprises > 1 GB data storage and the data blocks into which the data memory is partitioned are larger.

Referring now to Figure 10, this shows a schematic diagram of a data access device 220, such as a portable audio/video player. The data access device 220 comprises a conventional dedicated computer system including a processor 238, permanent program memory 236, such as ROM, working memory 234, such as RAM, and timing and control logic 226 all coupled by a data and communications bus 222. Also coupled to the bus are an audio interface 228, a display 230 and user controls 232, for providing a user interface. A smart Flash card interface 224 is coupled to bus 222 for interfacing with a smart Flash card for retrieving and playing stored content data.

Permanent program memory 236 stores program code for implementation by processor 238; this code may also be provided on a data carrier such as a ROM chip or disk 240. Processor 238 implements an SFC interface 238a, a user interface 238b, a content player 238d for retrieving stored content data from a smart Flash card interfaced to the device and for outputting audio and/or video data derived from the retrieved content data (which may comprise compressed audio and/or video data) to a user of the device.

Processor 238 also implements use control 238c for controlling access to and use of contents stored on the smart Flash card by the content access device user. Use control routine 238c and/or DRM and security code in permanent memory 216 on the smart Flash card may also implement digital watermarking and other Secure Digital Music Initiative (SDMI) content protection code as specified in the SDMI portable device specification, part one, version 1.0 (see [www.sdmi.org](http://www.sdmi.org)) which is hereby incorporated by reference.

Figures 11a and 11b show a flow diagram of a process for registering a data carrier or smart Flash card with a data supplier or scheme owner operating a data supply system as illustrated in Figure 6. A smart Flash card may be issued entirely blank, that is, with no prestored content or value, with prestored value but no prestored content, with prestored content but not prestored value (the content being provided free) or with both prestored value and prestored content. Thus, for example, a user may purchase a card with stored value but no stored content over the counter at a retailer. The process of Figures 11a and 11b illustrates the registration of a card with neither prestored content nor prestored value. As illustrated the registration process records user registration data in the access control data store 138 of Figure 6 and writes value data onto the blank card.

At step S10 a smart Flash card is inserted into a content access terminal smart Flash card interface. The scheme owner web page is then loaded onto the content access terminal and displayed to the user (step S11). User registration data is then entered into the content access terminal (step S12) and transmitted to the scheme owner (S13), the user registration data may include a user identity, a preferred e-payment system to use and, optionally, a content access PIN or password, and a service level (for example bronze, silver or gold). The optional password may be a password required by the e-payment system for validation of a payment by the user with the card or it may be a password to protect unauthorised access to content on a smart Flash card to protect stored data in the event, for example, of the card being stolen. A single password may serve both these functions. The content access terminal web browser is configured so that all sensitive data passing between the terminal and the scheme owner is securely transmitted, for example by using a conventional encryption system such as PKI (Public Key Infrastructure).

At step S14 a payment request is received from the scheme owner at the content access terminal and displayed to the user. At step S15 the user enters payment data into the content access terminal and this payment data is transmitted to the scheme owner, for adding value to the card. This may, for example, be a credit card transaction as is

conventionally used for purchase over the internet. Card value data and a card value access code is then received by the content access terminal from the scheme owner at step S16. The card value corresponds to the payment made by the user and the value access code may be a password entered by the user at step S12 or may comprise a password for PIN created by payment processor 128 or e-payment system 121 as illustrated in Figure 6. In a preferred embodiment, the user pays the scheme owner and the scheme owner then directly provides digital signature data representing value to the content access terminal for writing onto the smart Flash card.

At step S17, card registration data is received from the scheme owner by the content access terminal and written onto the smart Flash card. This card registration data comprises user identity data, access control data, payment system specifying data, scheme owner access data, such as a scheme owner web page address and other dial-up information. At this stage other data may be entered by the user and written onto the card including, for example, user preference data, retail outlet and CRM data (alternatively user preference data may be captured at step S12). At step S18 the card value data and card value access code received at step S16 is written onto the card and output to the user visually and, optionally, as a printed record. The card is then available for use, at step S19.

Figure 11b shows the corresponding registration steps performed by the scheme owner's data supply system 120. At step S20, a request for a smart card registration web page is received from a content access device and, at step S21, transmitted to the device. User registration data is then received, at step S22, from the content access terminal and stored in content access control data store 138. The scheme owner's computer system then transmits, at step S23, a payment request to the content access terminal and receives, at step S24, payment data in reply, this payment is then authenticated, at step S25, with an E-payment system such as payment system 121 a or b illustrated in Figure 6, and after verification the payment processor 128 of the computer system transmits, at step S26, value data and a value access code to the content access terminal, for writing onto the smart Flash card. The payment processor then updates the payment record data

store 136 with data relating to the transaction (step S27) and, at step S28, retrieves card registration data previously written into the access control data store and transmits this registration data to the content access terminal. At step S29 the transaction is then complete.

Referring now to Figures 12a to c, these illustrate a flow chart for downloading data to a smart Flash card using a data access terminal. At step S30 the smart Flash card is inserted into the content access terminal and the user then enters, at step S31, their password for gaining access to the functionality of the smart Flash card. At step S32, the content access terminal transmits the password to the smart card for verification and the terminal checks, at step S33, whether access is permitted. If access is not permitted a warning is displayed by the terminal, at step S34, and an access denied count is implemented. A threshold count is then read from the card together with a count of the total number of times access to the card has been denied (step S35). At step S36 the terminal checks whether the total number of denied accesses is within three of the card threshold, and if it is not, returns to step S31 whilst if it is, it proceeds to step S37 where the terminal displays a warning that a further denied access is likely to result in erasure of content stored on the card. At step S38 the terminal then checks whether its count of denied accesses is greater than its threshold value, returning to step S31 if not, and displaying an access refused message at step S39 if the total number of permitted accesses has been exceeded. The system then waits at step S39 for removal of the smart Flash card from the content access terminal.

If access is permitted at step S33, the terminal loads outline CRM data from the card (step S40) and loads retail data, such as targeted advertising, from the retailer LAN/WAN (step S41). At step S42, the terminal then displays a menu of options, retail data such as advertising or CRM-related data and outline CRM data, such as a total number of reward points earned, on the content access terminal. Many options include download content (from a scheme owner), add monetary value (to the card), check/spend CRM value stored on the card, follow website links, and exit. At step S43, the user inputs a menu option which, in the illustrated flow chart, is the download

option. The system thus passes to step S44 and loads the scheme owner's content access web page onto the content access terminal and displays this to the user.

At step S45, the user enters a content search request, which is transmitted to the scheme owner content distributor processor 134. Content search results are received back from the content distribution processor, including a content identifier, a brief description, and content cost data for at least one payment option, and these results are displayed on the user on the content access terminal. The user then selects one or more content items at step S47 and the selection is transmitted to the content distribution processor 134 where further content cost data and purchase option data is retrieved from data store 140. At step S48, this content cost and purchase data (including use rule data) is received from the scheme owner and displayed to the terminal user. The user then selects, at step S49, a purchase option and confirms a purchase request or, alternatively, selects "exit" to return to the menu display of step S42. After one or more content items have been selected, together with a purchase option, hard value and CRM data is read from the smart Flash card at step S50 and at step S51 a check is made to determine whether the monetary and/or CRM (reward points) value stored on the smart Flash card is sufficient to purchase the selected purchase data items. If the card value is insufficient, a warning is displayed at step S52 and the system returns to the menu display at step S42. If the card value is sufficient, at step S53 the content access terminal transmits a payment request to the smart Flash card.

Payment for the data item or items requested may either be made directly to the scheme owner or may be made to an e-payment system such as e-payment systems 121a and 121b of Figure 6, with these systems then forwarding payment confirmation data to the scheme owner computer system. Alternatively, the content access terminal may transmit data to the card to set up a transaction directly with a content provider who, being the copyright owner, would normally receive the majority of the payment.

At step S54, payment data for making a payment to the scheme owner is received from the smart Flash card by the content access terminal and forwarded to an e-payment

system such as E-payment system 121 in Figure 6. Payment record data, validating payment by the card to the scheme owner is then received back from the e-payment system at step S55 by the content access terminal and forwarded to the card for updating payment data on the card. In alternative embodiments, payment data from the card may be provided directly to the scheme owner's data supply computer for authentication and, optionally, further validation with an e-payment system by the scheme owner's computer.

Distribution of the payment received by the scheme owner from the card is performed by the scheme owner's computer system, as described elsewhere. Such payment distribution will normally provide a small percentage of the total payment to a "owner" or operator of the content access terminal, such as a retailer, distributor, or in other embodiments, mobile communications network operator or cable TV network operator.

In the presently described embodiment payment record data received in step S55 is transmitted to the scheme owner to confirm payment by the card and thus it is the content access terminal, in the described embodiment, which authenticates a payment before confirming that the payment has been made to the scheme owner.

In step S56, together with the payment record data, purchase request and card registration data is transmitted to the scheme owner to identify one or more content data items for purchase and to identify the purchaser. Then, at step S57, the content access terminal sets up a transaction between the scheme owner data supply computer and the smart Flash card for download of the identified content items requested from the data supplier to the smart Flash card. The download is preferably arranged so that there is no permanent storage of downloaded data on the content access terminal (although temporary storage in a disk cache may be permissible), and there is further preferably no temporary storage on the content access terminal of complete data for a content data item. This provides data security and reassurance to the content providers.



In the same way as with card registration described with regard to Figure 11, a secure and trusted link is set up between the content access terminal and/or the smart Flash card and the data supply computer in a conventional manner as is well known to those skilled in the art (for example, using public key data encryption). The data transaction may be set up directly between the smart Flash card and the data supply computer, in which case the content access terminal has no access to unencrypted content data, or it may be set up between the content access terminal and the data supply computer, in which case unencrypted data is written by the content access terminal to the smart Flash card. Standard transmission protocols are used to ensure complete transmission of a content data item, for example by re-transmitting blocks of data which are not correctly received.

Also at step S57, one or more content access rules is received from the scheme owner data supply computer and written to the smart Flash card so that each content data item has an associated use rule to specify under what conditions a user of the smart Flash card is allowed access to the content data item.

At step S58 the content access terminal receives CRM data from the content distribution processor 134 of the scheme owner, for example specifying a number of reward points earned by downloading the selected content items. This CRM data will normally be written to the smart Flash card (step S59), but may additionally or alternatively be stored in the content access terminal or in a data store of the content access terminal owner so that the reward points are held by the distributor/retailer/cable TV operator. Finally, also at step S59, a complete record of details of the transactions between the smart Flash card and the content access terminal, the smart Flash card and the scheme owner, the smart Flash card and the e-payment system, and the content access terminal and the e-payment system and/or data supply computer is recorded on the smart Flash card to provide an audit trail. The system then returns to the menu display at step S42.

The add monetary value menu option provided by the menu operates in a similar manner to that described with regard to steps S15 and S16 of Figure 11a and steps S24

to S27 of Figure 11b. In embodiments of the system in which the smart Flash card operates either in a debit (pre-pay) or credit mode, operating mode data may be loaded from the card together with outlying CRM data at step S40. If the card is operating in a credit mode then, at step S41, the content access terminal reads content use data records from the card and proceeds correspondingly to steps S47 and S48 to determine the value of the content accessed and then proceeds according to steps S15 and S16 of Figure 11a and steps S24 to S27 of Figure 11b to retrieve payment for the accessed content from the card owner. Where enhanced access control features are provided, access control data read from the smart Flash card or entered into the content access terminal at step S31 is used, in step S44, to access the scheme owner content access webpage and, in some embodiments, to set up a secure connection between the content access terminal and scheme owner data supply computer at step S44.

Referring now to Figures 12d and 12e, these show steps in a process implemented on the scheme owner's data supply computer, for providing content data to a content access terminal and thence to a data carrier such as a smart Flash card. At step S60 the scheme owner's content access web page is requested by a content access terminal and transmitted to the requesting terminal. A search request for searching for a content data item is received, at step S61, from the content access terminal and at step S62 content distribution processor 134 of the content supply system searches content access and DRM data store 140 and transmits the search results to the content access terminal. The search results will normally comprise a content item identifier, a content item description, optionally a content item sample, and at least one content item price, for example, for a default payment option. The search results may comprise a set of content data items, either selected by type or artist or comprising some predetermined selection in a similar manner to a compilation of tracks on a CD.

At step S63 content item selection data identifying one or more content items is retrieved from the content access terminal and at step S64 content item purchase data for the selected content items is retrieved from content access and DRM data store 140. This purchase data will normally include, for each selected content item, one or more

prices and purchase options. Purchase option data may simply comprise one of a set of standard options, for example, "1" to purchase outright, "2" to rent for a period of time, "3" to rent for a number of plays, and "4" to rent with a final purchase option. The purchase option data may also indicate when a content item is available free.

At step S65 the content purchase data is transmitted to the content access terminal, and at step S66 payment record data, indicating a payment made from the smart Flash card to the scheme owner, purchase request data, card registration data and, optionally, access control data is received from the content access terminal. The payment record data confirms a payment for the requested data items, the purchase request data specifies the payment option selected for the selected content items, and the card registration data provides data for keeping records of the transaction and providing reward points; the access control data may be required for additional data security. At step S67 the payment record data, in the described embodiment of the system, is validated with an e-payment system such as E-payment system 121 of Figure 6. As illustrated in the flow chart, the data supply system computer checks with the e-payment system that a payment has in fact been made to the scheme owner. In other embodiments of the system, payment may be made directly to the scheme owner and either concurrently with the content access and download process, or at some later stage, payment data received from the smart Flash card may be verified with the e-payment system for reimbursement of the scheme owner.

At step S68, payment distribution data is read from the content access data store 140. This data will indicate how payment made by the card for the data is to be distributed among recipients. In one embodiment, recipients' payment fractions are specified in general terms in the content access data store, for example, copyright owner 0.90, scheme owner 0.01, retailer/distributor 0.02, publisher 0.02, creator 0.05. Identification of who is the relevant copyright owner is stored in the data store together with the content item identifier, but may be selected from more than one possible content providers for the data item, and identification of who is the relevant retailer/distributor may be determined from, for example, content access identity information received from

the content access terminal when the scheme owner content access web page is accessed at step S60. At step S69, payments are then distributed in accordance with the payment distribution data, either by direct distribution of value-bearing digital signatures to the relevant parties, or by issuing a payment distribution instruction to e-payment system 121. Preferably the data supply system stores records of individual card payments and, at intervals, combines the payment distribution data for a plurality of individual records to output payment data for distributing the total payment received by the data supply system from a batch of individual payments.

At step S70, content access rules for the purchased level of service are read from the content access data store. These rules could, for example, specify that only a predetermined number of accesses to the content are permitted, for example 10 plays. Alternatively, the rules could provide access for, say, one month from the download date. Other rules may provide unlimited plays but only on specified players, for example, set top boxes owned by a particular cable TV network (as determined by content access device identification data provided to a smart Flash card from a content access device). A content provider identification for the requested content data is also read from the content access data store at step S70 together with CRM data for issuing reward points.

At step S71, content access rules for the requested content data items are retrieved from data store 140 and transmitted to the content access terminal. Then, at step S72, DRM processor 130 of the data supply system transmits a transaction request and authentication data to the content provider identified in step S70. This request identifies the scheme owner data supply system to the content provider in a secure manner, either by means of physical security, such as a dedicated connection from the scheme owner data supply system to the content provider, or by means of an electronically secure connection such as an encryption connection. Then, at step S73, the content access web server 124 receives protected content from the content provider, comprising the data items requested by the content access terminal, and transmits this protected content to the content access terminal. The content is preferably protected by data encryption but

may be protected in other ways, for example, by digital watermarking or simply by the large number of other transactions taking place at any one time over the internet. The data supply system computer, at this point, essentially acts as a transparent data forwarder, forwarding data from the content provider to the content access terminal, which itself is preferably effectively transparent, using data exchange interface 200c to transmit the protected content data directly to the smart Flash card. As described with regard to Figure 12d, the content download protocol includes error protection and transmission retry protocols to ensure substantially error free data transmission.

Once content has been downloaded to the content access terminal (and, hence, to the smart Flash card) at step S74 a record of the purchase data and content accessed is written to payment record data store 136, to provide an audit trail. Then, at step S75, updated CRM data is written to the content access data store 140, using rules stored in the content access data store, in conjunction with a record of the downloaded data items, to calculate the CRM data (i.e. reward points). The updated CRM data is then also transmitted to the content access terminal, where it can be forwarded to the smart Flash card. Then, at step S76, the process ends.

Referring now to Figure 13, this shows a flow chart for user access of stored data on a smart Flash card using a data access device such as the MP3 player of Figure 1. At step S77 the smart Flash card is inserted into the player and, at step S78, the user enters a password into the player, which is transmitted to the smart Flash card for validation (this step is optional). If access to stored data on the card is permitted, the process proceeds to step S79 where an index of content data items stored on the card is loaded from the card and displayed together with a menu. The menu provides options including access content, check value (stored on the card), check CRM data (such as reward points) stored on the card, and play options (such as no video, repeat play, random play, and the like). If the user wishes to access content data items stored on the smart Flash card, a user selection of such items is entered into the player at step S80, for example using cursor keys or a pointer; additionally or alternatively a default play option may be provided to, for example, play the most recently downloaded data.

At step S81 content use status data for the selected content items is loaded from the smart Flash card together with associated content use rules. Then, at step S82, the use rules and present use status for each selected content item are compared and the result is displayed together with a content play menu. The content play menu may comprise a simple list of the selected content items with items not available for access highlighted in, for example, red. Alternatively, more detailed content access permission data may be displayed such as the purchased contents use for a content data item, the actual use of the data item made so far, and the available remaining use. Then, at step S83, the layer determines whether content use is permitted. If use is not permitted, the process returns to step S79 to re-display the menu; if content use is permitted the system proceeds to step S84.

At step S84 the selected content data items whose use is permitted are retrieved sequentially from the card, decoded as necessary, and the decoded audio and/or video data is made available to the user, for example, by providing audio output at a headphone socket on the player and displaying video output on the player display. Preferably, the player also retrieves supplementary data stored in association with a content data item, such as advertising data, or for a web-enabled player, hot links to web sites for sale of goods or services, particularly those related to the accessed content data item or those identified to appeal to users accessing the data item (such as pop group merchandising or Harley Davidson (trade mark) motor bikes for rock music/video).

Preferably, the player is provided with "pause" and "continue" functions and corresponding user controls. When "pause" is selected the process passes to step S85 and writes a record to the smart Flash card comprising data specifying how much use has been made of the accessed content data item. In the case of music or video data, this may comprise start and end time markers or simply a play duration time (the start time being predetermined, for example at the start of the data item). In the case of a game the partial use data may comprise an elapsed play time or a number of lives left. In the case of a data item providing a service such as access to stock and share prices, or weather

information, or a share dealing service, the partial use information may comprise a status record indicating the status of an interrupted transaction. When the "continue" function is selected on the player the process returns to step S84.

To allow for the smart Flash card being removed from the player between pause and continue events, a check may be made at step S78, by reading a partial use status data from the card, to determine whether a content data item was left in a pause state when the card was lost used. If such a paused state is determined to exist for a content data item, the process may then jump directly to step S85 to allow a user to resume or continue with the content data item and proceed directly to step S84.

Once play is complete the process moves to step S85 where updated content use data is written to the smart Flash card. This updated use data provides a record of the use of a content made in step S84. This record can then be used in steps S81 to S83 to determine, on a subsequent occasion, whether further use of the content data item is permitted. Finally, at step S86, customer reward management reward rules are loaded from the smart Flash card together with CRM data stored on the card. The CRM data is then updated, using the CRM reward rules, to reflect the use of content data items made in step S84 and the updated data is written back to the smart Flash card.

In one embodiment the CRM reward rules are determined by the content access terminal owner (retailer/distributor/cable or mobile network operator) and are written onto the card when registering the card. The updated CRM data may then be accessed by a content access terminal for spending or other use when the smart Flash card is next inserted into a content access terminal. Once the CRM data has been updated, the process returns to step S79 to display the content index and menu.

The specific embodiments of the invention described above use communication over the internet and web-based technology but this is not essential, and the invention may be implemented using any electronic communications network, such as a wide area network, local area network, wireless network, or conventional land line network.

Likewise, the invention is applicable to the Internet, intranets, extranets, and other internet protocol networks.

The skilled person will understand that many variants to the system are possible and the invention is not limited to the described embodiments but encompasses modifications which lie within the spirit and scope of the present invention.



Further aspects of the invention are set out in the following clauses:

1. A mobile data retrieval device comprising:
  - a removable data storage means;
  - data access means, to access downloaded data on the data storage means;
  - storage interface means adapted to couple the data storage and data access means; and
  - data output means to provide the downloaded data, in a useful form, to a user of the device;wherein the data storage means further comprises payment validation means to validate payment for the downloaded data.
2. A mobile data retrieval device as in clause 1 wherein the data storage means receives power from the retrieval device when connected to the device and retains storage by the downloaded data when unpowered.
3. A mobile data retrieval device as in clause 1 or 2 wherein the data storage means comprises external data interface means to receive data downloaded from an external source onto the card for storage and wherein the payment validation means comprises means to validate payment to the external source.
4. A mobile data retrieval device according to any preceding clause wherein the payment validation means comprises memory means to store transaction value information on a cash value of transactions validatable by the data storage means.
5. A mobile data retrieval device according to any preceding clause wherein the payment validation means comprises memory means to store information to identify a payer for the downloaded data.

6. A mobile data retrieval device according to any preceding clause wherein one of the data storage means and the retrieval device further comprises data description means to at least partially decrypt downloaded data.
7. A mobile data retrieval device according to any preceding clause wherein one of the data storage means and the retrieval device comprises access control means to prevent unauthorised access to the downloaded data.
8. A mobile data retrieval device according to clause 7 wherein the access control means is responsive to the payment validation means.
9. A mobile data retrieval device according to any one of clauses 3 to 8 wherein the payment validation means comprises a payment validation means interface operable simultaneously with the external data interface means.
10. A mobile data retrieval device according to any preceding clause wherein the data storage means comprises an electronic memory card or smart card.
11. A mobile data retrieval device according to clause 10 having a housing with a slot therein to receive the data storage means.
12. A mobile data retrieval device according to clause 11 further comprising local storage means and means to copy data from the data storage means into the local storage means.
13. A mobile data retrieval device according to clause 11 or 12 wherein the retrieval device is portable and, in two directions, is not substantially larger than the data storage means.

14. A mobile data retrieval device according to any preceding clause wherein the storage interface means is adapted for repeated removal and reconnection of the data storage means to the retrieval device.

15. A mobile data retrieval device according to any preceding clause further comprising display means to display information derived from the downloaded data to the user.

16. A mobile data retrieval device according to any preceding clause further comprising audio output means to provide an audio output corresponding to the downloaded data to the user.

17. A mobile data retrieval device according to any preceding clause comprising a first set of contacts for the storage interface means and a second set of contacts for interfacing to the payment validation means.

18. A data providing system comprising a mobile data retrieval device as in any preceding clause, and  
a data access terminal to interface with the data storage means to download data and to co-operate with the payment validation means to validate payment for the downloaded data.

19. A data providing system as in clause 18 wherein the data access terminal is couplable to the internet and co-operates with the payment validation means to validate payment with a payment validation authority and is operable to download data to the data storage means from a data supplier on the internet.

20. A data providing system as in clause 19 wherein the data access terminal operates through a data access service provider, the data access service provider being configured to communicate with the payment validation authority and to control access of data access terminal to data from the data supplier.

21. A data storage means for use with the device or system of any preceding clause.
22. A data storage means comprising an external data interface means to receive data downloaded from an external source onto the card for storage; and payment validation means comprising means to validate payment to the external source, and/or to a payment validation authority.
23. A data storage means as in clause 22 further comprising data decryption means to at least partially decrypt the downloaded data.
24. A data storage means as in clause 22 or 23 further comprising access control means to prevent unauthorised access to the downloaded data.
25. A data storage means as in clause 24 wherein the access control means is responsive to the payment validation means.
26. A data storage means according to any one of clauses 22 to 25 wherein the payment validation means comprises a payment validation means interface operable simultaneously with the external data interface means.
27. A data storage means according to any one of clauses 22 to 26 wherein the data storage means comprises an electronic memory card or smart card.

**CLAIMS:**

1. A method of providing portable data comprising:  
providing a portable data storage device comprising downloaded data storage means and payment validation means;  
providing a terminal for internet access;  
coupling the portable data storage device to the terminal;  
reading payment information from the payment validation means using the terminal;  
validating the payment information; and  
downloading data into the portable storage device from a data supplier.
2. A method as claimed in claim 1 further comprising  
writing updated payment information into the payment validation means.
3. A method as claimed in claim 1 or 2 further comprising communicating a result of the payment information validating to the data supplier.
4. A method as claimed in any one of claims 1 to 3 further comprising controlling access by the terminal to data from the data supplier using a control data processing system coupled to the internet.
5. A method as claimed in claim 4 wherein the control data processing system performs said validating of the payment information.
6. A method as claimed according to any one of claims 1 to 5 wherein said coupling is performed by a mobile data retrieval device comprising:  
a removable data storage means;  
data access means, to access downloaded data on the data storage means;  
storage interface means adapted to couple the data storage and data access means; and

data output means to output data derived from the downloaded data, to a user of the device.

7. A method as claimed in claims 1 to 6 further comprising writing into the data storage device data relating to past use made of the downloaded data including data identifying downloaded data items; and/or data identifying data suppliers used; and/or data characterising a user spending pattern.
8. A method as claimed in claims 1 to 7 wherein said portable data storage device comprises an electronic memory card or smart card.
9. A method as claimed in any one of claims 1 to 8 wherein the downloaded data comprises compressed audio and/or video data.
10. A portable data carrier comprising:
  - an interface for reading and writing data from and to the carrier;
  - non-volatile data memory, coupled to the interface, for storing data on the carrier;
  - non-volatile payment data memory, coupled to the interface, for providing payment data to an external device.
11. A portable data carrier as claimed in claim 10, further comprising a program store storing code implementable by a processor; and
  - a processor, coupled to the content data memory, the payment data memory, the interface and to the program store for implementing code in the program store,
  - wherein the code comprises code to output payment data from the payment data memory to the interface and code to provide external access to the data memory.
12. A portable data carrier as claimed in claim 11, further comprising non-volatile use record memory, coupled to the processor, for storing a record of access made to the

data memory and code to update the use record memory in response to external access made to the data memory.

13. A portable data carrier as claimed in claim 12, further comprising non-volatile use rule memory, coupled to the processor for storing data use rules, and wherein the code further comprises code for storing at least one data item in the data memory and at least one corresponding use rule in the use rule memory and code to provide external access to the data item in accordance with the use rule.

14. A portable data carrier as claimed in claim 11, 12 or 13, further comprising a non-volatile access control memory coupled to the processor, for storing access control data and wherein said code to provide external access to the data memory includes code to receive access request data from the interface, code to determine access permission using the stored access control data and code to provide external access to the data memory in response to the result of the determination.

15. A portable data carrier as claimed in claim 14, further comprising non-volatile access record data memory, coupled to the processor, for storing a record of requests for external access to the data memory and wherein said code further comprises code to compare said access record data and said access request data and to erase stored content data in response to a result of said comparison.

16. A portable data carrier as claimed in any one of claims 11 to 15, configured for storing supplementary data in said data memory and further comprising code to output the supplementary data from the interface in addition to the stored data, in response to an external request to read the data memory.

17. A portable data carrier as claimed in any one of claims 11 to 16 further comprising data synthesis code to receive a first portion of data from the interface and to combine the first portion with a second portion of data stored in the data memory and to store the result in the data memory.

18. A portable data carrier as claimed in any one of claims 10 to 17, further comprising non-volatile communications parameter memory for storing data for accessing a communications network to receive data from the communications network for storage in the data memory.

19. A portable data carrier as claimed in any one of claims 10 to 18, wherein the data memory is partitioned for access on a block-by-block basis, each block comprising a plurality of data bytes read or written as a set.

20. A portable data carrier as claimed in any one of claims 10 to 19 wherein said data memory has a capacity of greater than 1 MByte, more preferably > 100 MBytes, and most preferably > 1 GByte.

21. A portable data carrier as claimed in any one of claims 10 to 20 substantially configured as an IC card or smart card.

22. A method of controlling access to data on a data carrier, the data carrier comprising non-volatile data memory and non-volatile parameter memory storing use status data and use rules, the method comprising:  
receiving a data access request;  
reading the use status data and use rules from memory; and  
evaluating the use status data using the use rules to determine whether access to the stored data is permitted.

23. A method as claimed in claim 22 wherein said parameter memory further stores payment data and further comprising selecting a said use rule dependent upon said payment data.

24. A computer system for providing data to a data requester, the system comprising:



a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and a pointer to a data provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester;

code to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code responsive to the request and to the received payment data, to read data for the requested data item from a content provider; and

code to transmit the read data to the requester over the communications interface.

25. A computer system as claimed in claim 24, wherein said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

26. A computer system as claimed in claim 24 or 25, wherein said data access data store further comprises data item access rule data for output to the requester with said data item.

27. A computer system as claimed in claim 26, further comprising code to select access rule data for output with a data item in response to said payment data.

28. A computer system as claimed in claim 27, wherein said data access data store further comprises requester reward data associated with a said data item, and said code further comprises code to update said reward data in response to said payment data.

29. A computer system as claimed in any one of claims 24 to 28, further comprising an access control data store coupled to said processor for storing access control data comprising a requester identifier, corresponding requester system access data and payment system data for identifying a payment system for use by the requester.

30. A computer system as claimed in any one of claims 24 to 29, further comprising content synthesis code to generate substantially complete item data from partial item data provided from two or more sources.

31. A method of providing data to a data requester comprising:  
receiving a request for a data item from the requester;  
receiving payment data from the requester relating to payment for the requested data;  
reading the requested data from a content provider responsive to the received payment data; and  
transmitting the read data to the requester.

32. A method of providing data to a data requester as claimed in claim 31 further comprising:  
reading payment distribution information from a data store; and  
outputting payment data to a payment system for distributing the payment for the requested data.

33. A method of providing data to a data requester as claimed in claim 31 or 32 further comprising:  
transmitting data access rule data to requester with the read data.

34. A method of providing data to a data requester as claimed in claim 33 further comprising:  
selecting said access rule data dependent upon said payment data.

35. A data access terminal for retrieving data from a data supplier and providing the retrieved data to a data carrier, the terminal comprising:
- a first interface for communicating with the data supplier;
  - a data carrier interface for interfacing with the data carrier;
  - a program store storing code implementable by a processor; and
  - a processor, coupled to the first interface, the data carrier interface and to the program store for implementing the stored code, the code comprising:
    - code to read payment data from the data carrier and to forward the payment data to a payment validation system;
    - code to receive payment validation data from the payment validation system;
    - code responsive to the payment validation data to retrieve data from the data supplier and to write the retrieved data into the data carrier.
36. A data access terminal as claimed in claim 35 further comprising code to transmit at least a portion of the payment validation data to the data supplier or to a destination received from the data supplier.
37. A data access terminal as claimed in claim 35 or 36 further comprising code to retrieve from the data supplier and output to a user stored data identifier data and associated value data and use rule data for a data item available from the data supplier.
38. A data access terminal as claimed in claim 37 further comprising code to write use rule data for a data item into the data carrier with the associated data item.
39. A data access terminal as claimed in claim 37 or 38 further comprising code to read a stored value from the data carrier, code to compare said stored value with said value data; and code to provide a modified output to a user of one or more of said stored data identifier data, said value data and said use rule data, in response to a result of the comparison.

40. A data access terminal according to any one of claims 35 to 39 further comprising code for user input of access control data, code to output the access control data to the data carrier, code to receive access permission data from the card, and code to output data to the user in response to the received access permission data.
41. A data access terminal as claimed in claim 40 further comprising code to output a data erasure warning in response to the received access permission data.
42. A data access terminal according to any one of claims 35 to 41 further comprising code to read reward data from the data carrier and to write modified reward data to the data carrier in response to said retrieval of data from the data supplier.
43. A data access terminal according to any one of claims 35 to 42 further comprising:  
code to read identity data from the data carrier;  
code to transmit the identity data to the data supplier;  
code to receive user characterising data from the data supplier;  
code to retrieve supplementary data in response to said characterising data; and  
code to output the supplementary data.
44. A data access terminal according to any one of claims 35 to 43 further comprising a cash input device coupled to the processor, to provide cash input value data; and code to update payment data in the data carrier, in accordance with the cash input value data.
45. A data access terminal according to any one of claims 35 to 44 integrated with a mobile communication device, a personal computer, an audio/video player, and/or a cable or satellite television interface device.
46. A method of providing data from a data supplier to a data carrier, the method comprising:

reading payment data from the data carrier;  
forwarding the payment data to a payment validation system;  
retrieving data from the data supplier; and  
writing the retrieved data into the data carrier.

47. A method of providing data from a data supplier according to claim 46 further comprising:  
receiving payment validation data from the payment validation system; and  
transmitting at least a portion of the payment validation data to the data supplier.
48. A method of providing data as claimed in claim 47, wherein the payment validation system comprises a payment processor at the data supplier.
49. A method of providing data as claimed in claim 46, 47 or 48, further comprising:  
retrieving from the data supplier a stored data item identifier and associated value data and use rule data; and  
writing use rule data for the data item into the data carrier.
50. A method of providing data as claimed in claim 48 or 49, further comprising:  
reading a stored value from the data carrier;  
comparing the stored value with said value data; and  
outputting to a user information indicating the result of said comparing.
51. A data access device for retrieving stored data from a data carrier, the device comprising:  
a user interface;  
a data carrier interface;  
a program store storing code implementable by a processor; and  
a processor coupled to the user interface, to the data carrier interface and to the program store for implementing the stored code, the code comprising:

code to retrieve use status data indicating a use status of data stored on the carrier, and use rules data indicating permissible use of data stored on the carrier;

code to evaluate the use status data using the use rules data to determine whether access is permitted to the stored data; and

code to access the stored data when access is permitted.

52. A data access device according to claim 51, further comprising code to write updated use status data to the carrier after user access to the stored data.

53. A data access device as claimed in claim 51 or 52, further comprising user access control code to input user access data, to transmit the user access data to the carrier, and to receive from the carrier user access permission data.

54. A data access device according to claim 53, further comprising code to select the use status and use rules data using the user access data.

55. A data access device as claimed in claim 53 or 54, further comprising code to retrieve and output supplementary data to the user.

56. A data access device according to any one of claims 51 to 55 wherein said use rules permit partial use of a data item stored on the carrier and further comprising code to write partial use status data to the data carrier when only part of a stored data item has been accessed.

57. A data access device according to any one of claims 51 to 56 wherein the device is portable and the data carrier interface is configured for interfacing with a removable data carrier.

58. A data access device according to claim 57 configured to interface with the data carrier of any one of claims 10 to 21.

59. A method of controlling access to data from a data carrier, comprising:  
retrieving use status data from the data carrier indicating past use of the stored data;  
retrieving use rules from the data carrier;  
evaluating the use status data using the use rules to determine whether access to data stored on the carrier is permitted; and  
permitting access to the data on the data carrier dependent on the result of said evaluating.
60. A method of controlling access according to claim 59, further comprising:  
writing updated use status data to the carrier after an access attempt.
61. A method of controlling access according to claim 60, wherein said use rules permit partial access to a data item and wherein said writing writes a record of what part of the data item has been accessed when only part of the data item has been accessed.
62. A method of controlling access according to any one of claims 59 to 61, further comprising:  
inputting a user access data;  
selecting the use rules dependent upon the user access data.
63. A data access system comprising a data supply computer system for forwarding data from a data provider to a data access terminal; a electronic payment system for confirming an electronic payment; a data access terminal for communicating with the data supply system to write data from the data supply system onto a data carrier; and a data carrier for storing data from the data supply system and payment data; wherein data is forwarded from the data provider to the data carrier on validation of payment data provided from the data carrier to the electronic payment system.
64. A data access system according to claim 63 further comprising a payment distribution store and wherein the electronic payment system makes payments according

to data in the payment distribution store associated with the forwarded data on confirmation of the payment and/or provision of the forwarded data to the card.

65. A data access system according to claim 63 or 64 further comprising a data use rule data store and wherein data use rule data is provided to the data carrier with the forwarded data for controlling user access to the forwarded data.

66. A data access system according to claim 65 wherein the data use rule data is selected dependent upon the payment data.

67. A portable data carrier comprising:  
an interface for sending and receiving data from and to the carrier;  
non-volatile data memory, coupled to the interface, for storing data on the carrier; and  
a digital rights management processor for controlling access to the stored data.

68. A portable data carrier comprising:  
an interface for sending and receiving data from and to the carrier;  
non-volatile data memory, coupled to the interface, for storing data on the carrier; and  
an access control processor;  
wherein the data memory is partitioned as data blocks and the access control processor controls external access to the data blocks.

69. A computer system for providing data to a data requester, the system comprising:  
a communication interface;  
a data access data store for storing records of data items available from the system, each record comprising a data item description and a resource locator a data provider for the data item;  
a program store storing code implementable by a processor;



a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code, responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and

further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

70. A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and location data identifying an electronic address for a provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

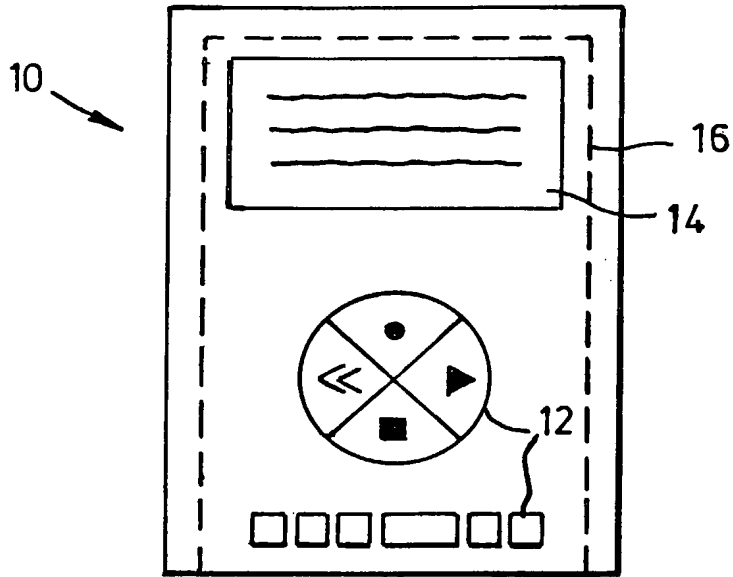
code responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises data item access rule data for output to the requester with a said data item; and

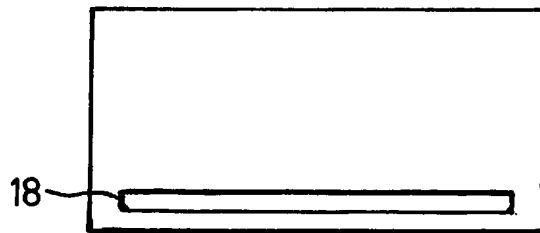
further comprising code to select access rule data for output with a data item in response to said payment data.

71. A method of providing data to a data requester comprising:  
receiving a request for a data item from the requester;  
receiving payment data from the requester relating to payment for the requested data;  
transmitting the requested data to the requester;  
reading payment distribution information from a data store; and  
outputting payment data to a payment system for distributing the payment for the requested data.
72. A method of providing data to a data requester comprising:  
receiving a request for a data item from the requester;  
receiving payment data from the requester relating to payment for the requested data;  
transmitting the requested data to the requester; and  
transmitting data access rule data to requester with the read data.
73. A computer program to, when running, carry out the method of any preceding method claim.
74. A computer readable medium carrying the computer program of claim 73.

1/17  
Fig. 1  
A



B



C

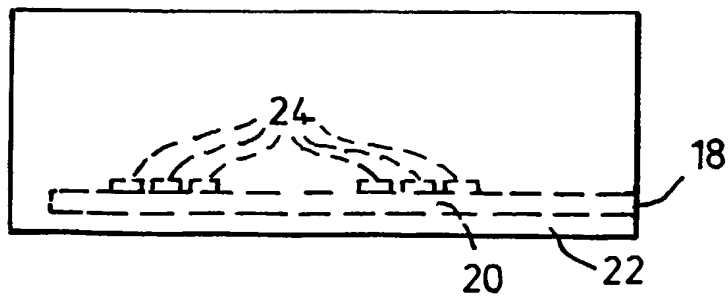


Fig. 2

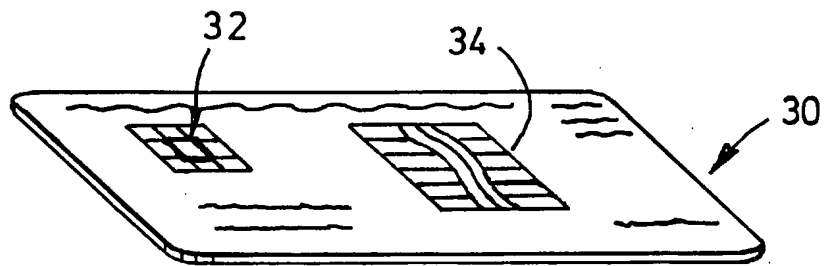
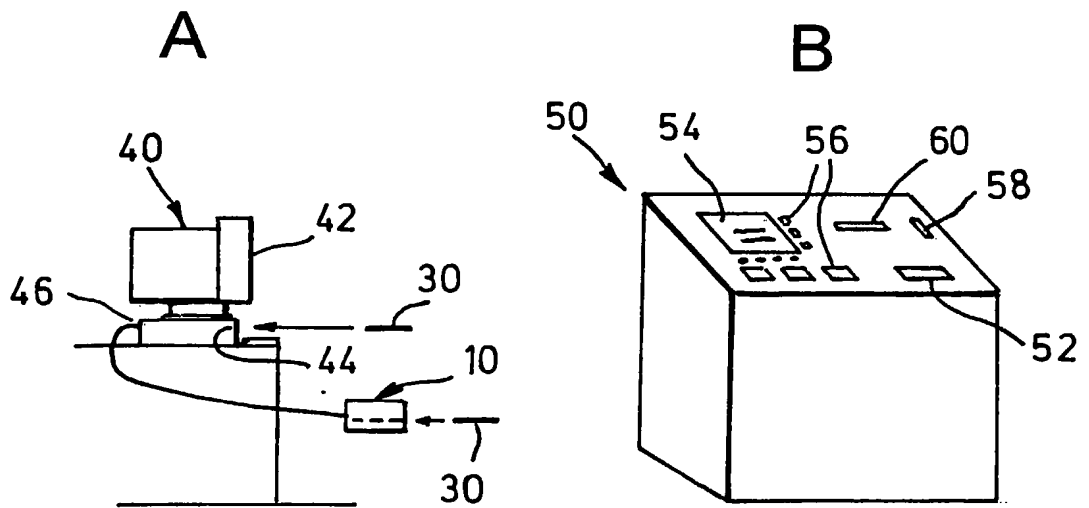


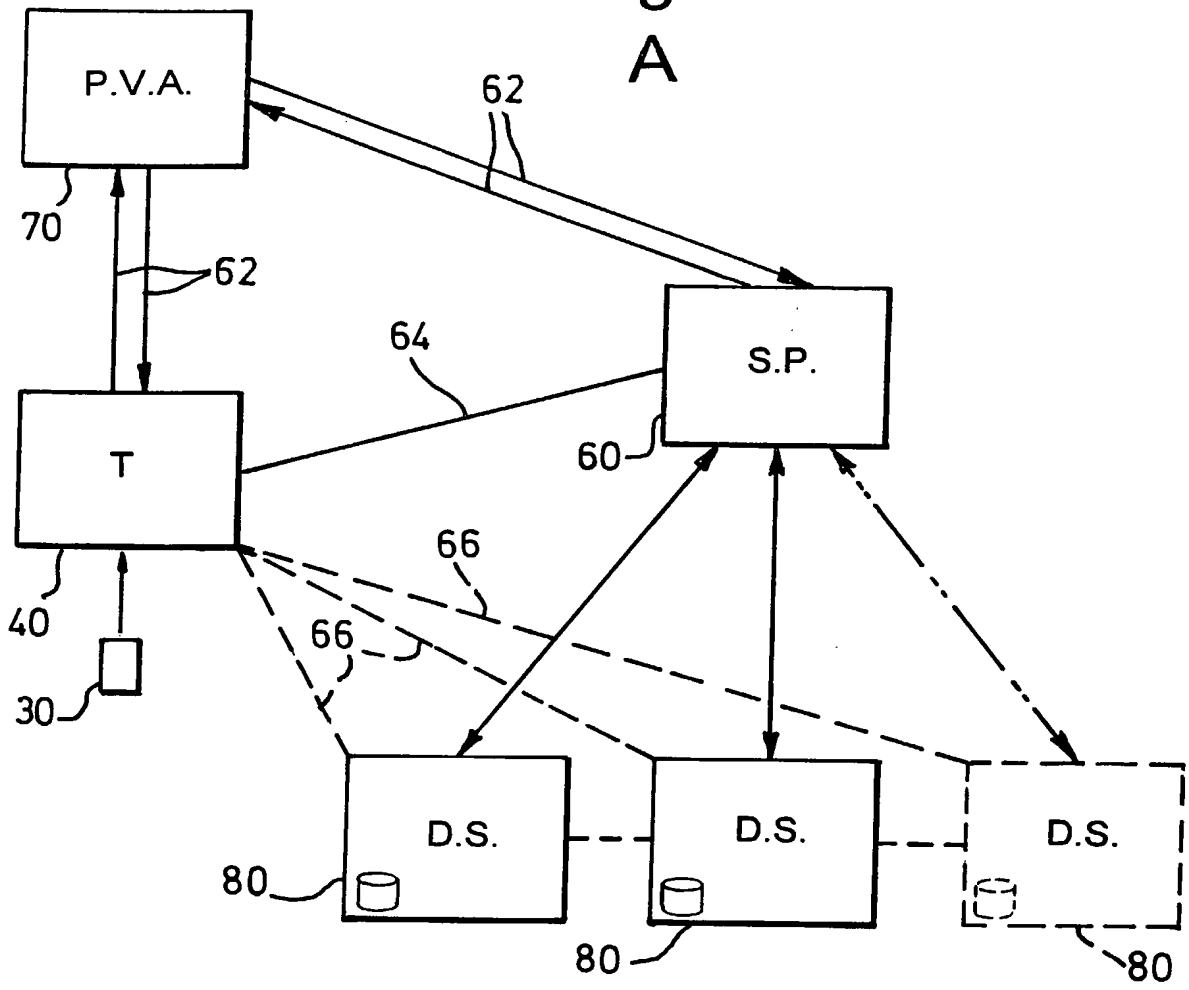
Fig. 3



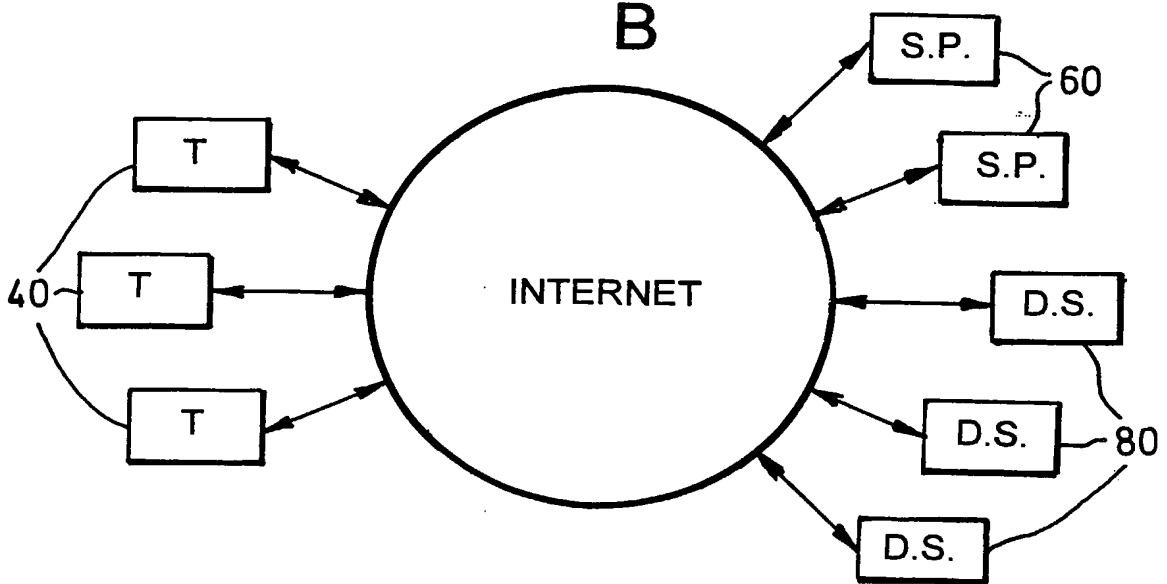
3/17

Fig. 4

A



B



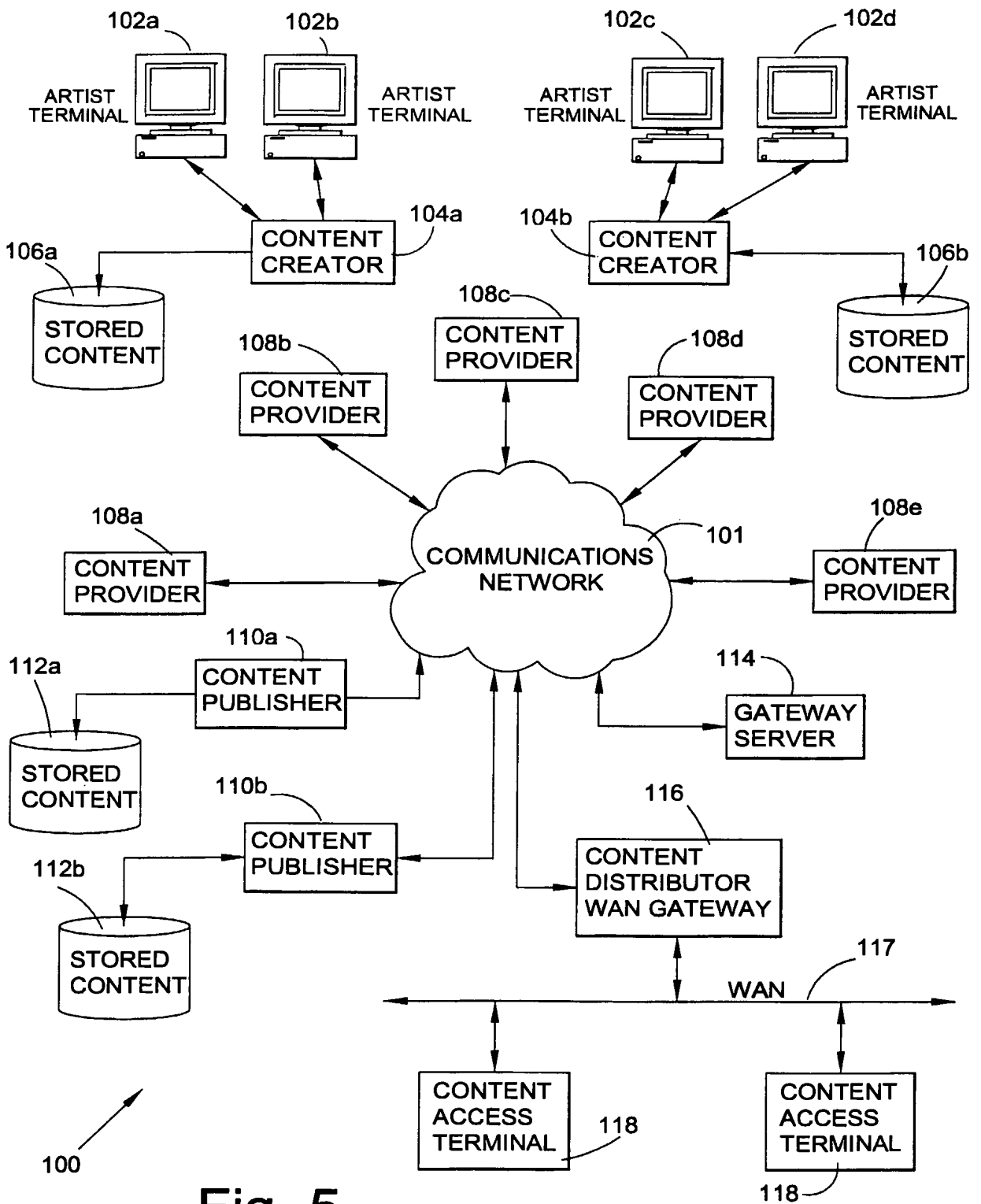


Fig. 5

5/17

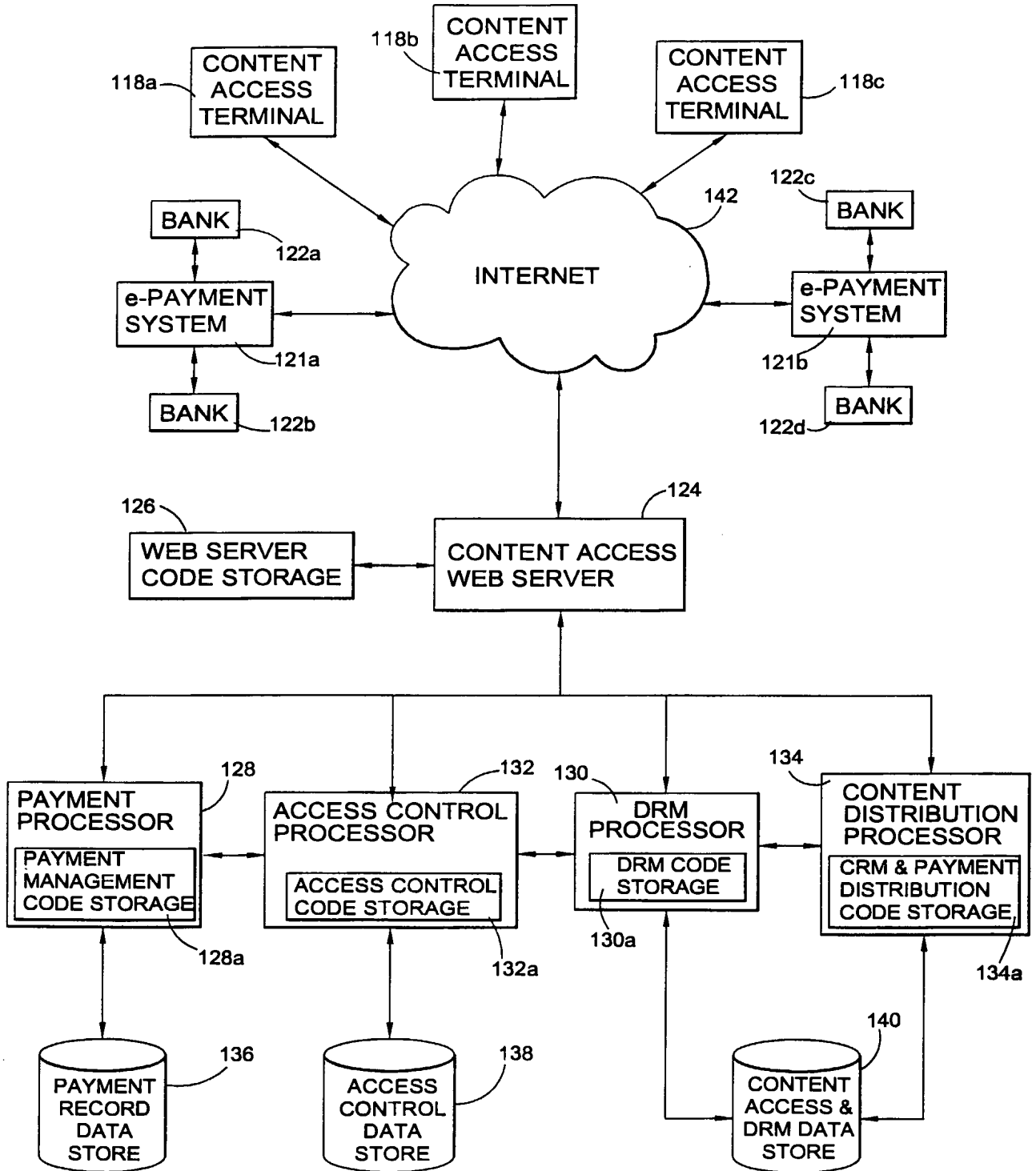


Fig.6

120

6/17

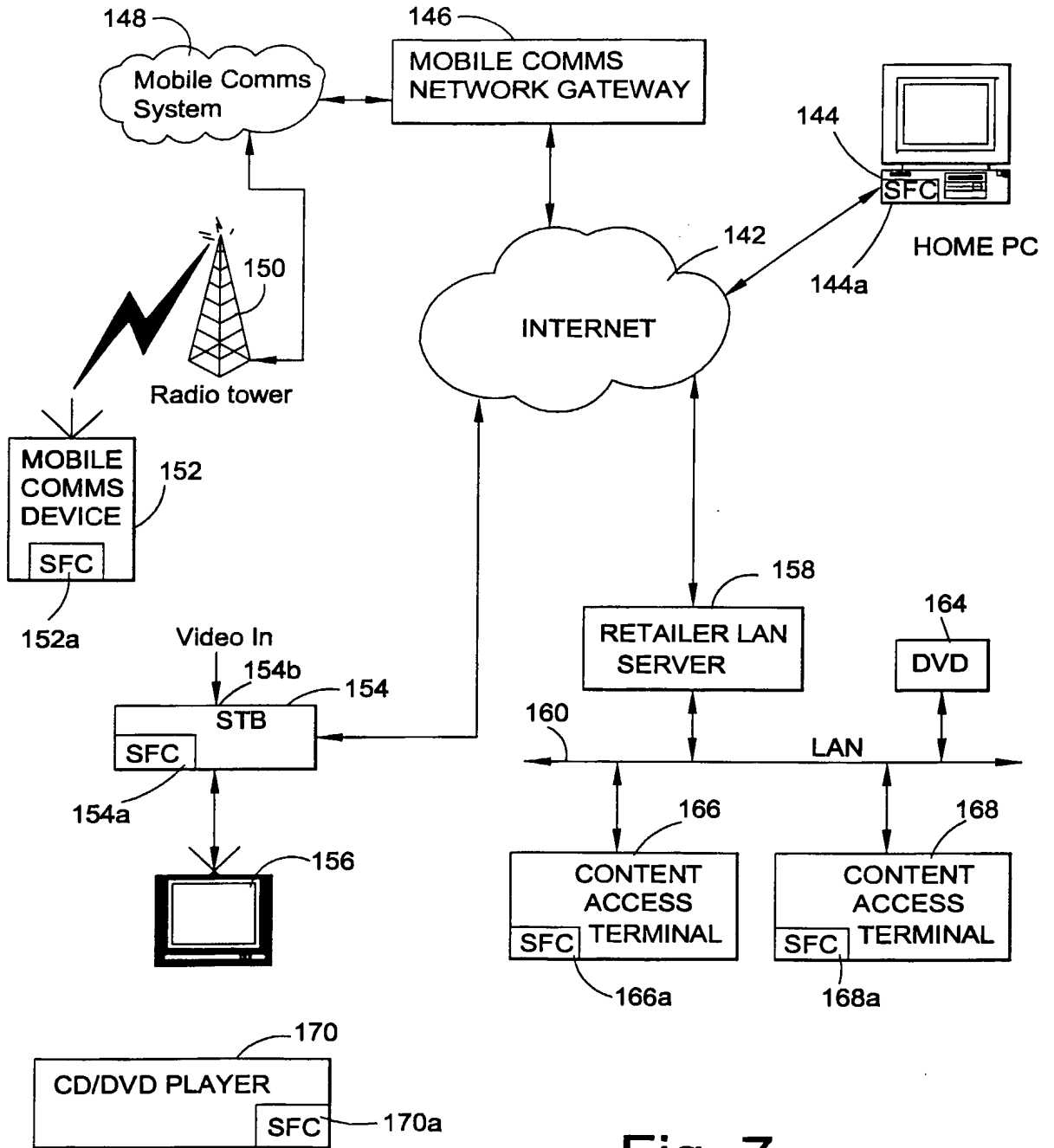


Fig. 7



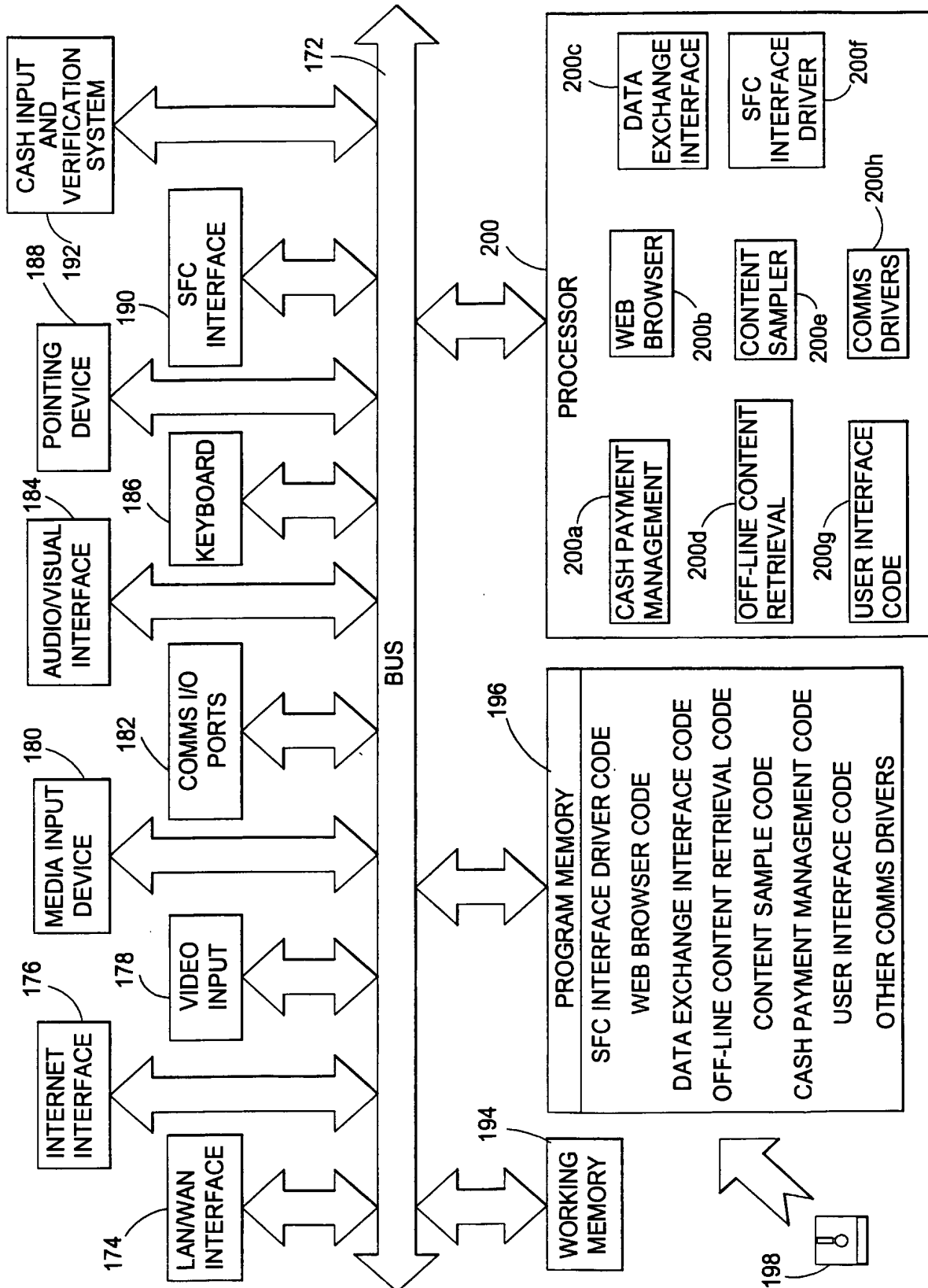


Fig. 8

8/17

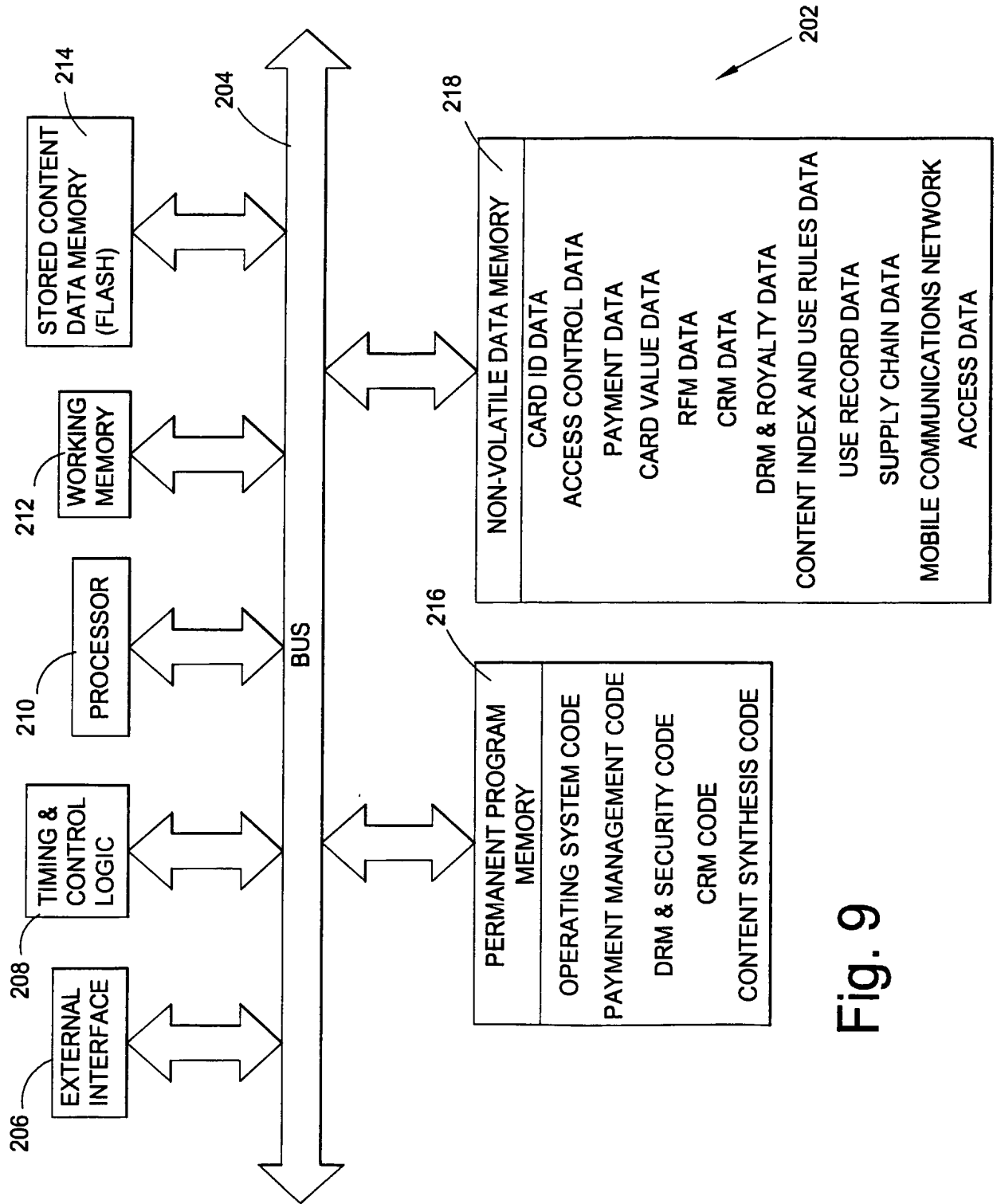


Fig. 9

9/17

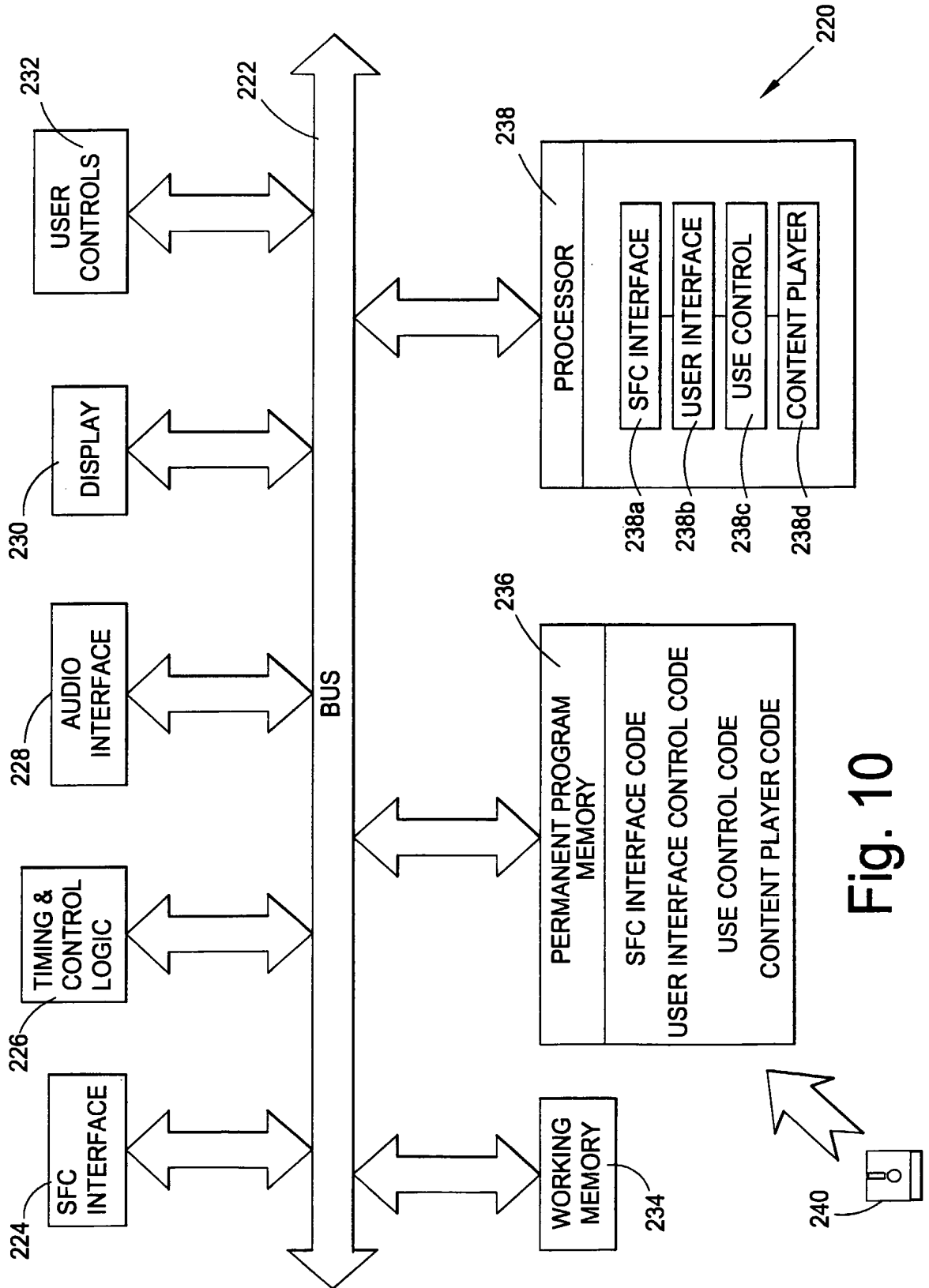


Fig. 10

10/17

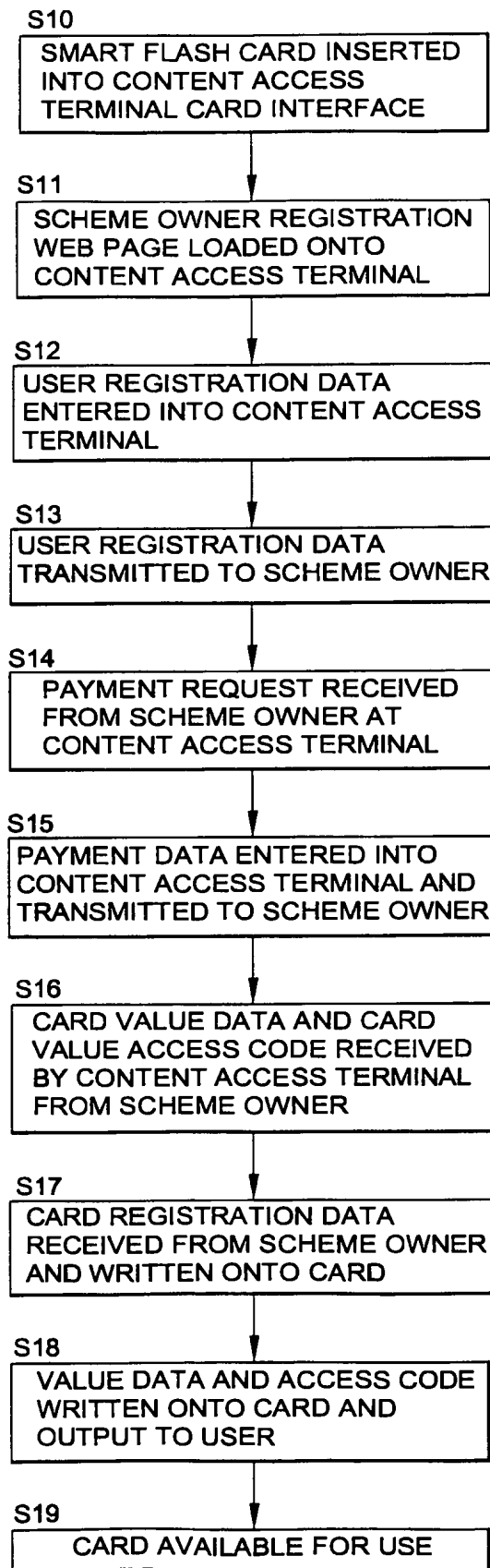


Fig11a

11/17

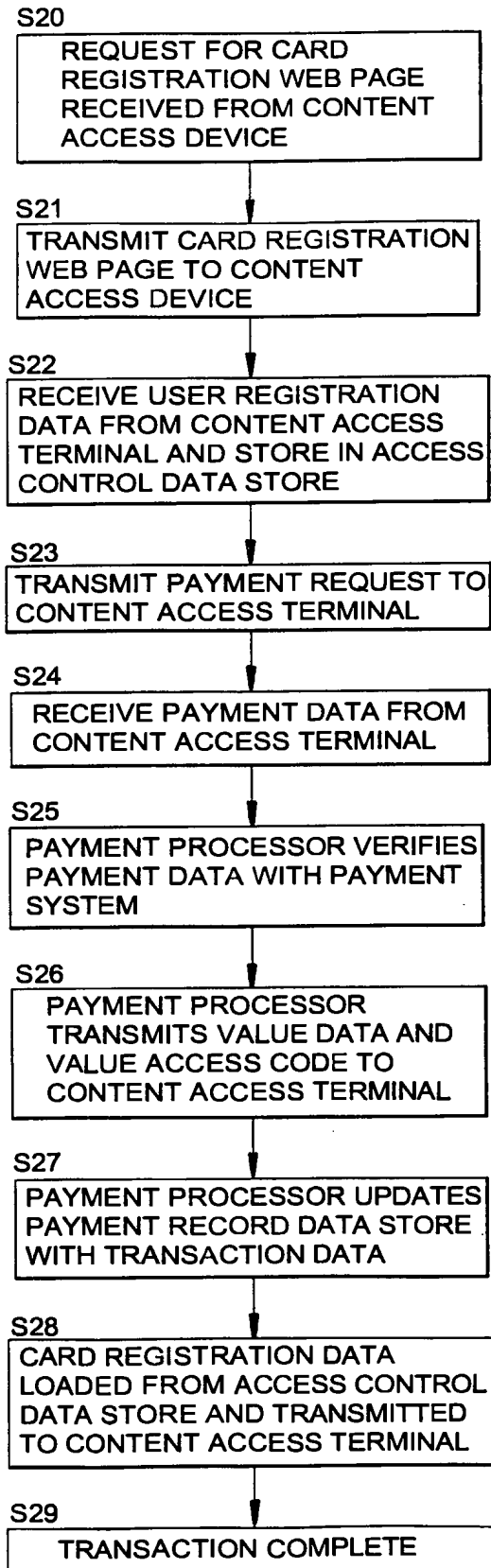


Fig.11b

12/17

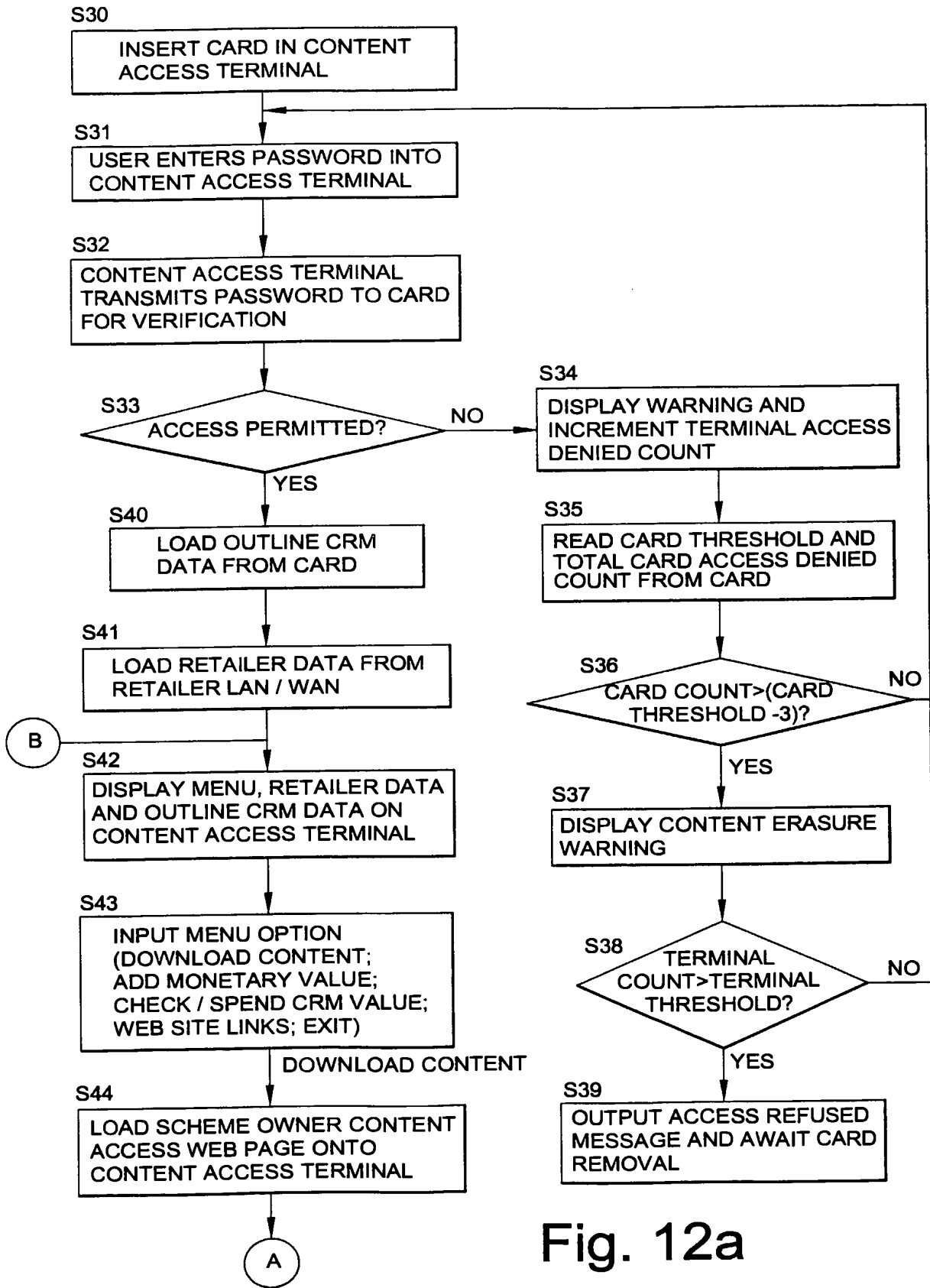


Fig. 12a

13/17

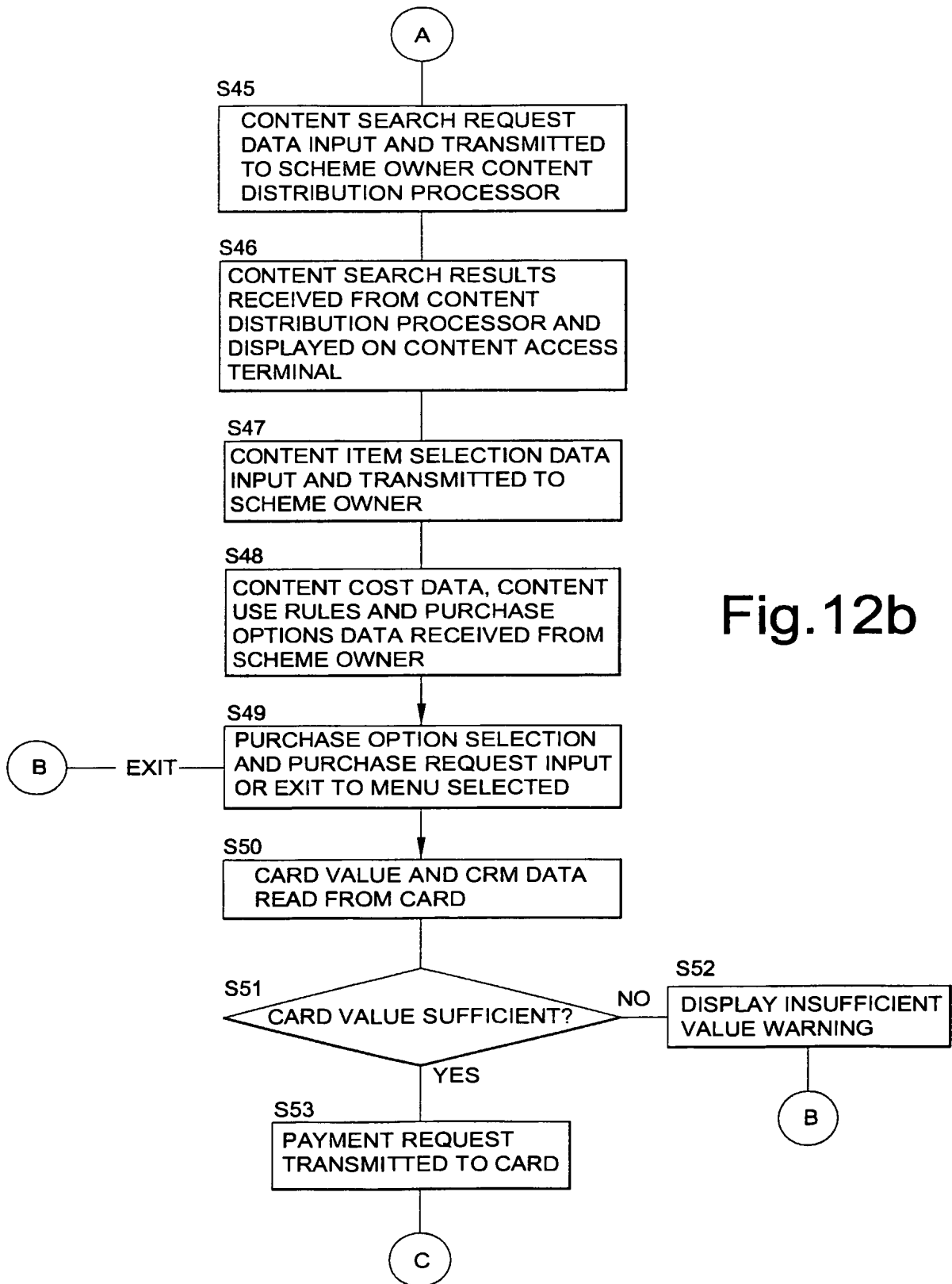


Fig.12b

14/17

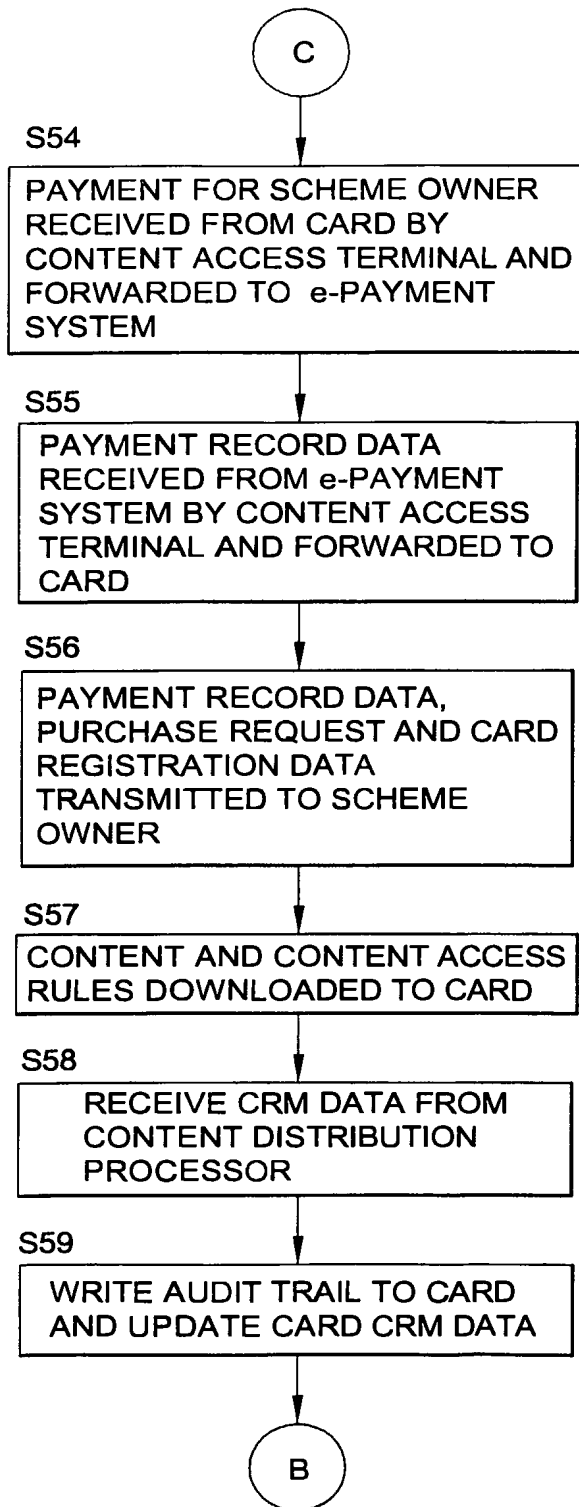


Fig.12c



15/17

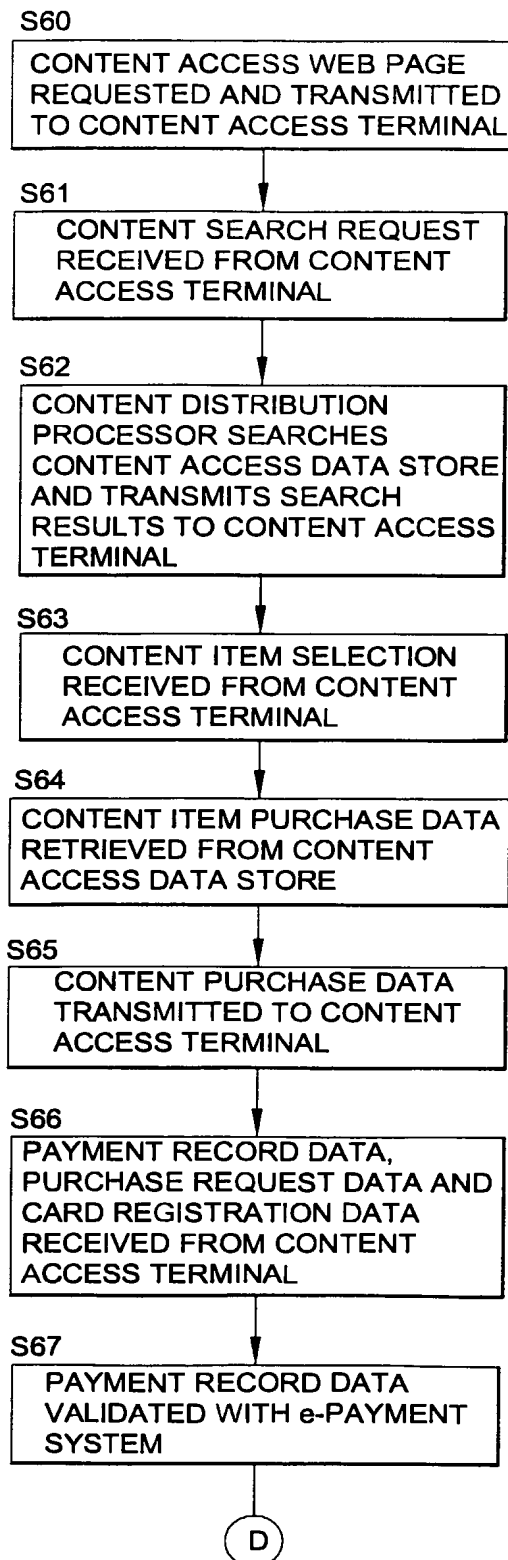


Fig. 12d

16/17

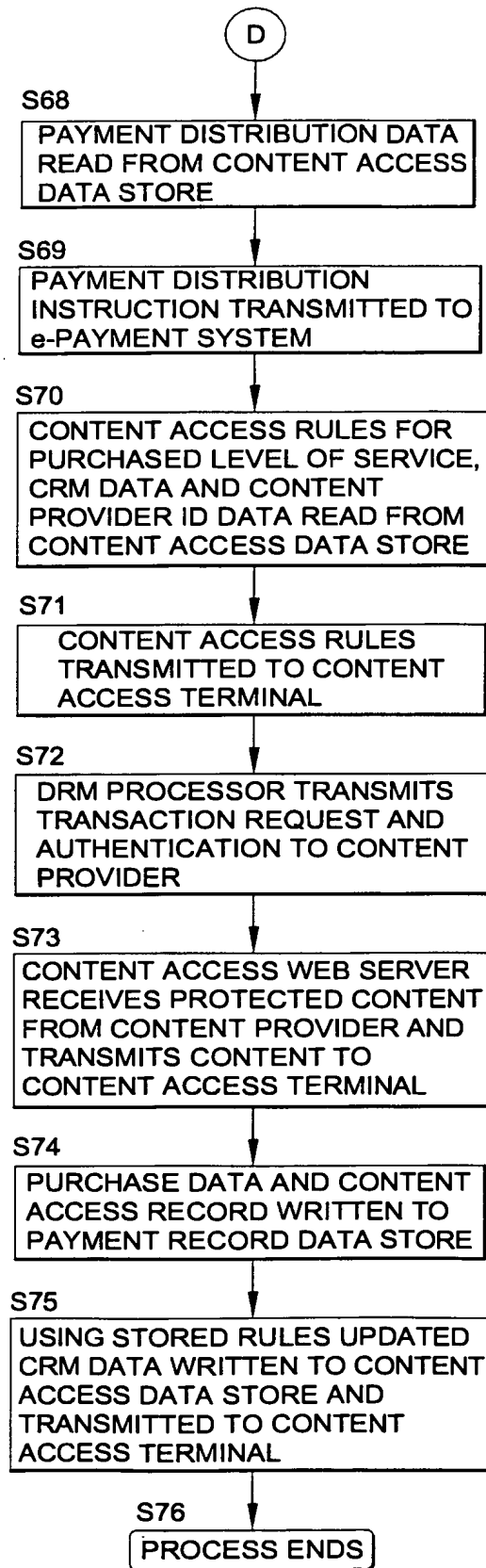


Fig. 12e

17/17

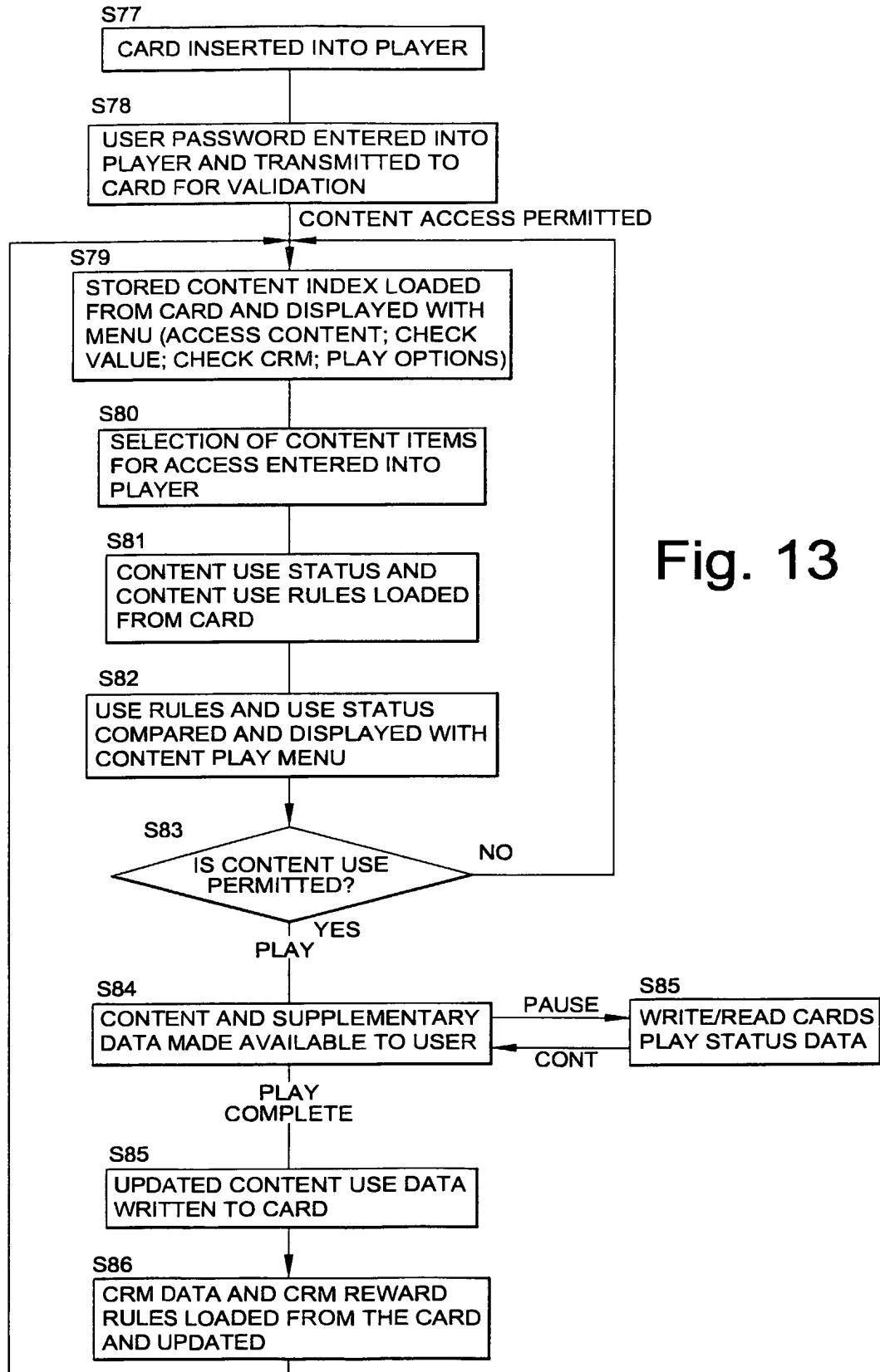


Fig. 13



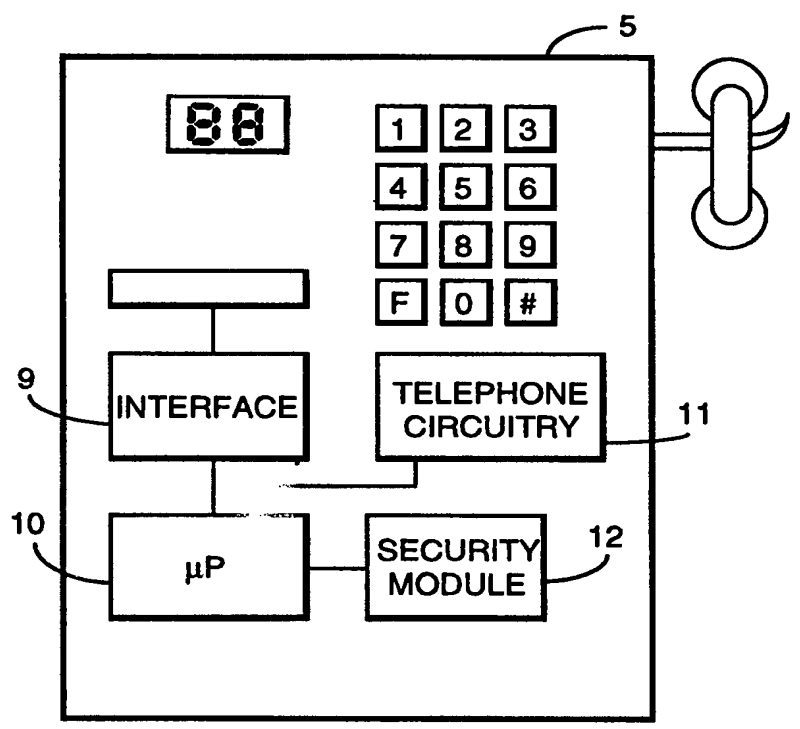
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>G06K 19/073, G07F 7/08</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 95/27955</b> (43) International Publication Date: 19 October 1995 (19.10.95)</p>
<p>(21) International Application Number: PCT/GB95/00795 (22) International Filing Date: 6 April 1995 (06.04.95) (30) Priority Data: 9406829.3 7 April 1994 (07.04.94) GB (71) Applicant (for all designated States except US): GPT LIMITED [GB/GB]; New Century Park, P.O. Box 53, Coventry CV3 1HJ (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): HUMMERSTON, William [GB/GB]; 26 Acacia Avenue, Huyton, Liverpool L36 5TW (GB). TIERNEY, John [GB/GB]; 48 Earlsfield Road, Wavetree, Liverpool L15 5BE (GB). (74) Agent: RODWELL, Jonathan; GEC Patent Dept., Waterhouse Lane, Chelmsford, Essex CM1 2QX (GB).</p>		<p>(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TT, UA, UG, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).  Published With international search report.</p>

(54) Title: SMART CARD

(57) Abstract

A smart card designed to be used as a pre-payment device comprises a multi-stage counter which includes a first stage which is decremented during payment. A second stage of the counter operates as set of one or more control bits designed to be switched by a recharging terminal to cause the first stage to be recharged. In this way a smart card having a predetermined capacity can be used as a card of lower capacity, but which can be recharged a limited number of times according to the number of control bits available.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AT</b>	Austria	<b>GB</b>	United Kingdom	<b>MR</b>	Mauritania
<b>AU</b>	Australia	<b>GE</b>	Georgia	<b>MW</b>	Malawi
<b>BB</b>	Barbados	<b>GN</b>	Guinea	<b>NE</b>	Niger
<b>BE</b>	Belgium	<b>GR</b>	Greece	<b>NL</b>	Netherlands
<b>BF</b>	Burkina Faso	<b>HU</b>	Hungary	<b>NO</b>	Norway
<b>BG</b>	Bulgaria	<b>IE</b>	Ireland	<b>NZ</b>	New Zealand
<b>BJ</b>	Benin	<b>IT</b>	Italy	<b>PL</b>	Poland
<b>BR</b>	Brazil	<b>JP</b>	Japan	<b>PT</b>	Portugal
<b>BY</b>	Belarus	<b>KE</b>	Kenya	<b>RO</b>	Romania
<b>CA</b>	Canada	<b>KG</b>	Kyrgystan	<b>RU</b>	Russian Federation
<b>CF</b>	Central African Republic	<b>KP</b>	Democratic People's Republic of Korea	<b>SD</b>	Sudan
<b>CG</b>	Congo	<b>KR</b>	Republic of Korea	<b>SE</b>	Sweden
<b>CH</b>	Switzerland	<b>KZ</b>	Kazakhstan	<b>SI</b>	Slovenia
<b>CI</b>	Côte d'Ivoire	<b>LI</b>	Liechtenstein	<b>SK</b>	Slovakia
<b>CM</b>	Cameroon	<b>LK</b>	Sri Lanka	<b>SN</b>	Senegal
<b>CN</b>	China	<b>LU</b>	Luxembourg	<b>TD</b>	Chad
<b>CS</b>	Czechoslovakia	<b>LV</b>	Latvia	<b>TG</b>	Togo
<b>CZ</b>	Czech Republic	<b>MC</b>	Monaco	<b>TJ</b>	Tajikistan
<b>DE</b>	Germany	<b>MD</b>	Republic of Moldova	<b>TT</b>	Trinidad and Tobago
<b>DK</b>	Denmark	<b>MG</b>	Madagascar	<b>UA</b>	Ukraine
<b>ES</b>	Spain	<b>ML</b>	Mali	<b>US</b>	United States of America
<b>FI</b>	Finland	<b>MN</b>	Mongolia	<b>UZ</b>	Uzbekistan
<b>FR</b>	France			<b>VN</b>	Viet Nam
<b>GA</b>	Gabon				

### Smart Card

This invention relates to smart cards designed to be used as pre-payment memory devices. A smart card basically comprises an integrated circuit which is embedded in the card. The circuit constitutes memory within which information is stored and is read when the card is in use. In the case of a card used for payment purposes, the information stored representing counter value is deducted from the memory as time progresses. One suitable available integrated circuit is known as "Eurochip" sold by Siemens. Such an arrangement can be useful when the card is used for paying the cost of a telephone conversation on a pay-phone or for some other pre-payment device, such as on a pay video channel or electricity meter. The information is stored in a plurality of bits constituting a counter which is decremented as time progresses. It is one object of the invention to provide a card which can be used more than once since this cuts down the considerably on the cost of the card in relation to its value.

According to the present invention in one aspect, there is provided a smart card to be used as a pre-payment device comprising a multi-stage counter including a first stage which is decremented during payment; and a second stage which operates as a set of one or more control bits designed to be switched by a recharging terminal to cause the first stage to be re-charged. In this way, for example, a smart card of a certain pre-payment capacity can be used as a card of a lower capacity, but which is re-chargeable a limited number of times according to the number of control bits provided.

Preferably the card includes a memory in which key-data from the recharging terminal is combined by means of an algorithm with data indicative of the respective card to generate a

certificate which is read during a payment transaction to certify that the card has been recharged by an authentic recharging terminal.

In this way, a way is provided of ensuring that the card has been recharged only by an authentic recharging terminal, as opposed to some fraudulent means.

In a preferred embodiment, the card indicative data includes data indicative of the number of times that the card has been recharged and the certificate generated is different according to that number.

In a preferred embodiment, the first stage of the counter is arranged in one or more ranks of bits, each rank corresponding to one power of the base of which the counter operates, a payment transaction being arranged to decrement the lowest order rank with the decrementing of a value greater than that in the lowest order rank being operative to decrement from a higher order rank and to recharge the lowest order rank, the control bits being located in the highest order rank.

In another aspect there is provided a system for recharging with credits a smart card designed to be used as a pre-payment device, the smart card including a first stage which is decremented during payment, and a second stage which operates as a set of one or more control bits designed, when switched, to cause the first stage to be recharged; and a recharging terminal which is operative to switch the control bits on the card.

In a further aspect there is provided a method of recharging with credits a smart card

designed to be used as a pre-payment device, the smart card including a multi-stage counter including a first stage which is decremented during payment, and a second stage which operates as a set of one or more control bits designed to cause the first stage to be recharged, the method comprising introducing the smart card to a recharging terminal which is operative to switch the control bits so as to cause the first stage of the counter to be recharged.

In order that the invention may be well understood, an embodiment thereof will now be described by way of example with reference to the accompanying diagrammatic drawings in which;

Figures 1A, 1B and 1C show the constituent parts of the system required for the invention;

Figure 2 shows the contents of the memory of the card shown in Figure 1A; and

Figure 3 shows arrangement of the counter which forms part of Figure 2.

Referring to Figures 1A to 1C, a smart card 1 includes a memory 2, in particular as will be described with reference to the "Eurochip" manufactured and sold by Siemens, and an interface 3 by which the card can communicate with a recharge terminal 4, shown in Figure 1B. In addition the system comprises a device, such as the telephone 5 shown in Figure 1C, with which the card shown in Figure 1A can be used for payment purposes.

As will be described in greater detail later on, the card 1 is designed to be sold with an



initial predetermined number of credits which are decremented in use by the telephone 5. Once the predetermined number of credits have been used up the card can be introduced into the recharge terminal 4 which comprises an interface 6 for communicating with the card 1, a microprocessor 7 and memory 8. The method of operation will be described in greater detail later on, but essentially the recharge terminal functions, upon payment by the user of the card to the terminal operator, to recharge the card 1 with credits, this can be repeated for a limited number of times. The telephone 5 includes an interface 9 for communicating with the card, a microprocessor 10 connected to telephone circuitry 11 and a security module 12 which provides a means of verifying the authentication of an inserted card.

A map showing the functions assigned to the various bits within the memory 2 on the card 1 is shown in Figure 2. In Figure 2, bits 0 to 63 comprise a read-only memory (in user mode) within which card identity, or ID, information is stored. Bits 64 to 104 comprise a counter which is decremented during payment. Figure 3 shows a base eight counter in which bits 72 to 103 are arranged in four rows or ranks R, where each rank corresponds to a power of the base which the counter operates. As shown, bits 96 to 103 represent the lowest value in the counter ie. each bit represents a value of 1 or  $8^0$ . Bits 88 to 95 each represent a value of 8, ie.  $8^1$ . Bits 64 and 69 - 71 are not available for the counter. Bits 65 to 68 are valid counter bits that can be written to once. The card is initially charged by writing a value to these bits and bits 72 to 103 giving a maximum charge of 20,480 units.

According to the invention some of the highest value bits, e.g. bits 65 to 68 are used as revaluation flag and only bits 72 to 103 are used as the counter itself (giving a reduced maximum charge of 4,096 units). The counter operates by decrementing from the lowest order

rank. Once those bits have been written to a value of zero, the next unit to be decremented causes the unit in the next highest available order rank to be written to a value of zero which thereby refigures all the succeeding bits. Bits 65 to 68 are designed to be switched in order to cause the counter to be recharged.

In order to prevent the revaluation bits 65 to 68 being recharged fraudulently a certificate is written into the memory of the card each time a revaluation is performed. Referring back to Figure 2, bits 320 to 383 provide the location for four 16 bit recharge certificates, stored in the cards memory.

Each recharge certificate is calculated as follows: a recharge algorithm R say, will take as an input a key k and some data d. It will produce as an output a certificate, C. More formally

$$C = R(k,d).$$

The input data, d, consists of a combination of the top counter stage (bits 65 - 68) and card identification data obtained from within bits 0 to 63. The key data k is stored within the memory 8 of the recharge terminal 4. In this way the data uniquely represents the card and its current recharge iteration. The algorithm is such that it is not feasible for an attacker to deduce the key data, k, from a knowledge of R, C and D, except by means of a "brute force" evaluation of all possible keys. The design such that only recharge terminals with valid keys will be able to consistently produce correct recharged certificates. No recharge certificate is required for the initial use.

Whenever the card is inserted into a telephone 5 the security module 12 determines

which certificate is currently active (e.g. if bits 65 - 68 have a value of 0011 then this implies that a second recharge has been performed). If the certificate stored on the card does not match that calculated by the security module 12, the card is rejected as having an invalid recharge certificate and cannot then be used for payment purposes. Each time the card is recharged, the appropriate bit is written to 0. For example, the first recharge will set bit 65 to 0.

Referring back to Figure 2 the memory additionally includes an activation certificate area, bits 112 to 127. The Activation Certificate is generated in a similar way to the recharge certificates described previously. The activation certificate is designed to be written onto the card at the point of sale in order to verify that the card has been sold from an authorised supplier and, for example, has not been stolen. As an alternative the activation certificate could be written into one of the spaces occupied by one of the recharge certificates. This would reduce the number of available re-uses, but would allow bits 112 to 127 to be used for other purposes. In other alternative embodiments different numbers of recharges are possible if a smaller certificate is used. Similarly, if more than four counter bits are used as the top stage of the counter, more recharges would be available. For example if an 8 bit certificate were used, bits 72-75 could also be used to control the number of recharges, but this would mean bits 76 - 79 could not be used for counter value, thus reducing the maximum recharge allowed each time, but allowing 8 recharges, and hence a total of 9 uses.

CLAIMS

1. A smart card to be used as a pre-payment device comprising a multi-stage counter including a first stage which is decremented during payment; and a second stage which operates as a set of one or more control bits designed to be switched by a recharging terminal to cause the first stage to be recharged.
2. A smart card according to claim 1 in which the card includes a memory within which a certificate is written by the recharging terminal, which certificate is readable during a payment transaction to certify that the card has been recharged by an authentic recharging terminal.
3. A smart card according to claim 2 in which key data from the recharging terminal is combined by means of an algorithm with data indicative of the card to generate the certificate.
4. A smart card according to any preceding claim in which the claim in which the card is rechargeable a limited number of times.
5. A smart card according to claim 4 as dependent on claim 3 in which the card indicative data includes data indicative of the number of times that the card has been recharged and in which the certificate generated is different according to that number.
6. A smart card according to any preceding claim in which the first stage of the counter is arranged in one or more ranks of bits, each rank corresponding to one power of the base

at which the counter operates, a payment transaction being arranged to decrement the lowest order rank, with the decrementing of a value greater than that in the lowest order rank being operative to decrement from a higher order rank and to recharge the lowest order rank, the control bits being located in the highest order rank.

7. A system for recharging with credits a smart card designed to be used as a pre-payment device, the smart card including a first stage which is decremented during payment, and a second stage which operates as a set of one or more control bits designed, when switched, to cause the first stage to be recharged; and a recharging terminal which is operative to switch the control bits on the card.
8. A system according to claim 7 in which the recharging terminal is additionally operative to write a certificate onto the card, which certificate is readable during a payment transaction to certify that the card has been recharged by an authentic recharging terminal.
9. A method of recharging with credits a smart card designed to be used as a pre-payment device, the smart card including a multi-stage counter including a first stage which is decremented during payment, and a second stage which operates as a set of one or more control bits designed to cause the first stage to be recharged, the method comprising introducing the smart card to a recharging terminal which is operative to switch the control bits so as to cause the first stage of the counter to be recharged.

10. A method according to claim 9 in which the recharging terminal writes a certificate onto the card which is readable during a payment transaction to certify that the card has been recharged by an authentic recharging terminal.

1/2

Fig.1a.

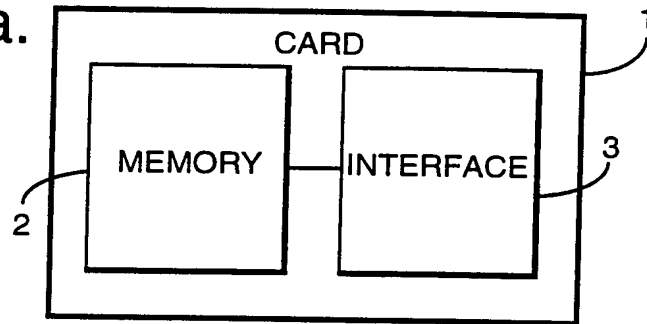


Fig.1b.

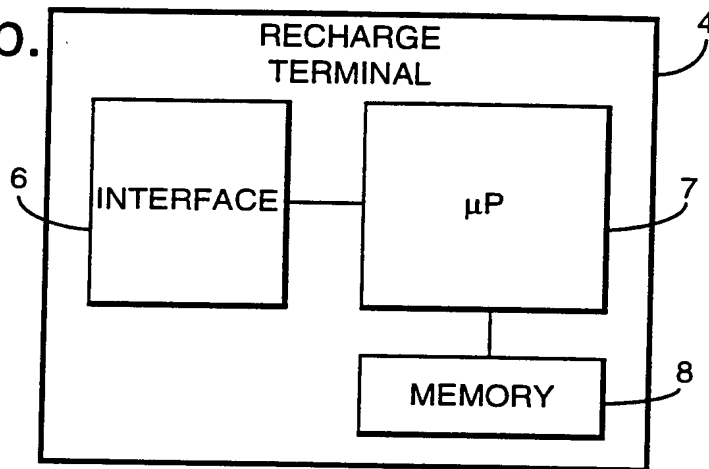
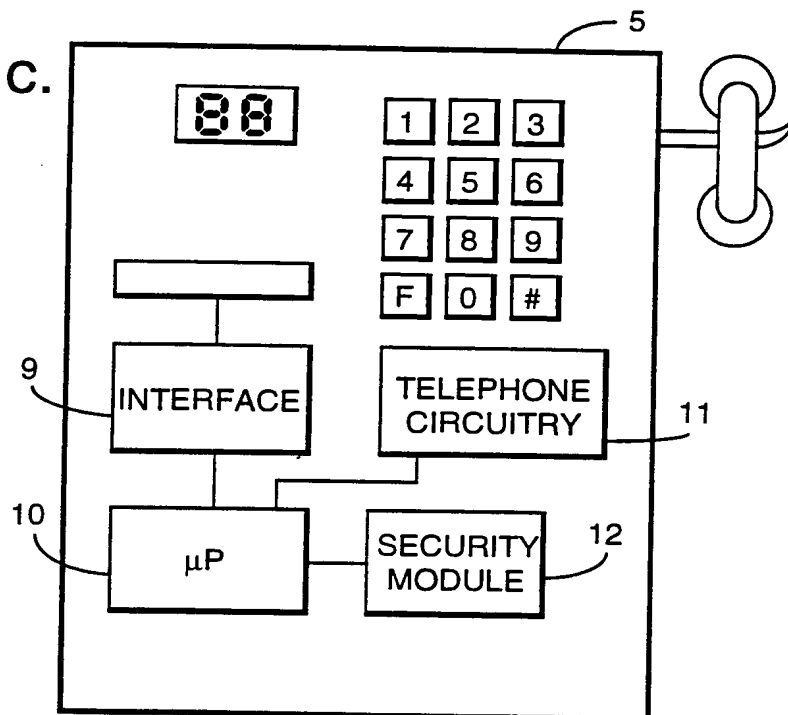


Fig.1c.



2/2

Fig.2.

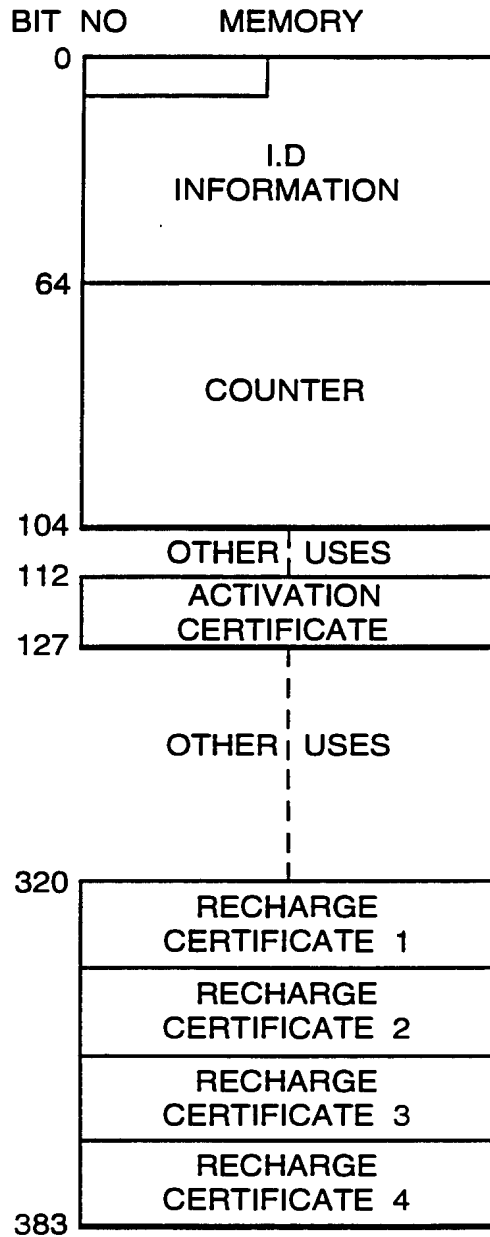


Fig.3.

BIT NO									NOTES	
64	R	x	c	c	c	c	x	x	x	EPROM 8 <sup>4</sup> =4096
72		c	c	c	c	c	c	c	c	EEPROM 8 <sup>3</sup> =512
80	R	c	c	c	c	c	c	c	c	EEPROM 8 <sup>2</sup> =64
88		c	c	c	c	c	c	c	c	EEPROM 8 <sup>1</sup> =8
96		c	c	c	c	c	c	c	c	EEPROM 8 <sup>0</sup> =1





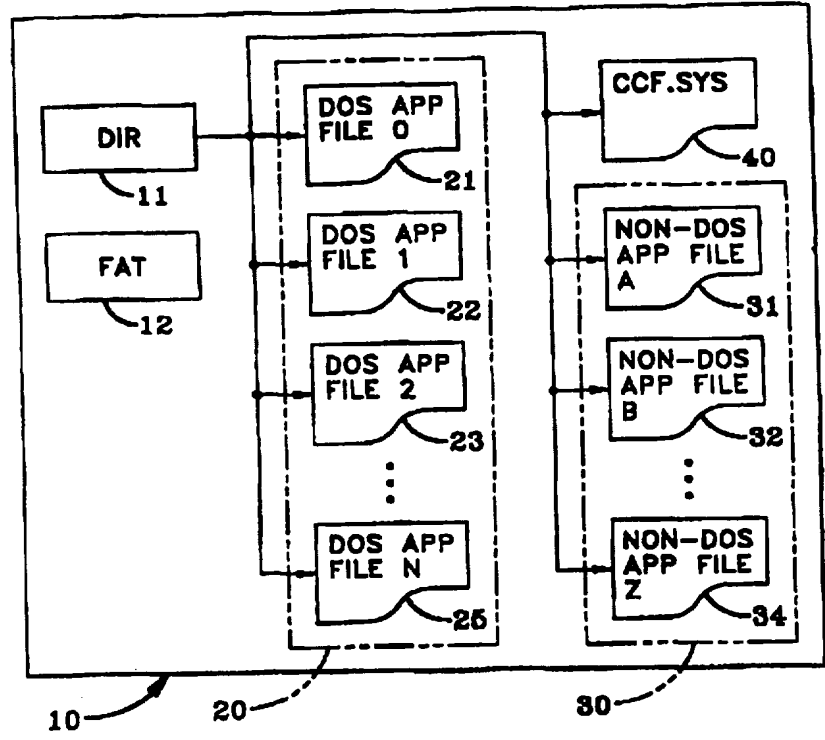
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>G06F 12/00, 9/44</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 96/19771</b> (43) International Publication Date: 27 June 1996 (27.06.96)</p>
<p>(21) International Application Number: PCT/US95/16741 (22) International Filing Date: 19 December 1995 (19.12.95) (30) Priority Data: 08/361,056 21 December 1994 (21.12.94) US (71) Applicant: EUROTRONICS COMPANY [US/US]; 770 Crosskeys Office Park, Fairport, NY 14450 (US). (72) Inventor: WEINER, Frank; 60 Tilstone Place, Rochester, NY 14618 (US). (74) Agents: SALAI, Stephen, B. et al.; Cumpston &amp; Shaw, Suite 850, Two State Street, Rochester, NY 14615 (US).</p>	<p>(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, LS, MW, SD, SZ, UG).  Published With international search report.</p>	

(54) Title: MEMORY CARD AND METHOD FOR OPERATION IN A PLURALITY OF SYSTEMS HAVING INCOMPATIBLE OBJECT CODE FORMAT REQUIREMENTS

(57) Abstract

Application software and data files (21-25, 31-34) for operating systems and processors having incompatible object code format requirements may be placed on the same memory card (10). Memory card (10) may be used by any system (16, 18) receiving the physical format of memory card (10) and whose operating system can read the logical format of memory card (10). At least one card configuration file (40) having a preselected name unique to each operating system having different object code format requirements is stored on memory card (10). Card configuration file (40) includes the names and location information for only application software and data files (21-25, 31-34) accessible and executable by that operating system. Consequently, each operating system recognizes only that application software and data files having compatible object code format requirements.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AT</b>	Austria	<b>GB</b>	United Kingdom	<b>MR</b>	Mauritania
<b>AU</b>	Australia	<b>GE</b>	Georgia	<b>MW</b>	Malawi
<b>BB</b>	Barbados	<b>GN</b>	Guinea	<b>NE</b>	Niger
<b>BE</b>	Belgium	<b>GR</b>	Greece	<b>NL</b>	Netherlands
<b>BF</b>	Burkina Faso	<b>HU</b>	Hungary	<b>NO</b>	Norway
<b>BG</b>	Bulgaria	<b>IE</b>	Ireland	<b>NZ</b>	New Zealand
<b>BJ</b>	Benin	<b>IT</b>	Italy	<b>PL</b>	Poland
<b>BR</b>	Brazil	<b>JP</b>	Japan	<b>PT</b>	Portugal
<b>BY</b>	Belarus	<b>KE</b>	Kenya	<b>RO</b>	Romania
<b>CA</b>	Canada	<b>KG</b>	Kyrgystan	<b>RU</b>	Russian Federation
<b>CF</b>	Central African Republic	<b>KP</b>	Democratic People's Republic of Korea	<b>SD</b>	Sudan
<b>CG</b>	Congo	<b>KR</b>	Republic of Korea	<b>SE</b>	Sweden
<b>CH</b>	Switzerland	<b>KZ</b>	Kazakhstan	<b>SI</b>	Slovenia
<b>CI</b>	Côte d'Ivoire	<b>LI</b>	Liechtenstein	<b>SK</b>	Slovakia
<b>CM</b>	Cameroon	<b>LK</b>	Sri Lanka	<b>SN</b>	Senegal
<b>CN</b>	China	<b>LU</b>	Luxembourg	<b>TD</b>	Chad
<b>CS</b>	Czechoslovakia	<b>LV</b>	Larvia	<b>TG</b>	Togo
<b>CZ</b>	Czech Republic	<b>MC</b>	Monaco	<b>TJ</b>	Tajikistan
<b>DE</b>	Germany	<b>MD</b>	Republic of Moldova	<b>TT</b>	Trinidad and Tobago
<b>DK</b>	Denmark	<b>MG</b>	Madagascar	<b>UA</b>	Ukraine
<b>ES</b>	Spain	<b>ML</b>	Mali	<b>US</b>	United States of America
<b>FI</b>	Finland	<b>MN</b>	Mongolia	<b>UZ</b>	Uzbekistan
<b>FR</b>	France			<b>VN</b>	Viet Nam
<b>GA</b>	Gabon				

- 1 -

**MEMORY CARD AND METHOD FOR OPERATION  
IN A PLURALITY OF SYSTEMS HAVING  
INCOMPATIBLE OBJECT CODE FORMAT REQUIREMENTS**

5

**TECHNICAL FIELD**

The present invention relates generally to devices which allow processor based systems, and especially portable processor based systems, to access additional application software or data. More particularly, the present invention relates to portable media for processor based systems such as memory cards. Still more specifically, the present invention pertains to a method by which application software and data for systems having incompatible object code formats may be stored on and operated from the same memory card or other portable media.

15

**BACKGROUND ART**

The advent of small, processor based systems has given rise to portable devices capable of performing a seemingly limitless variety of applications. The personal computer has become ubiquitous, and is now commonly available in portable form factors from laptop to notebook to the handheld palmtop. In addition, the use of systems where size and power consumption is minimized and tailored to the application, is becoming more widespread.

Users and manufacturers alike have appreciated that the utility of processor based systems, and especially such handheld systems, can be increased greatly where applications and data may be selectively added and removed by the user. This desire for greater versatility in small form factor packages has been recently accommodated by removable, business-card sized memory cards having non-volatile memory in which may be stored additional application software of interest to the user and data or other information for use with the additional or other applications native to the handheld system.

Some systems allow the user to search and retrieve the information stored on a removable memory card having an overall proprietary organization. A growing number of manufacturers now include in both handheld and larger systems connect-

- 2 -

ors to receive user installable memory cards conforming to the standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) of Sunnyvale, California.

5 Unfortunately, the object code type in many handheld systems is proprietary to the manufacturer. The result is that even though a memory card may be physically insertable into the connector provided on a given system, only the system for which it was specifically created is able to execute any application program and access any data stored thereon. This forces users to acquire separate memory cards with the same application and/or data for each system with which they desire to use the appli-  
10 cation or data.

A better understanding of the deficiencies of such existing memory devices may be achieved with a brief review of certain principals of digital memory storage. The way in which information is stored and accessed on digital memory media is a function of physical characteristics of the media and the hardware that reads from and  
15 writes to the media (collectively called the *physical format*), and various logical characteristics of the media set by the hardware according to immutable elements of the hardware and instructions from the operating system (collectively called the *logical format*). The logical format of a memory system defines the *file structure* — the form and location of the files which contain application software and data. Of  
20 course, the format with which the application software and data is recorded (collectively called the *object code*) is a function of the type of processor employed by the system. Thus, whether the contents of a file is useable in a given system (i.e., whether the application software can execute and data can be understood) further depends on the compatibility of a file's object code format with the processor type  
25 used by the handheld system.

The PCMCIA standard provides a common physical format for memory cards. The logical format most widely used with personal computers and many handheld systems is that specified by the Disk Operating System from Microsoft Corporation of Redmond, Washington (MS-DOS) executing on systems having a processor com-  
30 patible with the x86 family of microprocessors from Intel Corporation of Santa Clara California. The MS-DOS logical format separates the media into several areas including a directory, a file allocation table (FAT) and a data area. As is very well known, the directory includes the names of all files on the media, where they start

- 3 -

and their length; the FAT includes the location on the media of all parts of each file; and the data area includes the actual application program and data files.

Heretofore applications and data stored in removable memory could only be shared between devices if the physical, logical and object code formats were identical. But systems having the PCMCIA physical format and MS-DOS logical format still may and often do employ their own object code format. Even where the physical format and logical format of media is the same for two separate systems, attempted reading or execution of files whose object code is compatible with operating systems different from the one used with the system attempting access (the "foreign" system) could lockup the accessing system or at least result in unintelligible displays and/or actions confusing to users.

I have appreciated that what is necessary to overcome these shortcomings is a memory card that can store application software and data for a variety of object code formats in such a manner that application software and data for one system does not interfere with application software and data for another incompatible system. Moreover, specific application software and data should be accessible only when fully compatible with the processor used with the system attempting access, providing added security and ease of use. I have invented a memory card and method for placing application software and data in files for systems using incompatible object code types on a single memory card, and allowing any system employing the same physical and logical format to access just the files having the object code type utilized by that system.

#### SUMMARY OF THE INVENTION

It is, therefore, an object of the present invention to provide digital file storage media such as a memory card with application software and/or data for systems having incompatible object code formats.

It is another object of the present invention to provide digital file storage media such as a memory card, as set forth above, in which each system receiving the memory card recognizes as being present only application software and/or data in files stored on the memory card whose object code format is compatible with the object code format requirements of the accessing system.

- 4 -

It is still another object of the present invention to provide digital file storage media such as a memory card, as set forth above, in which each system receiving the memory card will execute the application software and access the data in files stored on the memory card which have compatible object code formats.

5 It is yet another object of the present invention to provide digital file storage media such as a memory card, as set forth above, in which no user action will be required for each system receiving the memory card to recognize and utilize the application software and/or data in files stored on the memory card which have compatible object code formats.

10 It is a further object of the present invention to provide digital file storage media such as a memory card, as set forth above, in which each system receiving the memory card will only present to the user the application software and data in files which have compatible object code format, thereby precluding user confusion about which application software and data may be accessed on that system.

15 It is still a further object of the present invention to provide digital file storage media such as a memory card, as set forth above, with any physical format and logical format desired, that will be shareable by all systems accepting memory with that physical format and logical format irrespective of the object code format requirements of the processor in use.

20 It is yet a further object of the present invention to provide digital file storage media such as a memory card, as set forth above, in which applications executing in one system can recognize common data files, thereby allowing data files to be shared across system boundaries and reducing total memory size requirements while maintaining full functionality.

25 These and other objects and advantages of the present invention over existing prior art forms will become more apparent and fully understood from the following description in conjunction with the accompanying drawings.

In general, a memory card for operating both in a first system having a first object code format and in a second system having a second object code format different than that of said first object code format, the memory card including at least one  
30 of an executable application file and a data file, includes a card configuration file stored on the memory card specifying the name and location information on the memory card of only each said executable application file having the second object

- 5 -

code format and each data file readable under the second object code format. A method for operating a memory card both in a first system having a first object code format and in a second system having a second object code format different than that of said first object code format, the memory card including at least one of an executable application file and a data file, includes storing a card configuration file specifying the name and location information on the memory card of only each executable application file and data file having the second object code format, reading the card configuration file, displaying the name of each application having the second object code format, selecting an application having the second object code format, and, executing the selected application.

### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 depicts a block diagram of a memory card having a physical format specified by PCMCIA and the logical format of Microsoft-DOS (MS-DOS) organized media. The memory card includes a plurality of files (Files 0 through n) readable and executable under MS-DOS in a system having an x86 Intel Corporation compatible processor, a plurality of files (Files A through Z) readable and executable under a proprietary operating system (not MS-DOS compatible) in a system having a processor other than an x86 Intel Corporation compatible processor, and a Card Configuration File (CCF.SYS) in accordance with the present invention.

Fig. 2 presents a perspective view of two exemplary devices, a conventional notebook computer operating under MS-DOS in a system having an x86 Intel Corporation compatible processor, and a handheld unit operating under a proprietary operating system in a system having a processor other than an x86 Intel Corporation compatible processor, which both receive the memory card shown in Fig. 1, and read and run executable files stored therein compliant with their respective operating systems and processor types.

Fig. 3 presents a flow chart of an exemplary method in accordance with the present invention by which the plurality of Files A through Z readable but not executable under the native operating system (MS-DOS) may be identified and executed from the same memory card under their respective operating system.

Fig. 4 presents a flow chart of an exemplary method in accordance with the present invention by which the applications of Files A through Z readable but not

- 6 -

executable under the native operating system (MS-DOS) may be identified to and selected by a user for execution.

#### **PREFERRED EMBODIMENT FOR CARRYING OUT THE INVENTION**

5           Fig. 1 presents a block diagram of an exemplary memory card, indicated generally by the numeral 10, in accordance with the concept of the present invention. Memory card 10 preferably has the physical format of PCMCIA organized media and the logical format of Microsoft DOS (MS-DOS) organized media, and therefore includes a directory 11, at least one file allocation table (FAT) 12, and a plurality of files 20 readable and, where in executable form, executable under MS-DOS in a system having an x86 Intel Corporation compatible processor. Memory card 10 further includes a plurality of files 30 readable but not, when in executable form, executable under MS-DOS in a system having an x86 Intel Corporation compatible processor, and a Card Configuration File 40 (CCF.SYS 40).

15           As is customary under the MS-DOS logical format, directory 11 includes the name, length, attributes and starting location of every file stored on memory card 10. Also, one MS-DOS logical format attribute allows each file to be hidden from most MS-DOS commands. For example, a file with the Hidden attribute bit set will not be displayed when a list directory command DIR is entered by the user to list the contents of the directory.

20           Memory card 10 may be a conventional memory card conforming to the standards of the Personal Computer Memory Card International Association (PCMCIA) of Sunnyvale, California, insertable into any PCMCIA compatible port 15, as illustrated in Fig. 2 in the notebook computer 16 employing the MS-DOS operating system, and port 17, as illustrated in the handheld unit 18 employing a proprietary, closed operating system capable of accessing memory organized in accordance with the MS-DOS logical format. Thus, in the present example, both the MS-DOS computer 16 and the non-DOS handheld unit 18 may receive memory card 10 and access files stored thereon. Handheld units, and particularly those that operate other than with the MS-DOS operating system like handheld unit 18, commonly include a menu manager and display 19 to simplify and facilitate user interaction by listing the available applications and, upon user selection, begin execution of the appropriate application software.



- 7 -

The Card Configuration File (CCF.SYS) 40 is a conventional MS-DOS file that stores the file name and associated application name for each file not intended for use with MS-DOS. The proprietary operating system must include software allowing it to locate and read card configuration file 40, and access directory 11 and FAT 12 for the additional information required to access the selected files as provided under the MS-DOS logical format. It will be understood that any name may be preselected for card configuration file 40, so long as that name is known to the proprietary operating system onboard the non-DOS accessing system, handheld unit 18 in the present example.

Operation of an application stored on memory card 10, or access of data stored on memory card 10 will of course depend on whether or not the system making use of memory card 10 employs an MS-DOS or some other operating system. In a system employing the MS-DOS operating system such as notebook computer 16, the card configuration file 40 and the files not intended for use with that operating system are hidden from the MS-DOS user and MS-DOS applications using the hidden file attribute. In this manner memory card 10 appears to the user as a conventional MS-DOS memory device, and can be used in the conventional manner.

In a system employing an operating system other than MS-DOS, operation of an application stored on memory card 10 may be best appreciated from the top-level flow-chart depicted in Fig. 3. Beginning with the start block 45, this exemplary operation can be seen to involve broadly two steps: housekeeping checks (in block 50) and, in block 60, registration of each non-MS-DOS application present on memory card 10 with a utility such as a main menu manager for identification to and selection by the user.

The housekeeping checks begin with a test in block 51 whether a memory card 10 is inserted into PCMCIA port 15 or 17, and, if not, the test is repeated until a memory card 10 is found. Once a memory card 10 is found, the directory of memory card 10 is scanned in step 52 to locate the card configuration file 40 having the preselected filename, CCF.SYS in the present example. If the card configuration file 40 is not found, an appropriate error message may be displayed to the user as noted in block 53, and testing for the presence of a suitable memory card 10 resumed. If the card configuration file 40 is found, it is read (block 54) and checked for form and content (block 55). If CCF.SYS is unreadable, damaged in form or empty, once

- 8 -

again an appropriate error message may be display to the user (block 56) and testing for a suitable memory card 10 resumed.

Once a CCF.SYS file in proper form has been located, an operating system pointer may be set to the first application software listed in the CCF.SYS file (block 61). This application software is tested (block 62) to determine if it is the last listed application software. If so, main menu manager 19 may be run as explained further hereinafter (block 63). If the application software to which the pointer is newly directed is not the last listed application software, the non-DOS operating system of handheld unit 18 loads that application software (block 64) and tests it to ascertain whether it is compatible with that operating system (block 65). If so, its presence and name is registered with the main menu manager (block 66), and the CCF.SYS file pointer is incremented (block 67) and the file to which the file pointer is now directed tested to determine if it is the last application software (block 62). If that application software is not compatible with that operating system, the CCF.SYS file pointer is directly incremented (block 67).

It will be understood that since data files are all in MS-DOS logical format, any application software knowing its name may access such a file using the conventional MS-DOS directory and FAT architecture. Thus, both the selected general operating system (here MS-DOS) and the proprietary, (non-MS-DOS) operating system may share selected files in a manner completely transparent to the user and the application software.

The skilled artisan should now appreciate several salient aspects of the present invention. For example, memory card 10 may have any physical format and logical format consistent with that used by media in the systems with which memory card 10 is to operate. The choice for the example hereinabove is based upon the widespread use of both the PCMCIA form factor and the MS-DOS logical format.

It will also be understood that the present invention allows files having any number of different object code formats to coexist on the same media. In that instance a separate card configuration file with a unique name may be selected for the files associated with each different operating system.

Another significant aspect of the present invention is that systems having different processor dictated object code formats may share the same data files by insuring that the application software can read data files having the file structure of

- 9 -

interest. Thus, applications such as Microsoft Word that utilize the same internal file organization whether operating under MS-DOS or Apple MacIntosh System 7 will be able to directly utilize the same word processing files.

5 Inasmuch as the present invention is subject to many variations, modifications and changes in detail, a number of which have been expressly stated herein, it is intended that all matter described throughout this entire specification or shown in the accompanying drawings be interpreted as illustrative and not in a limiting sense. It should thus be evident that a device constructed and method performed according to the concept of the present invention, and reasonably equivalent thereto, will accomplish the objects of the present invention and otherwise substantially improve the art of  
10 digital storage media such as memory card utilization in a plurality of systems having incompatible object code format requirements.

## CLAIMS:

- 1 1. A memory card for operating both in a first system having a first object code  
2 format and in a second system having a second object code format different than that  
3 of said first object code format, the memory card including at least one of an execut-  
4 able application file and a data file, comprising a card configuration file stored on the  
5 memory card specifying the name and location information on the memory card of  
6 only each said executable application file having said second object code format and  
7 each said data file readable under said second object code format.
- 1 2. A memory card, as set forth in claim 1, wherein the memory card has a phys-  
2 ical format and a logical format common to both said first system and said second  
3 system.
- 1 3. A memory card, as set forth in claim 2, wherein said logical format includes  
2 a directory in which is stored a preselected name for said card configuration file, and  
3 the names of and location information regarding all said executable application files  
4 and said data files stored on the memory card irrespective of the object code format  
5 of said executable application file and said data file.
- 1 4. A memory card, as set forth in claim 3, wherein said directory includes a  
2 hidden file attribute associated with said card configuration file and each said  
3 executable application file and said data file, said attribute set to hide said card  
4 configuration file and each said executable application file having said second object  
5 code format and each said data file readable under said second object code format.
- 1 5. A memory card for operating in a plurality of systems including a first system  
2 having a first object code format and in a plurality of additional systems each having  
3 an object code format different than that of said first object code format, the memory  
4 card including at least one of an executable application file and a data file, compris-  
5 ing a card configuration file stored on the memory card specifying the name and  
6 location information on the memory card of only each said executable application file  
7 having an object code format different from that of said first object code format and

- 11 -

8 each said data file readable under an object code format different from that of said  
9 first object code format.

1 6. A memory card, as set forth in claim 5, wherein the memory card has a  
2 physical format and a logical format common to said first system and all said  
3 additional systems.

1 7. A memory card, as set forth in claim 6, wherein the memory card includes a  
2 card configuration file for each said object code format different from that of said  
3 first object code format.

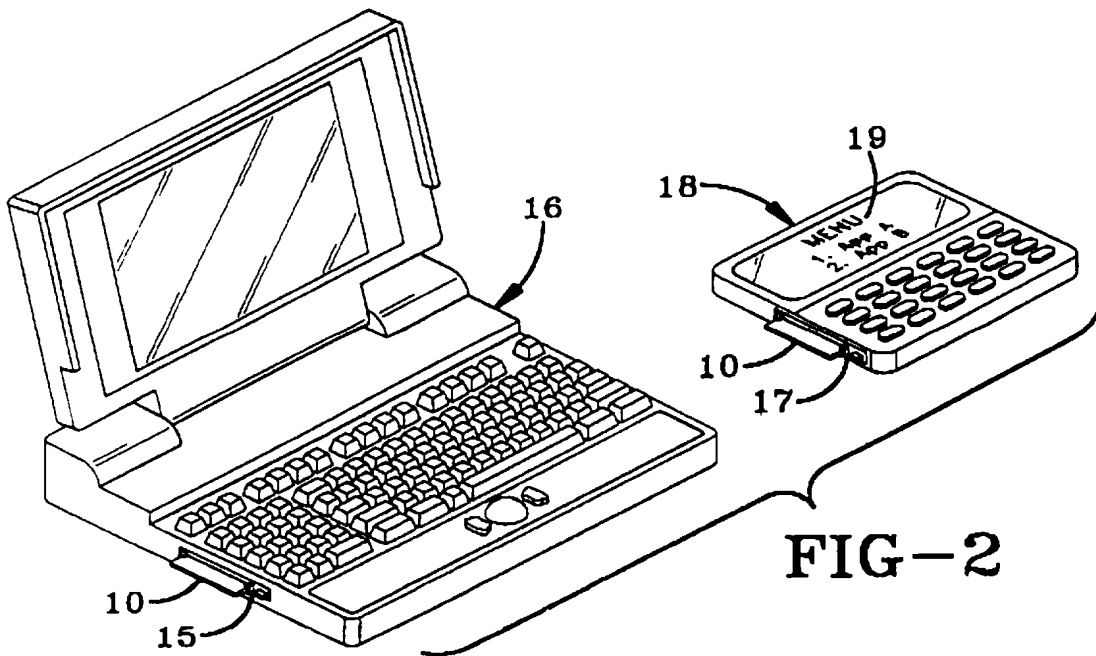
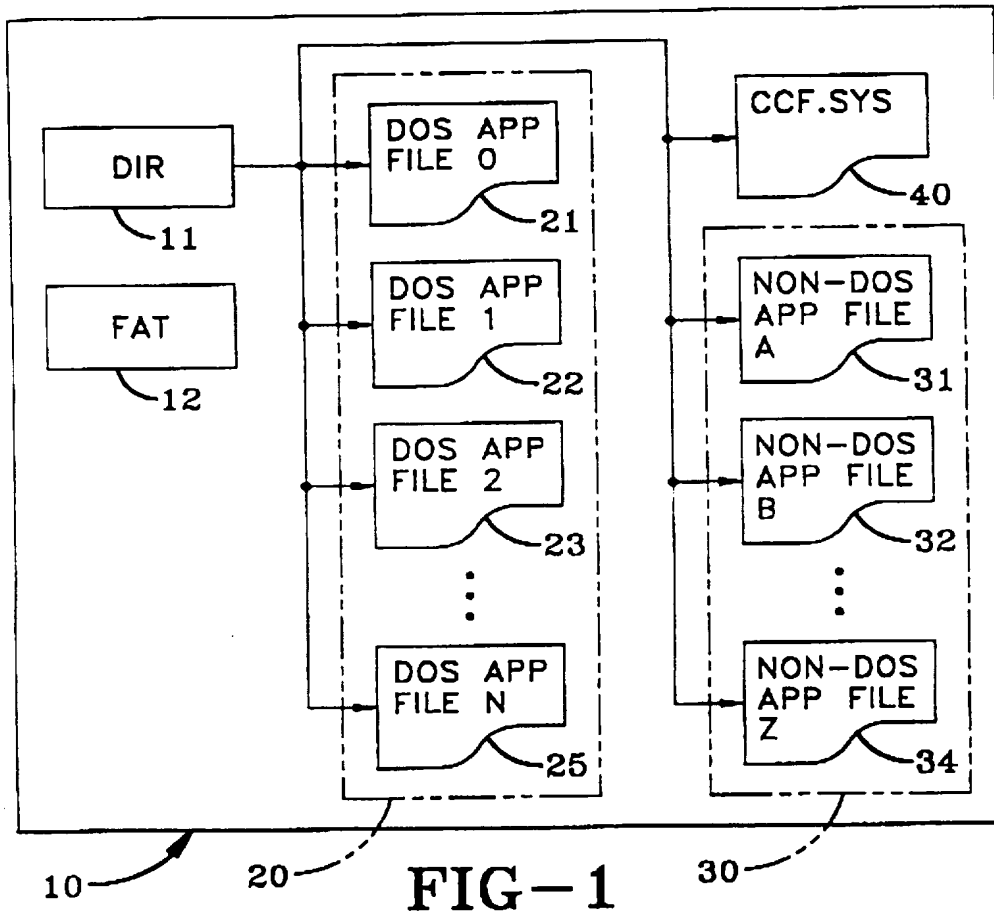
1 8. A memory card, as set forth in claim 7, wherein said logical format includes  
2 a directory in which is stored a preselected name for said card configuration file, and  
3 the names of and location information regarding all said executable application files  
4 and said data files stored on the memory card irrespective of the object code format  
5 of said executable application file and said data file.

1 9. A memory card, as set forth in claim 8, wherein said directory includes a  
2 hidden file attribute associated with said card configuration file and each said  
3 executable application file and said data file, said attribute set to hide said card  
4 configuration file and each said executable application file having an object code  
5 format different from said first object code format and each said data file readable  
6 under an object code format different from said first object code format.

1 10. A method for operating a memory card both in a first system having a first  
2 object code format and in a second system having a second object code format differ-  
3 ent than that of said first object code format, the memory card including at least one  
4 of an executable application file and a data file, comprising:

5 storing a card configuration file specifying the name and location  
6 information on the memory card of only each said executable application file  
7 and said data file having said second object code format;  
8 reading said card configuration file;  
9 displaying the name of each application having said second object code

- 10           format;
- 11            selecting an application having said second object code format; and,
- 12            executing said selected application.
- 1       11.    A method, as set forth in claim 10, further including testing for the presence
- 2            and form of said card configuration file on the memory card.
- 1       12.    A method, as set forth in claim 11, further including identifying each
- 2            application present on the memory card having said second object code format and
- 3            registering same with a user selection menu.
- 1       13.    A method, as set forth in claim 12, wherein said step of storing includes
- 2            setting an attribute for hiding said card configuration file and each said executable
- 3            application file and said data file having said second object code format.



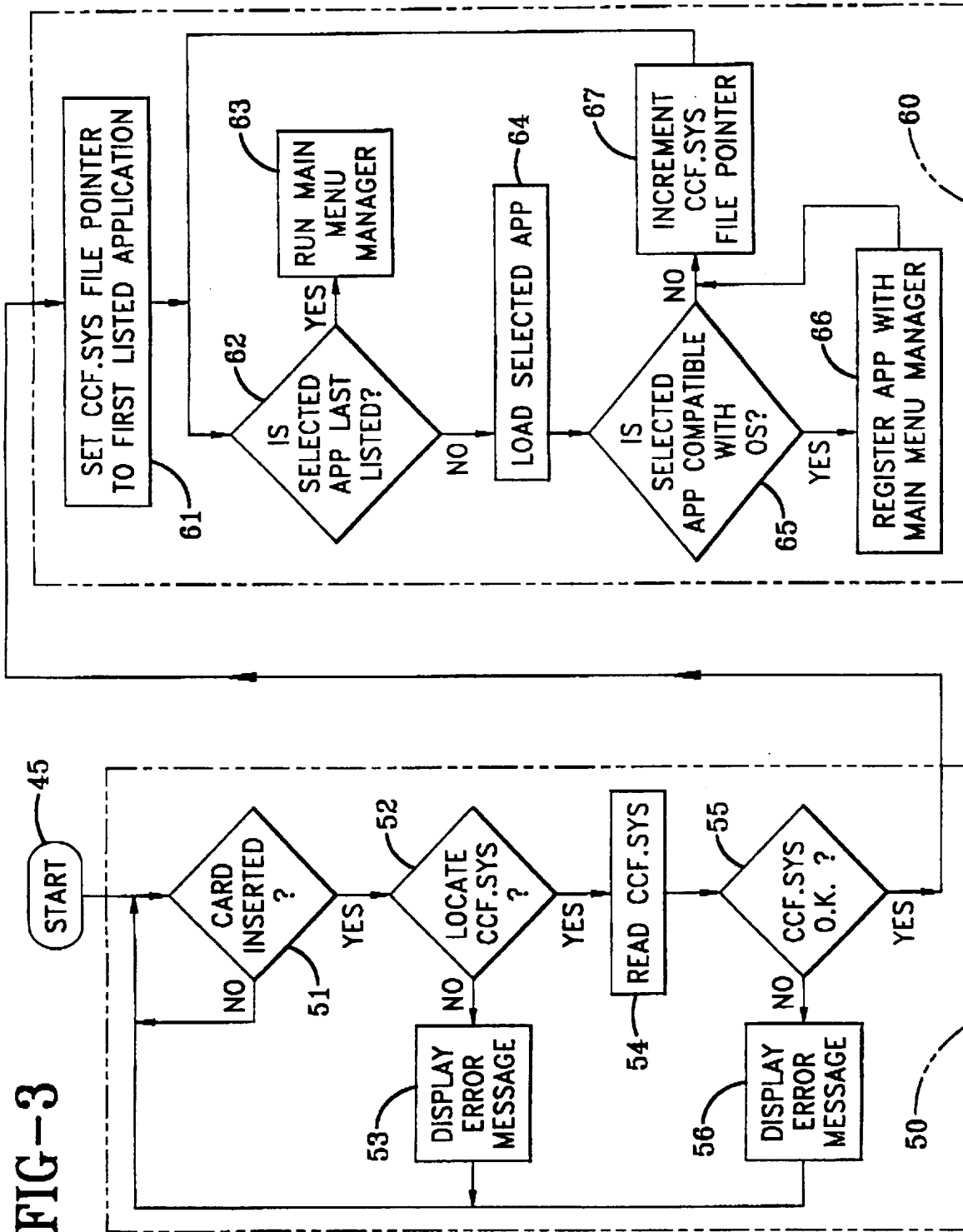


FIG-3



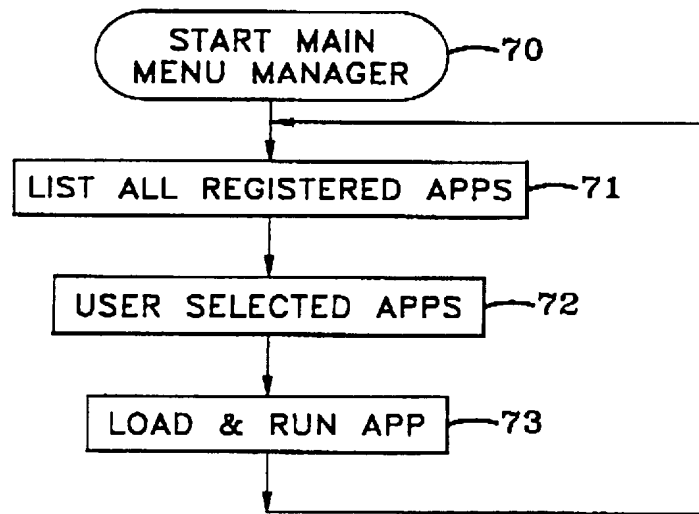


FIG-4



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>G07F 7/10, G06K 19/07</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 96/25724</b></p> <p>(43) International Publication Date: 22 August 1996 (22.08.96)</p>
<p>(21) International Application Number: PCT/BE95/00017</p> <p>(22) International Filing Date: 17 February 1995 (17.02.95)</p> <p>(71) Applicant (for all designated States except US): EUROPAY INTERNATIONAL S.A. [BE/BE]; Chaussée de Tervuren 198A, B-1410 Waterloo (BE).</p> <p>(72) Inventors; and</p> <p>(75) Inventors/Applicants (for US only): HEYNS, Guido [BE/BE]; Eekhoornlaan 23B, B-3210 Linden (BE). JOHANNES, Peter [BE/BE]; Edalzangerslaan 56/11, B-3010 Kessel-Lo (BE).</p> <p>(74) Agents: LEMAIRE, Guy et al.; Bureau Vander Haeghen-K.O.B. S.A., Rue Colonel Bourg 108A, B-1040 Bruxelles (BE).</p>		<p>(81) Designated States: AM, AU, BB, BG, BR, BY, CA, CN, CZ, EE, FI, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MN, MW, MX, NO, NZ, PL, RO, RU, SD, SI, SK, TJ, TT, UA, US, UZ, VN, ARIPO patent (KE, MW, SD, SZ, UG), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> <i>With international search report.</i></p>
<p>(54) Title: INTEGRATED CIRCUIT CONTROLLED TRANSACTION MANAGEMENT SYSTEM</p>		
<p>(57) Abstract</p> <p>An integrated circuit controlled transaction management system using an interpreter which deals with the execution of an application, either on an ICC, or on a terminal or on both, is particularly able to execute an application between the ICC and the terminal connected or not to a central unit, when the interpreter in the terminal is able to access and to use at least a part of the terminal memory and at least a part of the terminal peripherals while an optional interpreter in the ICC is able to access and to use at least a part of the ICC memory and at least a part of the ICC peripherals.</p>		

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AM</b>	Armenia	<b>GB</b>	United Kingdom	<b>MW</b>	Malawi
<b>AT</b>	Austria	<b>GE</b>	Georgia	<b>MX</b>	Mexico
<b>AU</b>	Australia	<b>GN</b>	Guinea	<b>NE</b>	Niger
<b>BB</b>	Barbados	<b>GR</b>	Greece	<b>NL</b>	Netherlands
<b>BE</b>	Belgium	<b>HU</b>	Hungary	<b>NO</b>	Norway
<b>BF</b>	Burkina Faso	<b>IE</b>	Ireland	<b>NZ</b>	New Zealand
<b>BG</b>	Bulgaria	<b>IT</b>	Italy	<b>PL</b>	Poland
<b>BJ</b>	Benin	<b>JP</b>	Japan	<b>PT</b>	Portugal
<b>BR</b>	Brazil	<b>KE</b>	Kenya	<b>RO</b>	Romania
<b>BY</b>	Belarus	<b>KG</b>	Kyrgystan	<b>RU</b>	Russian Federation
<b>CA</b>	Canada	<b>KP</b>	Democratic People's Republic of Korea	<b>SD</b>	Sudan
<b>CF</b>	Central African Republic	<b>KR</b>	Republic of Korea	<b>SE</b>	Sweden
<b>CG</b>	Congo	<b>KZ</b>	Kazakhstan	<b>SG</b>	Singapore
<b>CH</b>	Switzerland	<b>LI</b>	Liechtenstein	<b>SI</b>	Slovenia
<b>CI</b>	Côte d'Ivoire	<b>LU</b>	Luxembourg	<b>SK</b>	Slovakia
<b>CM</b>	Cameroon	<b>LK</b>	Sri Lanka	<b>SN</b>	Senegal
<b>CN</b>	China	<b>LR</b>	Liberia	<b>SZ</b>	Swaziland
<b>CS</b>	Czechoslovakia	<b>LT</b>	Lithuania	<b>TD</b>	Chad
<b>CZ</b>	Czech Republic	<b>LV</b>	Latvia	<b>TG</b>	Togo
<b>DE</b>	Germany	<b>MC</b>	Monaco	<b>TJ</b>	Tajikistan
<b>DK</b>	Denmark	<b>MD</b>	Republic of Moldova	<b>TT</b>	Trinidad and Tobago
<b>EE</b>	Estonia	<b>MG</b>	Madagascar	<b>UA</b>	Ukraine
<b>ES</b>	Spain	<b>ML</b>	Mali	<b>UG</b>	Uganda
<b>FI</b>	Finland	<b>MN</b>	Mongolia	<b>US</b>	United States of America
<b>FR</b>	France	<b>MR</b>	Mauritania	<b>UZ</b>	Uzbekistan
<b>GA</b>	Gabon			<b>VN</b>	Viet Nam

5 INTEGRATED CIRCUIT CONTROLLED TRANSACTION MANAGEMENT  
SYSTEM

10 The present invention relates to an integrated  
circuit controlled transaction management system  
intended to execute a transaction between an integrated  
circuit card (ICC) and a terminal connected or not to  
a central unit, a transaction consisting of at least one  
execution of the following sequence :

15

1. creating a communication link between the ICC and  
the terminal ;
2. performing a compatibility check to ensure that  
the ICC and the terminal are mechanically and  
20 electrically compatible ;
3. selection of an application supported both by the  
ICC and the terminal, that means the selection of  
a computer program and the associated data set  
that defines the transaction in terms of the  
25 specific ICC and terminal combination present ;
4. execution of said application on the ICC and  
terminal system, and
5. termination of the transaction, which optionally  
includes breaking of the communication link between  
30 the ICC and the terminal.

Document WO 92/13322 describes a secured  
method for loading a plurality of applications in a  
microprocessor memory ICC, containing means for creating  
35 a communication link in an ICC and terminal system.

There are several types of transactions between an ICC and a terminal :  
the terminal may control access to places where only ICC holders may have access to ; in so-called financial transactions the ICC can be loaded with tokens representing consumption goods obtainable at a terminal site (e.g. frequent flyer miles, telecommunication units, etc...) , or the ICC may act as a depository of bank account information which allows more general financial transactions ; or the ICC may be used as data storage, e.g. as an identity ICC or medical record storage.

Known features of said ICC and terminal system are :

1. The terminal hardware (i.e. the processor and the peripherals, which at least include the ICC communication device) is accessible via the terminal operating system. Terminal operating systems are vendor specific.
2. Each terminal that participates in certain types of standardised transaction types (e.g. international financial transactions) supports, for those transactions, a common standard allowing the ICCs to perform applications in a standard way with terminals from any vendor. By way of example, international financial transactions are currently based on the inter industry standards as defined in ISO 7810/7811/7812/7813/7816.
3. Each provider of standardised transactions on a terminal has to provide an application, i.e. a program and the associated data set, or an application specification, defined in terms of a common standard.
4. Some parties provide applications or application specifications that are only partly build on a

common standard. For special requirements which are outside the scope of the common standard, said parties need to rely on the terminal operating system.

- 5 5. Other parties provide applications or application specifications, which are proprietary to them or which are not based on any common standard. In this case they solely rely on the terminal operating system to perform the transaction.
- 10 6. Each application program needs to be compiled and linked separately for each terminal type. This means that specific software has to be resident in the terminal for each application .
- 15 7. Applications define large sets of terminal parameters governing the rules of their acceptance. These parameters may need to be shared with other applications.
8. Application software must be physically installed in each terminal.
- 20 9. Different versions of application software defining the same transaction may be required on the terminal during more or less extended conversion periods.

25 The features associated with said known ICC and terminal system loaded with multiple applications, impose heavy constraints on the terminal hardware, which must be able to store and to manage all possible application software and the assorted data sets.

30 Moreover, a considerable logistic effort is indispensable to manage the distribution and the maintenance of all the software in all the terminals. Those features have the following drawbacks :

- 35 \* Changing terminal software specifications or parts

- 5 thereof, changing application software specifications or parts thereof or changing the implementations of a specification or parts thereof or creating new applications requires to develop new software for each target terminal type and to load this new software in each target terminal. Moreover, certification against all ICC types in circulation at that moment and against those scheduled for future release is required ;
- 10 \* Restricted flexibility because even minor changes to a common standard have to be agreed between all parties that use it ;
- \* Every application requires storage capacity on the terminal, which is limited ;
- 15 \* Common standards are not complete enough to support all proprietary needs ;
- \* The applications need to be implemented carefully so that neither their programs, nor their parameters interfere with each other ;
- 20 \* This approach reduces the ICC to a mere memory device, as it is not possible to give the ICC the control over each type of terminal due to the plethora of different operating systems in use.

25 The above mentioned drawbacks result in a lack of flexibility of said ICC and terminal system. Hence the time to market new, upgraded or improved applications is extremely long, in the order of several years as all ICCs and all terminals are affected.

30 The present invention aims to ease the management of all possible applications with all possible ICCs on all possible terminals. This purpose is achieved by means of an ICC transaction management system of the type described in the preamble of the

35

enclosed claim 1 by using an interpreter which deals with the execution of an application either on the ICC, or on the terminal, or on both whereby the interpreter in the terminal is able to access and to use at least  
5 a part of the terminal memory and a part of the terminal peripherals, e.g. keyboard, display, printer, modem, while an optional interpreter in the ICC is able to access and to use at least a part of the ICC memory and at least a part of ICC peripherals , e.g. keyboard,  
10 display.

Indeed, an interpreter performs the interpretation between a program written in a compact high level and universal language and the language  
15 specific to operate the terminal or the ICC. For all practical purposes an interpreter consists of a program which reads an input stream (the interpreter on the ICC reads the input stream coming from the terminal and the interpreter on the terminal reads the input stream  
20 coming from the ICC) and of one or more dictionaries, whereby a dictionary is a collection of words, each referring to executable statements. The interpreter language is independent of the ICC and terminal system, and may e.g. be FORTH (see ANSI standard : X3J14  
25 Secretary, c/o FORTH Inc. 111 Sepulveda Blvd. Suite 300, Manhattan Beach, CA 90266).

A first advantage of using an interpreter in an ICC controlled transaction management system  
30 according to the invention, is the possibility to store new applications or parts thereof or upgrades or improvements to existing applications or parts thereof on the ICC coded in an interpreted language. This allows to reduce the time to market new applications or to up-  
35 grade or improve existing applications or parts thereof.



Time or effort required to market new, upgraded or improved applications is reduced to the time or effort required to load them in terms of the interpreter language in the ICC, which may require loading new, improved or upgraded dictionaries on the ICC. In this way the ICC has control over the application. No time or effort is required to update terminals. Even when changes to terminal dictionaries must be made, it is sufficient to load the new, upgraded or improved definitions in the ICC during an introductory or reconversion period until the new upgraded or improved definitions are available on the terminal. It is possible to implement the ICC and terminal system in such a way that the new , upgraded or improved definitions in the ICC are transferred to the terminal during a transaction and stored permanently in the terminal memory thereafter .

Management of terminal functionality is reduced to the installation once of the same interpreter program and the same interpreter language dictionary, hereafter referred to as interpreter core dictionary, either during the manufacturing process of the terminal or thereafter . It is possible to upgrade or improve the interpreter after installation of the terminal, e.g. by means of on-line down-loading or through an ICC . Optional additional dictionaries, e.g. proprietary dictionaries or common standard dictionaries may be loaded on the terminal.

A second advantage of using an interpreter in an ICC controlled transaction management system according to the invention is that the support for many applications on the terminal is reduced to the availability on the terminal of the interpreter program and the interpreter core dictionary and identifications

of the supported applications. Additional dictionaries are optional.

5 A third advantage of using an interpreter in an ICC controlled transaction management system according to the invention is the possibility for the ICC to fully define and hence control the application.

10 The present invention provides the possibility to efficiently manage many applications on many fundamentally different terminals and the possibility to install new or improved or upgraded applications or parts thereof in a very efficient way,  
15 to have an extremely short time to market of new, upgraded or improved transactions and to allow the ICC to control the transaction.

Positive implications of the above are:

- 20 \* Changing terminal software specifications only affects the interpreter implementation on that terminal. The only effort needed to maintain compatibility with existing applications is to ensure that the interpreter program and the interpreter core remain implemented correctly.  
25 Hence only one software needs to be recertified, and only against one specification, namely the interpreter definition. ICCs need not to be recertified as the interpreter language used in the application retains the same specification.
- 30 \* The need for common standards is reduced to the availability of the interpreter as each standard function can be coded in the interpreter language and stored in the ICC.
- 35 \* Introducing new, improved or upgraded applications needs not to affect dictionaries that have to be

stored on the terminal, as all applications and related dictionaries are defined in terms of the interpreter language and can be loaded on the ICC.

- 5 \* The application data sets are all managed by the interpreter, which eases their management.
- \* The ICC can take actively part in the execution of the application program or parts thereof by also implementing an interpreter program and core dictionary on the ICC. If the ICC is a mere memory  
10 ICC, it can still control the application by completely storing it, i.e. the terminal acts completely according to the ICC definitions.

Some applications may require specific  
15 security services, e.g. data integrity, ICC authentication, terminal authentication or data confidentiality. These can be provided with state of the art techniques as defined e.g. in ISO 10202.

20 According to a first particularity of the invention, an application consists of one or more functions, each function consisting of a controlling part referred to as the header of the function and an executable part referred to as the body of said  
25 function. The header determines which bodies have to be executed and under which conditions. Both parts of the function are able to be independently stored in a dictionary. Functions may be defined in terms of other functions, i.e. functions may be nested.

30 A body which is stored in a dictionary is accessible via its body name, and a header stored in a dictionary is accessible via its header name. This does not prevent in any way to program a function in the  
35 interpreter language, it merely offers the possibility

to write compact and yet flexible applications by carefully mixing body names, header names and interpreter language code. Functions themselves can also be stored in dictionaries, referred to by means of their header names. This reference method allows to  
5 define each function in four ways:

1. Both the header and the body can be interpreter language code ;
2. The header can be interpreter language code while  
10 the body is activated through its body name ;
3. The header is defined through its header name, while the body is fully expanded interpreter language code ;
4. Both the header and the body are stored as  
15 references, header name and body name respectively.

The invention allows the presence of several types of dictionaries in the ICC and terminal system:

1. the interpreter core, a mandatory dictionary;
- 20 2. a number of optional dictionaries including definitions relating to :
  - a) certain types of standardized transactions, e.g. the dictionary containing all functions defined in ISO/IEC 7816 used in international  
25 financial transactions, referred to as the standard dictionary ;
  - b) proprietary transactions, requiring non standard definitions, referred to as proprietary dictionary ;

30 The dictionary defined on the ICC may contain new, improved or upgraded functions or parts thereof. Those dictionaries normally take precedence over terminal dictionaries. However the security of some  
35 applications may prohibit the redefinition of certain

words in certain dictionaries.

Security features can be provided through the specific protection mechanisms available in state of the art interpreter implementations.

5

The invention allows to store an application efficiently on the ICC and allows for flexible execution on the ICC and terminal system. Indeed, the following storage scenarios are possible thanks to the invention:

- 10 1. The transaction fully adheres to a standard. This means that the ICC only has to store the function name of the application, which is defined in the standard dictionary on the terminal;
- 15 2. If the transaction is proprietary and the application is defined on the terminal it communicates with, the ICC only has to store the function name of the application, which is defined in the proprietary dictionary on the terminal;
- 20 3. If the transaction is proprietary and the application is not defined on the terminal it communicates with, the definition of the application must then be stored on the ICC, in the ICC dictionary. The functions of the application
- 25 can use body names and header names of both the standard and the proprietary dictionaries, but can also include interpreter language code.

30 Example 1 :

Assuming an application with the following header (given in pseudo-code) :

```
if (x=1) then func_a(y)
                else if (x_2) then func_b(y)
35                else func_c(y)
```

whereby func\_a, func\_b and func\_c are defined in the terminal proprietary dictionary. Assuming func\_a(y)=y+x, in that dictionary. Then the header as presented above is all that needs to be stored in the ICC to be able to execute it. In this case there is no need for an ICC dictionary. Now, assuming the interpreter implementation allows ICC dictionaries to take precedence over terminal dictionaries, and assuming the application provider wants to redefine func\_a(y), into func\_a(y)=y-x. In this case he can still use the same header, and he now has the choice to either update all proprietary dictionaries in all terminals, or to include the new definition in the ICC dictionary. This new definition will then be used during the execution of the application.

The invention allows that :

- a) a ICC dictionary can be used to add to, improve or upgrade terminal dictionary definitions. A mechanism to do this is e.g. provided in the FORTH language, where the words defined last can redefine earlier dictionary entries.
- b) some dictionaries, e.g. the interpreter core or the standard dictionary for some applications, may be protected against erasure and against redefinitions. Techniques to achieve such protection are state of the art; an example is presented in patent WO90/05347.

The following execution scenarios are possible thanks to the invention:

1. The terminal executes the application program or parts thereof, whereby the ICC only acts as a data container and possibly as a storage device for the

- proprietary application program, or parts thereof.
2. Both the ICC and the terminal execute parts of the application. For security reasons it might be required that certain data do not leave the ICC, hence all manipulations involving such data must be executed by the ICC. Hence the ICC and the terminal communicate results of data manipulations instead of the data itself.
  3. The ICC executes the application, whereby the terminal only needs to contain application identifications it supports. In this case the terminal may be used as a mere storage device, e.g. the terminal can provide the ICC with a dictionary that contains definitions of functions in terms of the interpreter language that are used during the execution of the application by the ICC.  
This allows the ICC to use definitions without having to store them.

20

The above means that the invention brings following advantages :

1. The flexibility to define, improve or upgrade applications very easily and quickly by storing them on the ICC, relying on the terminal interpreter for execution and relying on the terminal interpreter core dictionary for definitions.
2. The flexibility to store applications in a compact way on the ICC using dictionaries on the terminal.
3. The flexibility to execute the application in either the ICC, the terminal or both ICC and terminal, depending on the availability of processing power in the ICC and the terminal.
4. The flexibility to allow multiple ICCs to

35

participate in a transaction. The interpreter can be implemented in a terminal with multiple ICC readers.

5 In such a system it is possible to provide applications, either stored on one or more ICCs, a terminal or any combination of terminal and ICCs, that perform ICC to ICC transactions. In this case the terminal could be very simple, only providing the communication means between the ICCs and  
10 possibly providing some dictionaries to reduce the storage requirements on the ICCs.

The ICCs could also provide resources to each other.

5. The flexibility to control the transaction from  
15 both the ICC, the terminal or both the ICC and the terminal.

The transaction is the result of the execution of an application and hence is fully determined by the application program and the associated data  
20 set. As such control of the transaction or parts thereof is determined by the contribution from the ICC, the terminal or both the ICC and the terminal. When the transaction is fully determined by a terminal resident application the card can  
25 only contribute to the application with a data set it contains and then undergoes the transaction . When the transaction is fully determined by the ICC resident application, the terminal contributes to it with its data set and undergoes the transaction.  
30 The terminal and the ICC can also perform the transaction as equals, whereby both determine and perform the transaction . It may occur that the ICC and terminal system is connected to a central unit from which it requests additional services,  
35 in which case the central unit may dynamically



contribute to the application. E.g. the ICC can force the terminal to connect to its central unit and request the update of data on the ICC. The control of the application does not need to be  
5 strictly on the ICC or on the terminal .

In an initial step an application has to be selected for execution on the ICC and terminal system. This selection is trivial when the ICC and the terminal  
10 have no application or exactly one application in common. When multiple applications are supported both by the terminal and by the ICC, the current practice is to let the ICC holder or the terminal operator define interactively which application is chosen. This is not  
15 precluded by the invention which also provides an intelligent mechanism to select the application, depending on ICC parameters, terminal parameters and ICC capabilities and terminal capabilities.

Indeed, after insertion of the ICC in the terminal and  
20 after the ICC has satisfied all compatibility checks, the first action the terminal undertakes is to check whether the ICC supports an application it knows. In order to find this out, the terminal will try to consecutively select one of its resident applications.

25 If an application is present on the ICC, the ICC contains the description of the application. According to the invention, a possible body in the application header is an application select function. This application select function is to be executed by the  
30 interpreter with arguments determined by the ICC. This means that with an application supported by the terminal and defined in the ICC, the selection of one of the many applications only defined on the ICC is made possible . Since the bodies of an application selection function  
35 may be application select functions, the application

may be selected recursively.

5     Example 2 :

          The following example is considered :

          The ICC contains the following applications: Euro, Euro-Debit, Euro-Credit, Us-Debit, Us-Credit. The terminal  
10     only knows the application Euro. When the terminal inspects the ICC, the result of the select application function will be Euro and its related data.

          The definition of application EURO can be stored either on the terminal or in the ICC. Assume it is stored in  
15     the ICC, then it could be defined as follows (in pseudo code):

start

if (ICC amount <100)

    then if (terminal is located in Europe)

20     then select application Euro-Debit  
    else if (terminal is located in US)  
        then select application US-Debit  
        else abort transaction

    else if (terminal is located in Europe)

25     then select application Euro-Credit  
    else if (terminal is located in US)  
        then select application US-Credit  
        else abort transaction

end transaction,

30     wherein

\*     not underlined text means the header, and  
       underlined text means a body.

          In this case, the terminal only knowing EURO can select applications defined in the ICC.

35

Any implementation of the present invention entails the following effort :

- 1 If the ICC is to be used as a mere memory ICC:
  - 5 a) implementing a secure interpreter on the terminal, with its interpreter core dictionary ;
  - b) defining and implementing dictionaries for the application ;
  - 10 c) implementing the application in the interpreter language, possibly making use of available dictionaries ;
  - d) implementing a mechanism to use the ICC dictionaries.
2. If the ICC takes an active part in the execution  
15 of the application:
  - a) implementing a secure interpreter and its core dictionary on the terminal and implementing a secure interpreter and its core dictionary on the ICC .
  - 20 b) defining and implementing dictionaries for the applications ;
  - c) implementing the application in the interpreter language, possibly making use of the available dictionaries ;
  - 25 d) implementing a mechanism on the terminal to use ICC dictionaries.
  - e) implementing a mechanism on the ICC and the terminal to manage the execution of the applications on the ICC and terminal system
  - 30 f) implement a mechanism on the card to use terminal dictionaries.

The invention is obviously not limited to a transaction management system using a card . Many  
35 changes may be made in the shape, the arrangement and

the constitution of the integrated circuit carrier ,  
without departing from the scope of the invention , e.g.  
a key or a badge .

## CLAIMS

1. An integrated circuit controlled transaction management system intended to execute between an ICC and a terminal connected or not to a central unit, a transaction consisting of at least one execution of the following sequence :
1. creating a communication link between the ICC and the terminal ;
  2. performing a compatibility check to ensure that the ICC and the terminal are mechanically and electrically compatible ;
  3. selection of an application contained in the ICC and the terminal, that means the selection of computer program and the associated data set that defines the transaction in terms of the specific ICC and terminal combination present ;
  4. execution of said application on the ICC terminal system, and
  5. termination of the transaction, which optionally includes breaking of the communication link between the ICC and the terminal,
- characterized in that it uses an interpreter which deals with the execution of an application, either on the ICC, or on the terminal or on both, whereby the interpreter in the terminal is able to access and to use at least a part of the terminal memory and at least a part of the terminal peripherals while an optional interpreter in the ICC is able to access and to use at least a part of the ICC memory and at least a part of the ICC peripherals .
2. Transaction management system according to

claim 1, characterized in that each application consists of a number of functions , each function consisting of controlling part referred to as the header and an executable part referred to as the body of said function, both parts of said function possibly being independently stored in a dictionary.

3. Transaction management system according to claim 1, characterized in that functions may be nested.

4. Transaction management system according to anyone of claims 1 to 3, characterized in that a function in the application description is a "select application function" which is executed by the interpreter with arguments determined by the ICC, so that the application select may be executed recursively.

5. Transaction management system according to anyone of the previous claims , characterized in that the interpreter in the ICC is able to access and to use at least a part of the ICC memory and at least a part of the associated ICC peripherals.

6. Transaction management system according to one of the previous claims, characterized in that the interpreter in the terminal is able to access and to use at least a part of the terminal memory and at least a part of the terminal peripherals.

7. Transaction management system according to one of the previous claims, characterized in that the ICC is a mere memory ICC which undergoes the transaction as determined by the terminal .

8. Transaction management system according to one

of the claims 1 to 6, characterized in that the ICC determines the transaction and the terminal which needs only to recognise an application on the ICC and able to select it, undergoes the transaction.

5

9. Transaction management system according to one of the claims 1 to 6, characterized in that the ICC and the terminal both determine and perform the transaction.

10

10. Transaction management system according to claim 8, characterized in that the terminal is a pure interface device between a number of ICCs.

15

11. Transaction management system according to one of the claims 7 to 9, characterized in that each ICC contains a differently personalised application.

20

12. Transaction management system according to one of the previous claims, characterized in that an interpreter is implemented in a terminal with many ICC readers, and provided with applications, either on the ICC, terminal or both, that perform combination of transactions.

25

30

35



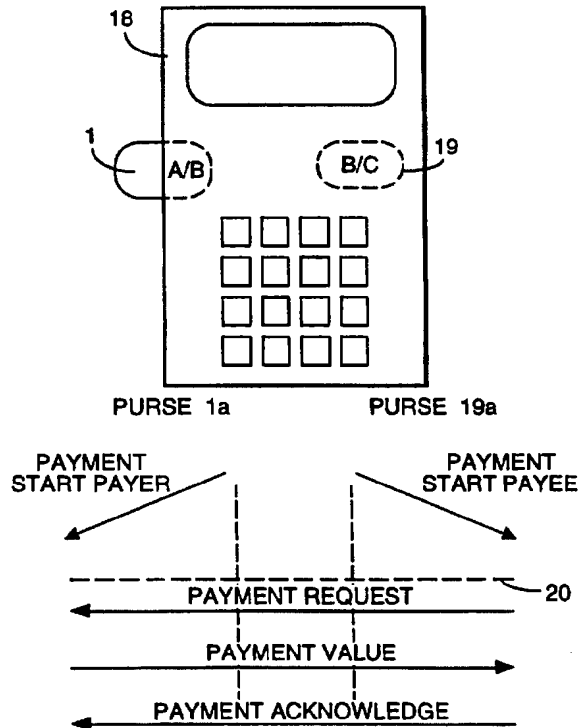
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>G07F 7/10</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 97/02548</b> (43) International Publication Date: 23 January 1997 (23.01.97)</p>
<p>(21) International Application Number: PCT/GB96/01564 (22) International Filing Date: 28 June 1996 (28.06.96) (30) Priority Data: 9513379.9 30 June 1995 (30.06.95) GB (71) Applicant (for all designated States except US): NATIONAL WESTMINSTER BANK PLC [GB/GB]; 41 Lothbury, London EC2P 2BP (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): EVERETT, David, Barrington [GB/GB]; 31 Ashdown Avenue, Brighton, East Sussex BN2 8AH (GB). VINER, John [GB/GB]; "Hydes", Woodlands Lane, Wyndlesham, Surrey GU20 6AN (GB). (74) Agent: BOYDELL, John, Christopher; Stevens, Hewlett &amp; Perkins, 1 Serjeants' Inn, Fleet Street, London EC4Y 1LL (GB).</p>	<p>(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>	

(54) Title: VALUE TRANSFER SYSTEM

(57) Abstract

A value transfer system using integrated circuit cards for exchanging electronic cash in off-line transactions employs cryptographically secure message protocols. Cards are loaded each with two schemes from a series and interaction between cards determines and uses the oldest scheme shared by the cards, causing one card to switch schemes irrevocably if that common scheme is its second scheme. In this way a switch to a new scheme can migrate through the system.





**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LU	Luxembourg	SZ	Swaziland
CS	Czechoslovakia	LV	Latvia	TD	Chad
CZ	Czech Republic	LT	Lithuania	TG	Togo
DE	Germany	LU	Luxembourg	TJ	Tajikistan
DK	Denmark	LV	Latvia	TT	Trinidad and Tobago
EE	Estonia	MC	Monaco	UA	Ukraine
ES	Spain	MD	Republic of Moldova	UG	Uganda
FI	Finland	MG	Madagascar	US	United States of America
FR	France	ML	Mali	UZ	Uzbekistan
GA	Gabon	MN	Mongolia	VN	Viet Nam
		MR	Mauritania		

## "VALUE TRANSFER SYSTEM"

The invention relates to a value transfer system in which value is transferred between electronic purses. One such system is described, for example, in patent application WO 91/16691.

In the system described in the above-mentioned patent specification integrated circuit cards (ICC's) or "Smart Cards" are used as application carrier devices (ACD's) to carry electronic purses. An electronic purse is a program application which controls the storage in memory on the ACD of a value record which represents "electronic cash". By coupling two ACD's together via interface devices (IFD's) the respective purses are coupled together and exchange a series of messages which results in the transfer of value from one purse to the other.

It is clear that security against fraud is vital in a value transfer system. The manufacturing process of ICC's and increasingly sophisticated security measures included in their manufacture and programming make it virtually impossible to counterfeit the smart cards. Interception and duplication of the value transfer messages is prevented by cryptographically encoding messages exchanged in a transaction. In spite of the extremely high security levels achieved by modern cryptography there is a theoretical risk that a particular cryptographic system could be compromised, if not by crypto-analysis then perhaps by a breach of physical security which leads to leakage of algorithms or keys.

An object of the present invention is to provide a value transfer system in which the cryptographic system currently in use may be changed. Administratively, change may be effected as a regular precautionary measure or in response to an attack on the system currently in use.

According to one aspect of the invention there is provided a value transfer system comprising a multiplicity of electronic programmed

microprocessor application carrier devices (ACD's) each comprising an electronic purse having a value store, the ACD's being adapted to be coupled together in pairs so as to couple the purses and enable value to be exchanged in transactions between the purses, said value exchange  
5 being effected by exchanges of messages secured by a cryptographic security scheme, the system further comprising a sequential series of cryptographic security schemes ranging from old to new and each purse being programmed with at least two schemes in said series, the purses being further programmed to identify and use, when coupled in a pair to  
10 exchange value between electronic purses, the older or oldest usable common cryptographic security scheme of the purse pair and to inhibit thereafter as superceded any older cryptographic security scheme of the series in either purse. With this arrangement a first purse can be automatically switched from an old cryptographic system to a new one on  
15 encountering a second purse which has the new system but not the old. On being switched, the first purse will then have no usable old system and then can itself cause other purses to switch to the new system. Thus, by seeding the population of purses with new purses which omit the old cryptographic system, the new cryptographic system will migrate through  
20 the population of purses in a chain reaction.

Preferably each purse has a memory region in which is stored an identifier for the cryptographic security scheme currently in use by the purse, the scheme identifiers being exchanged between a coupled pair of purses as a preliminary in a value exchange transaction.

25 Whilst it is envisaged that the purses may have three or more cryptographic systems to which to be switched in sequence, in a preferred embodiment of the invention each purse is programmed with two successive cryptographic security schemes in the sequential series.

Preferably each cryptographic security scheme comprises at  
30 least one cryptographic algorithm and at least one cryptographic key and

members of the series differ in respect of their algorithms and/or their keys. The above-mentioned patent application describes use of the RSA encryption system, which is an asymmetric public/private key system. Also there is described exchange of keys by means of the DES system.

- 5 The encryption schemes of the present invention may differ from each other because they employ different single encryption algorithms such as RSA or DES or because they combine the algorithms of different systems or because the keys are different.

Successive cryptographic schemes in the series are not  
10 necessarily different. It may be desirable to force current smart cards towards obsolescence by making them switch to a new cryptographic scheme even though it is the same as the old one. Thus, in one embodiment of the invention successive members of the series of cryptographic security schemes are the same except that they are  
15 associated with different scheme identifiers, the scheme identifiers being stored in the purses and being used to identify the oldest common cryptographic scheme of a pair of coupled purses and to control the inhibition of any older cryptographic security scheme of the series in either purse.

20 Furthermore, selected ACD's may be provided with two electronic purses programmed with respective and different cryptographic security schemes, said selected ACD's being programmed, on being coupled to another ACD, to select a purse so as to allow a transaction between the purse of the said other ACD and the selected purse according  
25 to compatibility of the purse cryptographic security systems.

According to another aspect of the invention there is provided a value transfer system comprising a multiplicity of electronic programmed microprocessor application carrier devices (ACD's) each comprising an electronic purse having a value store, the ACD's being adapted to be  
30 coupled together in pairs so as to couple the purses and enable value to

be exchanged in transactions between the purses, said value exchange being effected by exchange of messages secured by a cryptographic security scheme, wherein selected ACD's are provided with two electronic purses programmed with respective and different cryptographic security schemes, said selected ACD's being programmed, on being coupled to another ACD to select a purse so as to allow a transaction between the purse of the said other ACD and the selected purse according to compatibility of the purse cryptographic security systems. With this arrangement it is possible to provide a cut-off strategy for a particular cryptographic scheme or set of schemes. By providing selected purses, for example retailers and banks, with dual purse smart cards (ACD's), one purse having the old schemes and the other purse having new schemes, it is possible to isolate "old money" from "new money" while allowing transactions with the old schemes to continue, perhaps for a limited time.

The invention will further be described with reference to the accompanying drawings, of which:-

Figure 1 is a schematic diagram of an application carrier device in the form of an integrated circuit card (ICC) in a system according to the invention;

Figure 2 is a diagram illustrating memory allocation in an electronic purse loaded on the ICC of Figure 1;

Figure 3 is a diagram illustrating a value transfer transaction between two purses of a system in accordance with the invention; and

Figure 4 is a diagram illustrating a purse arrangement for effecting cryptographic cut-off in a system in accordance with the invention.

It is to be understood that the present invention is a development of the value transfer system described in patent application No. WO 91/16691. That specification describes the use of ICC's as application carrier devices for carrying electronic purses. The electronic purses have records of various kinds held in electrically erasable

programmable read-only memory (EEPROM) including value records for holding value, log records etc. The purse may be coupled via interface devices to exchange value in accordance with protocols involving the exchange of cryptographically secure messages. Electronic cash may thus be withdrawn from a bank, exchanged in off-line transactions with, for example, retailers and redeemed at a bank. For the sake of brevity many of the technical details of the system will not be repeated herein but where necessary reference may be made to the above-mentioned earlier patent specification.

Figure 1 illustrates an application carrier device (ACD) in the form of an ICC 1. The ICC has on one surface a contact pad 2 carrying several separate electrical contacts whereby an external power source may be connected to power the card and a serial communication channel may be established to transmit data to and from the card. The card includes a microprocessor 3, an EEPROM 4 and a random access memory 5.

The EEPROM 4 holds an operating system which comprises three sub-systems: (a) a file manager; (b) a run-time executive; and (c) a BIOS (binary input/output system). When loaded, the operating system is used to load into the EEPROM an electronic purse, which is an application, namely a program with associated data files.

Figure 2 shows some of the elements of an electronic purse as schematic allocations of regions of the EEPROM. Operation of the purse is controlled by a program at 6 which has associated data files. For example there is a value record at 7, transaction logs at 8 and a unique purse identifier at 9. Security is maintained by the use of cryptographic schemes and this purse holds two schemes. Scheme A has algorithms at 10 and a set of cryptographic keys at 11. Scheme B has algorithms at 12 and a set of cryptographic keys at 13. A crypto file 14 includes three single-byte fields: cut-off domain 15; migration level 16 and migrated flag

17.

The value of the cut-off domain byte indicates the particular cut-off domain in which the purse exists. Purses of different domains do not communicate with each other. Thus, if a major change in the system is deemed desirable from a particular cut-off date then all new purses from that date will have a new cut-off domain byte at 15. In a particular domain, a series of cryptographic schemes is defined. For example, in the first domain there may be the series A, B, C, D, E where A is the first, or oldest scheme to be used and E is the last, or newest in the series. Each purse includes two successive schemes of the series. The first set of purses will include schemes A and B, which can be termed respectively the initial and final schemes for this purse. This set of purses may be called Issue 1. The migration level byte 16 holds, for example, "A" which indicates that the purse includes schemes A and B, namely that this purse is Issue 1 in the cut-off domain. In a manner to be described, the purse can be irrevocably switched from using scheme A to using scheme B. The value of the migrated flag byte 17 indicates whether this switch has taken place. Thus, by reading bytes 15 to 17 the particular cryptographic scheme currently in use by the purse can be determined.

20                   When two purses, X and Y, communicate for a value transfer the security schemes used are determined by the following rules:-

- i)       If the current schemes of X and Y are the same then this scheme is used, and no scheme changes take place;
- ii)      If the current schemes of X and Y differ, are adjacent in the cryptographic series, and if the earlier of the two schemes is the initial scheme for the purse to which it belongs, then a permanent switch is made in the purse using its initial scheme so that it will always use its final scheme from now on. Thus the 'final' scheme is designated the current scheme, and the initial scheme on this purse is never used again.

- iii) If neither (i) nor (ii) holds, then the purses cannot communicate. The value transfer cannot take place, and no change is made to the security scheme of either.

It will be seen that value transfers between Issue 1 purses  
5 take place using scheme A, since this is the oldest common scheme of the  
two purses. When it is required to phase out Scheme A an issue 2 of  
purses is released containing schemes B and C. When a value transfer  
takes place between an Issue 1 and an Issue 2 purse rule (ii) comes into  
play and an irreversible switch is made in the Issue 1 purse to use scheme  
10 B from now on. Then, the Issue 1 purse becomes an agent for change  
itself, since when a value transfer takes place between it and another Issue  
1 purse, which has not been switched to scheme B, then rule (ii) again  
comes into play and the second Issue 1 purse is switched to scheme B.  
The switching is effected by changing the migrated byte 17 in the  
15 EEPROM.

Gradually, by a process of osmosis, the Issue 1 purses  
switch over to scheme B. The changeover will be quite rapid if Issue 2 is  
released widely (to retail outlets for example), though in theory one purse  
could be sufficient to trigger the whole process.

20 A change from B to C is carried out in the same way by  
creating an Issue 3 with schemes C and D. Once this Issue, and hence  
scheme C, are established, Issue 1 purses are no longer usable.

Note that the switchover does not depend in any way on  
dates. This is deliberate as dates cannot necessarily be relied on, and  
25 clocks are not mandated for all equipment. No decision on the life of a  
scheme needs to be taken when the purses containing it are issued.

Figure 3 shows a point-of-sale terminal 18 at a retailer site.  
Terminal 18 is an interface device and holds the retailer's ICC 19 which  
includes the retailer purse 19a. The customer ICC 1 of Figures 1 and 2  
30 can be inserted into a slot in the body of the terminal 18. In this example



the customer card 1 has a purse 1a with schemes A and B and the retailer card 19 has a purse 19a with schemes B and C.

As described in the above-mentioned earlier patent specification a value transfer transaction includes three essential  
5 cryptographically signed messages:-

- (a) Request to Send - from the payee (retailer) purse to the payer (customer) purse requesting an agreed value V.
- (b) Payment value - from the payer purse to the payee purse  
10 including the payment command to pay V.
- (c) Payment Acknowledge - from the payee purse to the payer purse to acknowledge receipt of value V.

These are the payment messages and as described in the earlier patent specification these are cryptographically signed and verified.  
15

Before the payment phase in which the payment messages are sent there is a pre-payment phase in which information is exchanged between the purses concerning purse status. This information is transmitted in clear, i.e. non-cryptographically. Data received at this stage by one purse from the other purse is "counterparty purse data".

20 Referring to Figure 3 a sequence of messages is shown for the transaction between the customer purse 1a and the retailer purse 19a. Messages above line 20 are pre-payment messages sent in clear and messages below line 20 are cryptographically signed. Firstly, by sending interrogation commands to both purses the terminal 18 derives responses  
25 which contain purse status information. Included in the purse status information is the value of bytes 15 to 17 which collectively indicate the current cryptographic scheme of the series A to E under which each purse is operating.

Purse 1a receives a "Payment Start Payer" message from the  
30 terminal 18 and from counterparty purse data it determines that purse 19a

is currently on scheme B and deduces that it (purse 1a) will migrate to scheme B.

Purse 19a receives a "Payment Start Payee" message from the terminal 18 and from counterparty purse data it recognises that purse 5 1a is currently at scheme A and will migrate to scheme B. Purse 19a sends a Payment Request message based on scheme B and containing information as to the value of bytes 15 to 17 in its EEPROM. Purse 1a expects purse 19a to be using scheme B. It checks the Payment Request signature using scheme B. As part of checking the incoming signature, it 10 checks that purse 19a has a correct understanding of what migration will occur - i.e. purse 1a will migrate and purse 19a will not. In this way any anomalies can be resolved. For example, it is not possible for both purses to migrate. If this should be indicated then the transaction is aborted and neither purse migrates. If the Payment Request signature is valid purse 15 1a migrates irrevocably to scheme B by setting byte 17 in its EEPROM.

Purse 1a sends a Payment Value message to purse 19a. This is cryptographically signed and includes information concerning bytes 15 to 17, showing that the purse 1a has migrated to scheme B. Purse 19a uses scheme B to check the signature from purse 1a. Finally, purse 19a 20 sends a Payment Acknowledge message to purse 1a, signed cryptographically and including again information concerning its bytes 15 to 17. Thus, it is to be noted that scheme status information is firstly exchanged in clear between the purses and is then incorporated in all three of the basic cryptographically signed payment phase messages. 25 The information in these signed messages is derived internally within the ICC and cannot be simulated externally in an attempt to fraudulently force scheme migration.

A similar procedure to that described above takes place when the cryptographic scheme of the payee purse is to be caused to migrate 30 because of a transaction with a customer purse with a newer current

scheme. Here migration is effected in the payee purse on receipt of a valid signed Payment Value message.

While the above description relates to progressive migration to successive cryptographic schemes there may be occasions when it is necessary to implement cut-off. Cut-off is a strategy for abandoning all cryptographic schemes hitherto in use in a system and re-starting with a new cryptographic scheme or series of schemes. Cut-off may be necessary, for example, to force re-call of existing ICC's if a significant improvement in the system is to be implemented or if a serious breach of security is discovered.

In order to implement cut-off special ICC's would be introduced into the scheme. The EEPROM of one such ICC is shown in Figure 4 at 21. The EEPROM has two purses 22 and 23, each with two cryptographic schemes.

In the event of a security breach, the two purses would have schemes belonging to an "old" and a "new" series and the two series would be totally distinct and non-overlapping. However, if the system is not cryptographically compromised and cut-off is introduced for administrative reasons it is possible that the two series could be the same. However, the two purses belong to different cut-off domains and have different respective values in byte 15. The programs of the purses will therefore not recognise any common cryptographic scheme with another purse having a different cut-off domain value, since this value is part of the cryptographic scheme identifier. Thus, purses may exchange value only with purses of the same cut-off domain. Selection of which purse to use in ICC 21 is made by a program routine which identifies the value of byte 15 in the customer purse from the counter party purse data.

The provision of retailer cards with two purses of different domains allows transactions to continue with old purses while new cards are introduced. This period of overlap can be time-limited. The

consequence of the arrangement is that electronic cash issued under the original domain is isolated from that under the new domain so that any damage to the system as a whole may be limited.

CLAIMS

1. A value transfer system comprising a multiplicity of electronic programmed microprocessor application carrier devices (ACD's) each  
5 comprising an electronic purse having a value store, the ACD's being adapted to be coupled together in pairs so as to couple the purses and enable value to be exchanged in transactions between the purses, said value exchange being effected by exchanges of messages secured by a cryptographic security scheme, the system further comprising a sequential  
10 series of cryptographic security schemes ranging from old to new and each purse being programmed with at least two schemes in said series, the purses being further programmed to identify and use, when coupled in a pair to exchange value between electronic purses, the older or oldest usable common cryptographic security scheme of the purse pair and to  
15 inhibit thereafter as superseded any older cryptographic security scheme of the series in either purse.
2. A value transfer system as claimed in claim 1 wherein each purse has a memory region in which is stored an identifier for the cryptographic security scheme currently in use by the purse, the scheme  
20 identifiers being exchanged between a coupled pair of purses as a preliminary in a value exchange transaction.
3. A value transfer system as claimed in either of the preceding claims wherein each purse is programmed with two successive cryptographic security schemes in the sequential series.
- 25 4. A value transfer system as claimed in any of the preceding claims wherein each cryptographic security scheme comprises at least one cryptographic algorithm and at least one cryptographic key and members of the series differ in respect of their algorithms and/or their keys.
5. A value transfer system as claimed in any of the preceding  
30 claims wherein successive members of the series of cryptographic security

schemes are the same except that they are associated with different scheme identifiers, the scheme identifiers being stored in the purses and being used to identify the oldest common cryptographic scheme of a pair of coupled purses and to control the inhibition of any older cryptographic security scheme of the series in either purse.

5

6. A value transfer system as claimed in any of the preceding claims wherein selected ACD's are provided with two electronic purses programmed with respective and different cryptographic security schemes, said selected ACD's being programmed, on being coupled to another ACD to select a purse so as to allow a transaction between the purse of the said other ACD and the selected purse according to compatibility of the purse cryptographic security systems.

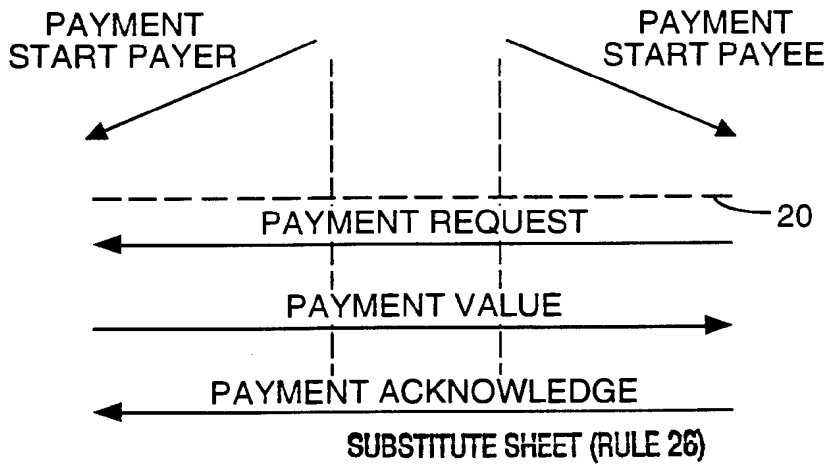
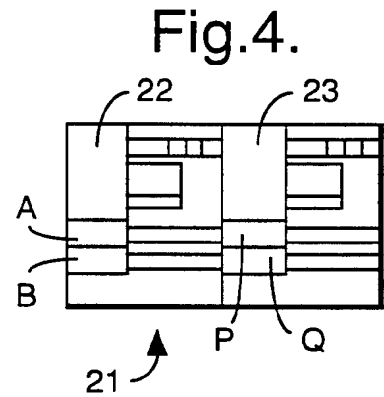
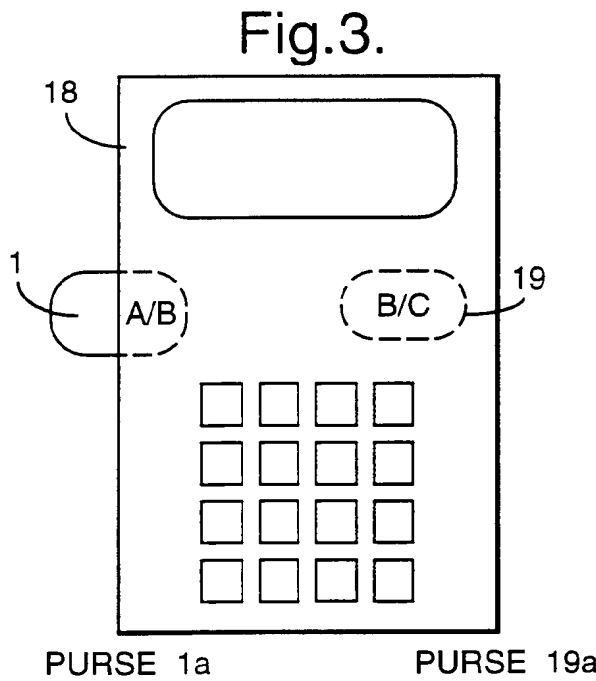
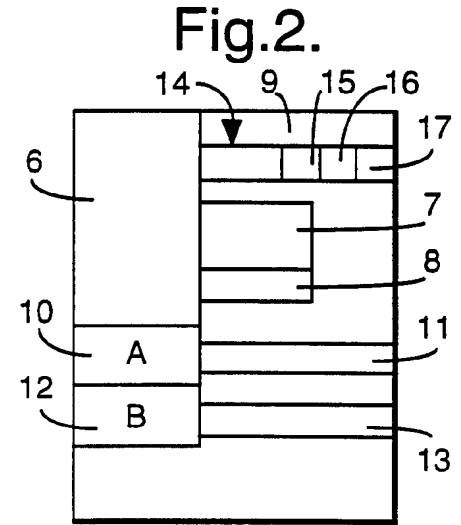
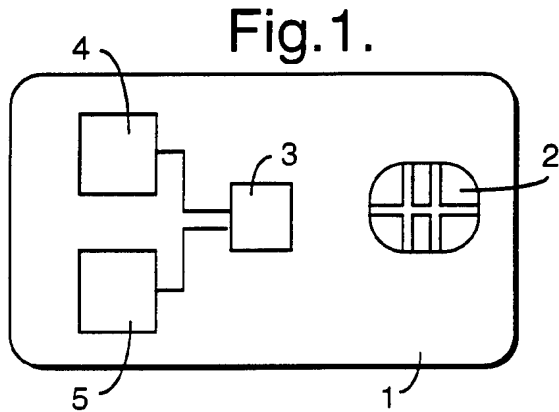
10

7. A value transfer system comprising a multiplicity of electronic programmed microprocessor application carrier devices (ACD's) each comprising an electronic purse having a value store, the ACD's being adapted to be coupled together in pairs so as to couple the purses and enable value to be exchanged in transactions between the purses, said value exchange being effected by exchange of messages secured by a cryptographic security scheme, wherein selected ACD's are provided with two electronic purses programmed with respective and different cryptographic security schemes, said selected ACD's being programmed, on being coupled to another ACD to select a purse so as to allow a transaction between the purse of the said other ACD and the selected purse according to compatibility of the purse cryptographic security systems.

15

20

25





INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

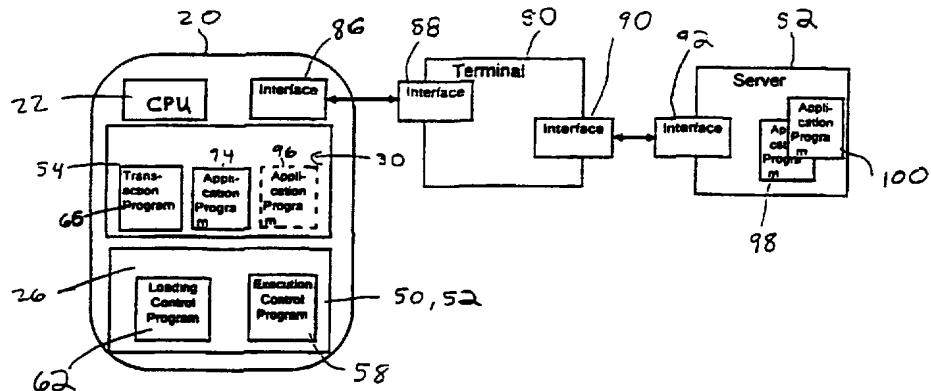
<p>(51) International Patent Classification <sup>6</sup> : <b>G07F 7/10</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 98/09257</b> (43) International Publication Date: 5 March 1998 (05.03.98)</p>
<p>(21) International Application Number: PCT/IB97/01042 (22) International Filing Date: 29 August 1997 (29.08.97) (30) Priority Data: 08/706,396 30 August 1996 (30.08.96) US (71) Applicant: GEMPLUS S.C.A. [FR/FR]; Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, Boîte postale 100, F-13881 Gémenos (FR). (72) Inventors: LISIMAQUE, Gilles; Gemplus S.C.A., Z.I. Athélia III, Voie Antiope, F-13705 La Ciotat (FR). PEYRET, Patrice; Gemplus S.C.A., Z.I. Athélia III, Voie Antiope, F-13705 La Ciotat (FR). (74) Agent: NONNENMACHER, Bernard; Gemplus S.C.A., Z.I. Athélia III, Voie Antiope, F-13705 La Ciotat (FR).</p>		<p>(81) Designated States: AT, AU, CA, CN, RU, SG, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). <b>Published</b> <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>

(54) Title: A SYSTEM AND METHOD FOR LOADING APPLICATIONS ONTO A SMART CARD

(57) Abstract

A system for loading an applet and its associated use rights into a smart card having other applets with associated use rights with values that change as the application is used is provided that stores, remotely from said smart card, an applet and use rights with a predetermined initial value, associated with the applet, and has a smart card having a processing unit, and a memory unit, the memory unit being connected to the processing unit and storing a second application having use rights. The smart card may be connected to said remote storage means, and the application, having use rights with a predetermined value, may be loaded from said remote storage means into said smart card. A smart card is also provided having a

processor for executing an application, a memory, connected to the processor, for storing multiple applications, including a first application having first use rights and having first values associated with the first use rights, the first value changing from a predetermined initial value with use of the first use rights, a system for loading in the smart card a second application from a remote location over an interface, the second application having second use rights, a system for storing said second application into said memory in said smart card, and a system for changing the use rights of said first application and said second application. A method of replenishing the use rights in a smart card is also provided.





**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

A SYSTEM AND METHOD FOR LOADING APPLICATIONS ONTO  
A SMART CARD

5

Background of the Invention

This invention relates generally to secure portable tokens, such as smart cards and in particular to smart cards having reloadable applications.

10

As is well known, a smart card may be a plastic, credit card-sized card containing a semiconductor chip, such as a microprocessor built into the smart card so that it may execute some simple application programs, which may be referred to as applets. Some examples of the applications in a smart card include security and authentication, information storage and retrieval, and credit and debit operations for managing value accounts, such as prepaid phone time and debit accounts. Each value account application on the smart card has a particular type of use rights associated with the application. For example, a prepaid phone time application may have a predetermined number of prepaid phone minutes that are used up as phone calls are made with the card, and a prepaid public transit account may have an initial preset monetary values which is debited with each use of public transportation. To store and execute these applets, these smart cards have a built-in memory and processor. In order to ensure the security of the use rights on these smart cards, only the processor within the smart card may ordinarily alter the value of the use rights, and only after an authorization sequence has been successfully conducted. The network in which the smart card

15

20

25

is being used does not have any direct access to the memory of the smart card nor to the use rights of any application.

5 There are generally two different types of smart cards, i.e., disposable smart cards and permanent, non-disposable smart cards. A disposable smart card may have a rudimentary semiconductor chip embedded within the smart card and may have a limited amount of memory and some hardwired logic. The disposable smart cards may have a predetermined initial amount of prepaid use rights or other value stored in the memory of the smart card established when  
10 the smart card is manufactured. The prepaid use rights are then depleted as the smart card is used. A prepaid phone card or a subway fare card are examples of disposable smart cards because these smart cards are thrown away after the prepaid use rights are depleted. These disposable smart cards are inexpensive because of the rudimentary semiconductor chip, but they have limited utility  
15 since their stored value cannot be replenished, and other applications cannot be installed on them. Due to the limited memory and processing power, these disposable smart cards also cannot execute sophisticated cryptographic algorithms, which means that these disposable smart cards are less secure.

20 The non-disposable, permanent smart cards may have a more complex semiconductor chip embedded within the card, and may have a programmable micro-controller and an expanded memory. The memory may store one or more applets that have separate predetermined amounts of use rights for different

functions. Importantly, these permanent smart cards have use rights that may be replenished so that the permanent smart card need not be discarded once the use rights are depleted. Examples of these permanent smart cards include banking cards according to the Europay/Mastercard/Visa standard, and pay television access control cards. These permanent smart cards have more memory for storage of multiple applets and the use rights on the smart card may be separately and independently replenished. However, these permanent smart cards are also more expensive due to the additional memory and the micro-controller, and the replenishment can only be performed by the card issuer.

Initially, many companies issued disposable smart cards due to the lower initial investment. However, due to the security concerns of these disposable smart cards and the limited applications that may be run on these disposable cards, the current trend is to use permanent smart cards because several applications may be loaded onto a single permanent smart card. The permanent smart card is also more secure because more sophisticated cryptographic techniques may be used.

Most conventional permanent smart cards may have a memory unit that may include a read only memory (ROM), a random access memory (RAM), and a non-volatile memory (NVM). The NVM may be, for example, a flash memory such as a flash electrically erasable programmable read only memory (Flash EEPROM), or a EEPROM. These permanent smart cards receive all of their

5 electrical power from the terminal to which they are connected during use. As a consequence, the RAM, which is volatile memory, may be used only as a scratch pad memory for simple computations that do not need to be stored. The ROM, which is permanent, may store the operating system (OS) of the smart card and other programs which do not need to be updated or changed, such as certain permanent applets. The NVM may store certain applets and the use rights secrets or values associated with all applications in the smart card. These conventional permanent smart cards may have multiple applications that reside in the memory of the smart card.

10 Some conventional permanent smart cards have fixed application programs that are stored in the ROM at the time that the smart card is manufactured. These smart cards do not permit any applications to be stored in the NVM due to security concerns. The programs that are stored in the ROM cannot be altered. The applications for these ROM-based smart cards, however, take a great amount of time to develop because the application must be developed and then be hard wired into the ROM. In addition, these fixed applications are not changeable or removable.

20 To solve the problems of a fixed application in the ROM, some current smart cards permit applications to be stored in the NVM. However, handling of applications and their associated use rights in the NVM of the smart card poses several problems.

5 First, there is a security problem since access to the application within the NVM may also permit access, by a clever individual, to the other applications within the NVM unless carefully controlled. In addition, a clever person may figure out a way to replenish his use rights illegally as they are also stored in the NVM. This is an especially large problem for banks that want to issue debit or electronic purse cards since a person could replenish the money available on the smart card without debiting his bank account. For a bank, it is desirable that no one, but the bank have access to the use rights within the smart card. This means that the use rights of any applet on a smart card may only be replenished  
10 by the card issuer, such as the bank, which may be inconvenient. In addition, any other company with applets on that smart card must have a relationship with the card issuer.

15 Second, the replenishing of the use rights of an applet in the smart card may be slow because there must be a number of security procedures that must be followed when use rights are being changed. For example, there must be several authentication procedures to ensure that no illegal activities are occurring.

20 Third, since each type of application may have a different type of use rights in various different units, such as phone minutes in time units versus cash in monetary units, each different application will probably require a different use rights reload procedure. For example, a use rights reload procedure for phone

minutes may not be able to replenish the cash of a debit account on a smart card. Thus, procedures that loads use rights into the smart card must be duplicated.

To limit access to these use right values, conventional permanent smart cards have done several different things. First, some conventional permanent smart cards have controlled the access to certain areas of memory, known as memory zones, so that these memory zones are write-once areas. Other conventional permanent smart cards use a data dictionary, which keeps track of the memory areas in which each of the application must reside. Thus, some sort a memory management system must constantly verify that none of the applications are doing illegal activities.

In summary, some conventional permanent smart cards do not allow any applications to reside in the NVM to reduce security risks. Other conventional permanent smart cards have systems for replenishing the use rights of an application contained on a smart card, but limit this capability to the issuer of the smart card, and require separate loading procedures for each applet. None of these conventional smart card systems provide a system for loading an entire application of any type, including the use rights, into the memory of a permanent smart card. Accordingly, conventional smart cards cannot store disposable applications, such as a prepaid telephone time applet, because there is no method for removing the disposable application once it is depleted or replacing the disposable applet with a new applet. Thus, in conventional smart cards, these

depleted disposable applications would remain in the smart card taking up valuable memory space. For this reason, most permanent smart cards today do not have any ability to handle disposable applications.

5           Thus, there is a need for a system and method for universally reloading different types of use rights in multiple application smart cards which avoid these and other problems of known devices, and it is to this end that the present invention is directed.

10           Summary of the Invention

          The invention provides a smart card, as well as a system and method for loading applications into the memory of a smart card which may load any type of application and its associated use rights, wherein the use rights may have any  
15           type of units. In addition, the system may load one or more disposable applications onto a permanent smart card since those disposable applications, once depleted, may be replaced with a new applet.

          The invention also provides an applet loading system for a smart card  
20           wherein the use rights associated with an applet may be replenished by reloading the applet and the use rights into the memory of the smart card. The system for loading applications into a smart card may be universal so that a single loading system may be used for a variety of applications. In accordance



with the invention, a system and method for reloading applications within a smart card is provided wherein the system may have a storage, remotely from said smart card, that stores an applet and use rights with a predetermined initial value, associated with the applet, and has a smart card having a processing unit, and a memory unit, the memory unit being connected to the processing unit and storing a second application having use rights. The smart card may be connected to said remote storage means, and the application, having use rights with a predetermined value, may be loaded from said remote storage means into said smart card. A smart card is also provided having a processor for executing an application, a memory, connected to the processor, for storing multiple applications, including a first application having first use rights and having first values associated with the first use rights, the first value changing from a predetermined initial value with use of the first use rights, a system for loading in the smart card a second application from a remote location over an interface, the second application having second use rights, a system for storing said second application into said memory in said smart card, and a system for changing the use rights of said first application and said second application. A method of replenishing the use rights in a smart card is also provided.

Brief Description of the Drawings

Figure 1 is a block diagram of a smart card with which the invention may be employed;

5 Figure 2 is a block diagram depicting the creation of a program that may run on the smart card of Figure 1;

Figure 3 is a block diagram of the memory organization of the smart card of Figure 1;

Figure 4 is a block diagram of a preferred system for reloading applications onto a smart card;

10 Figure 5 is a block diagram of a first embodiment of a method in accordance with the invention of reloading an application into a smart card;

Figure 6 is a block diagram of a second embodiment of a method in accordance with the invention of reloading an application into a smart card;

15 Figure 7 is a block diagram of a third embodiment of a method in accordance with the invention of reloading an application into a smart card;

Figure 8 is a flowchart of a method of debiting use rights in a smart card; and

Figure 9 is a flowchart of a method of replenishing the use rights of an application within a smart card in accordance with the invention.

20

Detailed Description of a Preferred Embodiment

The invention is particularly applicable to a system and method for reloading applications having use rights onto a permanent smart card so that the

use rights of the application may be replenished when they have been depleted. It is in this context that the invention will be described. It will be appreciated, however, that the system and method in accordance with the invention has greater utility.

5

10

15

20

Figure 1 is a block diagram of a smart card 20, also known as a token, of the type with which the invention may be employed. The smart card may be used in connection with the system and method of loading applications into a smart card in accordance with the invention. The smart card may preferably be a permanent smart card, but may also be a disposable smart card. This smart card 20 may have a processor or CPU 22 and a memory 24. The memory may comprise a read only memory (ROM) 26, a random access memory (RAM) 28, and a non-volatile memory (NVM) 30. The NVM may be any type of writable nonvolatile memory, such as an electrically erasable, programmable read only memory (EEPROM), a battery backed RAM, or a flash memory, that can retain stored data when no electrical power is supplied to the memory. The ROM may preferably store the operating system (OS) which controls the operation of the CPU of the smart card, and the RAM may be used as a temporary scratchpad memory. Because the smart card receives its electrical power from the terminal into which it is inserted, as described below, all of the contents of the RAM will be lost when the smart card is removed from the terminal. The NVM may preferably be used to store one or more applications which may be referred to as applets due to the small size of the actual program code. Each of these applets

may have associated use rights which are specific to the applet. Other permanent applications that do not change, such as a credit/debit program, may be stored in the ROM.

5           The processor 22 controls the operation of the smart card. The processor may be connected to all of the memories within the memory system 24. Since there are use rights associated with an application, there is a need to make the smart card secure to prevent theft or alteration of the use rights. To accomplish this security, the processor is the only system that is capable of accessing any of  
10 the memories. There is no direct access to any of the memories from outside of the smart card. In addition, any outside access to the memories of the smart card must be conducted through an input/cutput (I/O) line 32 that is connected to the processor 22. The smart card may also have more than one I/O line provided that access to each I/O line is carefully controlled so that there is no direct access  
15 to any of the memories from outside of the smart card. Thus, the processor may authenticate and validate incoming requests prior to making any change in the use rights of an application stored in the smart card, and may prevent unwanted or illegal attempts to decrease the use rights of an application. This authentication and validation may be conducted using cryptographic systems,  
20 such as public key encryption, or any other security system. Now, a preferred system for generating applets for a smart card will be briefly described.

Figure 2 is a block diagram showing the architecture of the smart card and the manner in which an applet is generated for the smart card. To provide sufficient security for the smart card, a preferred embodiment of a smart card may have a virtual machine 40 contained within the smart card. The virtual machine is comprised of a software interpreter 42 running on the hardware processor 22. The interpreter is a piece of software that acts as an interface between the hardware processor and the applets. In this manner, the applets run through the interpreter so that the applets do not have any direct access to the hardware of the smart card. Thus, the interpreter may verify that none of the applets are performing illegal operations. Instead of a complete interpreter and virtual machine, the smart card may have a command dispatcher to control the access of the applets to various portions of the smart card. The dispatcher may control access of the applets to the hardware by preventing the applets from receiving any access until an authentication check has been completed. A command dispatcher may be considered to be a reduced version of a general interpreter, and the command dispatcher interprets commands received from the applications instead of interpreting the entirety of the code of the applications.

To execute an applet on an interpreter, as shown, source code 46 of an applet is compiled into a byte code 48. The byte code may then be executed by any interpreter on any smart card. The details of the architecture of the preferred smart card are set forth in more detail in PCT Application No. PCT/NL95/00055, published as International Publication No. WO 95/22126, which is incorporated

herein by reference. The organization of programs within the memory of the smart card will now be described.

Figure 3 is a block diagram of the memory organization of the smart card 5 20 that may include a system for loading applets into the smart card in accordance with the invention. The memory 24 of the smart card, which may include the ROM and NVM, may be logically organized into an OS layer 50, an executive layer 52, and an application layer 54. The OS layer may contain the most basic operating software, such as a cryptographic library 56, and an 10 interpreter 58. These programs are permanent and may be stored in the ROM. The cryptographic library may be used for authenticating access to the smart card, as described above. The interpreter 58, as described above, may be used to prevent an applet from directly accessing the hardware of the smart card.

15 The executive layer 52 may contain, for example, an application launcher 60, a conditional application loader 62 in accordance with the invention, and other OS sub-systems 64. The application launcher receives a request to access an application, and after appropriate authentication, launches and controls the applet. The conditional application loader 62 controls the loading of an 20 application, or applet, into the NVM of the smart card. The application loader may verify that the remote system desiring to load an applet into the smart card has the appropriate authority, and then may perform the necessary operations, as

described in more detail below, to load the applet into the NVM of the smart card.

5 The application layer 54 may contain a permanent application 66 and one or more disposable applications 68 having associated use rights. The permanent application may be stored in the ROM since it is permanent and may be a credit/debit system that performs all of credit and debit transactions for all of the disposable applications having use rights within the smart card. The credit/debit system may operate with any type of use rights so that only a single credit/debit application is needed for each smart card. In this manner, the use rights of any applet within the smart card may be changed by the permanent credit/debit application 66. In a preferred embodiment of the invention, the loader 62 and the credit/debit application 66 may be a single program since both programs operate on all of the applets having use rights. For example, an applet with use rights needs the credit/debit application to authorize the reload if the applet 10 when the use rights have been depleted, as described below.

15 The disposable application 68 may be any type of application or applet with a limited lifetime, as defined by a certain number of use rights, such as a predetermined number of telephone call minutes, a predetermined amount of money, or a predetermined number of store credits. As described below in more detail, conventional smart cards that replenished the use rights of a particular application require a separate use rights loading system for each different 20

application because the use rights of each application may require different handling and security. For example, replenishing a certain number of store frequent buyer points onto a smart card may be different than replenishing the cash value of a debit applet, such as a point-of-sale applet, in the smart card. In addition, in order to replenish the use rights of any applet, the smart card needed to be physically connected with or returned to the card issuer since only the card issuer had the authority to alter the use rights for an applet. Therefore, every company who may have an applet on the smart card, must have a relationship with the card issuer so that the card issuer can replenish the use rights of that applet.

Significantly, however, the smart card in accordance with the invention may have a universal applet loader that may delete and then reload an entire applet instead of establishing a connection between the smart card and the applet issuer who then just reloads the use rights. Reloading the entire applet into the smart card means that the loader does not have to be specialized to handle the multiplicity of different types of use rights which could be present in the smart card since the entire applet, including the use rights, is being reloaded into the smart card. The loading of an applet into a smart card to permit the replenishment of the use rights of an applet will be described in more detail below.



The universal loader 62 in accordance with the invention may also be used to load new applets into a smart card, provided that the smart card has available memory. In addition, the universal loader may also permit an applet with depleted use rights to be deleted from the memory of the smart card and replaced with a new different application having refreshed use rights. Each of these operations will be described in more detail below. A preferred system, external to the smart card, for loading applets having use rights, into the smart card will now be described.

Figure 4 is a block diagram showing a system in accordance with the invention for loading an applet having use rights into a smart card. The system may include the smart card 20, a terminal 80, and a server 82. The smart card 20 is described above with reference to Figures 1-3. The terminal may be operated by the smart card issuer, or by some other entity, such as a bank. The terminal may be a bank ATM teller, a terminal in a bank or a home computer system. The server may be maintained by a bank or the issuer of the smart card, and may contain downloadable applets. The connection between the terminal and the server may be any conventional network, such as the usual connection between ATM machines across the world.

As described above, the smart card may have the processor 22, the OS layer 50 and the executive layer 52 stored in the ROM 26, and the applications layer 54 stored in the NVM 30. In addition, the smart card may have an interface

system 86 that may connect the smart card to the terminal 80 using a corresponding interface 88. A second interface 90 may connect the terminal to the server 82 via an interface 92. Thus, the smart card may be connected, through the terminal, to the server. A preferred method of loading an application into the smart card will now be described.

When the smart card is connected to the terminal, the processor 22, using the loader 62, verifies the authenticity of the terminal and of the server. The terminal and the server may also verify the authenticity of the smart card. For example, when the smart card is connected to the terminal, the user may enter a personal identification number (PIN) that may be verified by the server. As another example, the server may send a coded word that must be correctly answered by the smart card. If the server and the smart card authenticate each other, then the universal loader 62 within the smart card begins the loading process. The applets stored on the server, regardless of the type of use rights, may all have a common structure so that the universal loader does not have to distinguish between different types of applets except to identify which one(s) to load. As shown, the NVM 30 may currently store the permanent credit/debit application 66, and an existing first applet 94 with use rights. After the loading operation, as described below, the NVM memory may also have a second new applet 96 with use rights. In the smart card shown, the use rights of the first applet 94 have been depleted. Therefore, a new copy of the applet 98 with refreshed use rights, located on the server 82, may be loaded into the NVM of the

smart card. The applet 98 with refreshed use rights replaces the original applet 94 with depleted use rights.

In addition to the replenishment of use rights, a new 100 applet having use rights may be loaded into the smart card 20 from the server 82 in a similar manner. Therefore, after the load process is complete, the smart card may have a first applet with replenished use rights, and the new second applet 96 with predetermined use rights. As an example, a smart card that has a telephone call applet with depleted use rights may have a new telephone call applet with refreshed use rights as well as a debit applet with a predetermined value, e.g., \$100, loaded onto the smart card. The connections between the terminal 80 and the server 82 may be conventional network system that may be used for home banking and the like. Several examples of loading applets into a smart card, in accordance with the invention, will now be described.

As described above, conventional smart cards replenish the use rights of an applet by reloading new use rights into an applet on the smart card. The problems with reloading the use rights of an applet into a smart card have been described above. Now, several examples of the operation of the applet loading system in accordance with the invention will be described.

Figure 5 is a block diagram of the loading system in accordance with the invention being used to replenish the use rights of an applet within a smart card.

As shown, the smart card 20 may have, for example, a first applet 102, a second applet 104, and a third applet 106. In this example, the first and third applets have use rights remaining, whereas the second applet needs to have its use rights replenished. In accordance with the invention, a new second applet 108 with replenished use rights is loaded into the smart card 20 and replaces the old second applet 104. Thus, after the loading process, the smart card may have a first applet 102, a third applet 106, and a new second applet 108 with replenished use rights. As shown, only the second applet is affected by the loading process. As described above, since the entire applet is loaded back into the smart card, the type of the use right of the applet is irrelevant, and the loading system may reload any type of applet within the smart card regardless of the type of use rights that the applet may have.

Figure 6 is a block diagram of the loading system in accordance with the invention being used to load a disposable application onto an existing smart card. As shown, the smart card 20 may have a first applet 102. In addition, at a remote system 112, a disposable applet 114 may be stored. The disposable applet may be loaded into the smart card 20 so that the smart card may contain the first applet 102 and the new disposable applet 114. The disposable applets may be easily loaded into the smart card. In addition, once the use rights of the disposable applet are exhausted, the disposable applet may be replaced, using the loading method in accordance with the invention, with a new applet having new use rights.

For example, a user may take a trip to a foreign country and desire some local currency to be placed on the smart card so that he does not have to carry any cash. At the end of the trip, the user does not want to keep the foreign currency applet since he will not have any further need for it. Thus, the invention enables the foreign currency applet to be replaced by, for example, a prepaid telephone call applet.

Figure 7 is a block diagram of the loading system in accordance with the invention being used to replenish the use rights of an applet in a smart card. In this example, the smart card 20 has a single applet 116 with use rights. After some time, the use rights of the applet have been depleted. In accordance with the invention, the applet 116 may be replaced by a new applet 120 that has the same functions as the old applet, but has replenished use rights.

The invention, as shown, is not limited to any particular number of applets and may be used to replenish the use rights of as few as a single applet or to replenish the use rights multiple applets. The invention may also be used to load and replace a single disposable applet onto a smart card. A method of debiting use rights in a smart card will now be described.

Figure 8 is flowchart of a method 200 of debiting use rights in a smart card. First in step 202, an applet within the smart card may be selected. For example, when a smart card is placed into a telephone terminal, then the applet

with the telephone use rights may be selected by the terminal. In order to select the applet, the smart card may verify that the terminal has the proper authority to access that particular applet. Then, at step 204, the smart card receives an application selection command from the terminal, for example. If the application selected is not initialized or present in the smart card, the method ends in step 5 206. If a valid application is selected, then in step 208, after a debit use rights command is issued, the smart card receives a debit use rights command at step 208. If the use rights have been exhausted already, then in step 210, the debit fails, and in step 212, the use rights of the applet may be replenished, as described below. If a valid debit command is received, then in step 214, the 10 decreased use rights of the applet are calculated and stored in the memory of the smart card. Then, if there are additional debits for the applet, the method loops to step 208, otherwise the method ends at step 216. The method of replenishing the use rights for an applet on the smart card in accordance with the invention will now be described. 15

Figure 9 is a flowchart of the step 212 of Figure 8, for replenishing the use rights of the applet in accordance with the invention. The applet may be selected because it has expended its use rights or because the user selects a particular 20 applet. As described above, the universal loader can load any type of applet with any type of use rights from the server to the memory of the smart card. In addition, since the loader can load any type of applet, it is not necessary to get

the use rights of the applet reloaded by the card issuer. Thus, the universal loader permits a greater amount of flexibility.

5           Once any of the applet with the associated use rights has been selected, at step 230, the smart card verifies the authenticity of the provider, such as the server, of the applet. If the authentication fails, then the method ends at step 232. If the authentication is successful, then in step 234, the provider, with the help of the loader, loads the applet into the NVM of the smart card.

10           Typically, authentication of the applet code may be achieved by the smart card through the verification of a digital signature, a cryptographic check sum or a predetermined hash value. In step 236, the smart card verifies the authenticity of the program code of the applet to detect viruses, and the like. In step 238, if the authentication of the applet code fails, then the applet code is deleted from  
15 the memory of the smart card.

          The next step is an optional step that is not required in order to load an application into a smart card in accordance with the invention. This step requires a smart card with a larger amount of memory. In this optional step 240, the  
20 smart card may perform static type checking and a syntax check of the code of the applet. If this check fails, then in step 242, the applet code is deleted from the memory of the smart card. In the last step 244, the smart card initializes the

code of the applet so that the use rights of the applet may be debited, as described above with reference to Figure 8.

5 While the foregoing has been with reference to a particular embodiment of the invention, it will be appreciated by those skilled in the art that changes in this embodiment may be made without departing from the principles and spirit of the invention, the scope of which is defined by the appended claims.



Claims:

1           1.       A system for loading an application and its associated use rights  
2           into a smart card having other applications, some of the other applications with  
3           associated use rights that have values that change as the application is used, the  
4           system comprising:

5                 means for storing, remotely from said smart card, an application and use  
6                 rights with a predetermined initial value, associated with the application;

7                 said smart card having a processing unit, and a memory unit, the memory  
8                 unit being connected to the processing unit and storing a second application  
9                 having use rights;

10                means for connecting said smart card to said remote storage means; and

11                means for loading said application, having use rights with a  
12                predetermined value, from said remote storage means into said smart card.

1           2.       The system of Claim 1, wherein the use rights have a refreshed state  
2           and a depleted state, the use rights of the second application being depleted and  
3           the use rights of the application being refreshed, and further comprising means  
4           for replacing said second application stored in the memory with said application  
5           at the remote storage means so that the use rights of the application in the  
6           memory are replenished.

1           3.       The system of Claim 2, wherein the connecting means further  
2           comprises means for verifying the authority of the remote storage means to load  
3           an application into the memory of the smart card.

1           4.       Smart card apparatus for loading an application having use rights  
2           with values which meter use of the application, the smart card comprising:  
3           a processor for executing an application;  
4           a memory, connected to the processor, for storing multiple applications,  
5           including a first application having first use rights and having first values  
6           associated with the first use rights, the first value changing from a predetermined  
7           initial value with use of the first use rights;  
8           an interface enabling the processor of said smart card to communicate with  
9           a remote location;  
10          means for receiving in the smart card a second application from said  
11          remote location over said interface, the second application having second use  
12          rights; and  
13          means for storing said second application into said memory in said smart  
14          card.

1           5.       The smart card apparatus of Claim 4 further comprising means for  
2           replacing said first application stored in the memory with said second application  
3           from said remote location so that the use rights of the application in the memory  
4           are replenished.

1           6.       The smart card apparatus of Claim 5, wherein the receiving means  
2 further comprises means for verifying the authority of the remote location to load  
3 an application into the memory of the smart card.

1           7.       A method of replenishing use rights in an application stored in a  
2 smart card, the use rights having a refreshed state and a depleted state and being  
3 depleted with use of the application, the smart card having a processor and a  
4 memory for storing the application, the method comprising:

5                 connecting a smart card having a first application with use rights in a  
6 depleted state to a communications system, the communications system being  
7 connected to a system remotely located from said smart card, the system storing  
8 a second application having equivalent use rights to the first use rights, the  
9 equivalent use rights having a refreshed state;

10                verifying in the card that said remote storage system has the authority to  
11 replace the first application in the smart card; and

12                replacing the first application in said memory with said second application  
13 having refreshed use rights so that the use rights of the application located  
within the memory of the smart card are replenished.

1           8.       The method of Claim 7, wherein replacing further comprises  
2 deleting said first application from said memory of said smart card, and loading  
3 said second application having refreshed use rights from said remote storage

4 location into said memory of said smart card so that the use rights of the  
5 application located within the memory of the smart card are replenished.

1 9. A method of loading an application into a smart card, the  
2 application having use rights with a refreshed state and a depleted state and  
3 being depleted with use of the application, the smart card having a processor and  
4 a memory for storing the application, the method comprising:

5 connecting a smart card having a first application with use rights to a  
6 communications system, the communications system being connected to a system  
7 remotely located from said smart card, the system storing a second application  
8 having use rights;

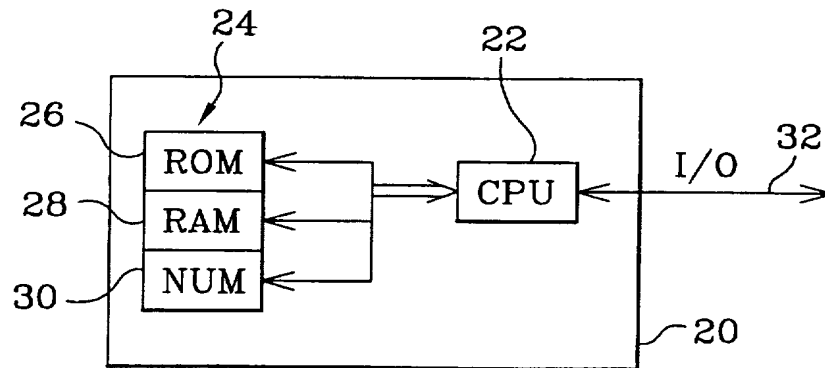
9 verifying in the smart card that said remote storage system has the  
10 authority to load the second application into the smart card; and

11 loading said second application having refreshed use rights into the  
12 memory of the smart card so that the second application may be used.

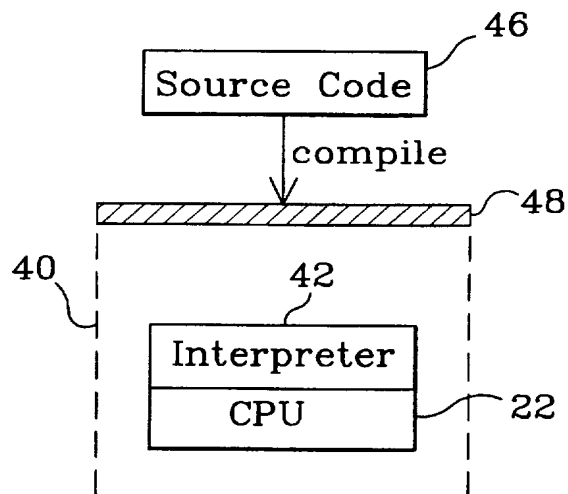
13 10. The method of Claim 11, wherein the first application has depleted  
14 use rights, the second application having refreshed equivalent use rights to the  
15 first application, and wherein the loading comprises replacing the first  
16 application in said memory with said second application having refreshed use  
17 rights so that the use rights of the application located within the memory of the  
18 smart card are replenished.

1           11. Smart card apparatus for loading an application having use rights  
2 with values which meter use of the application, the smart card comprising:  
3           a processor for executing an application;  
4           a memory, connected to the processor, for storing multiple applications,  
5 including a first application having first use rights and having first values  
6 associated with the first use rights, the first value changing from a predetermined  
7 initial value with use of the first use rights;  
8           means for loading in the smart card a second application from a remote  
9 location over an interface, the second application having second use rights;  
10          means for storing said second application into said memory in said smart  
11 card; and  
12          means for changing the use rights of said first application and said second  
13 application.

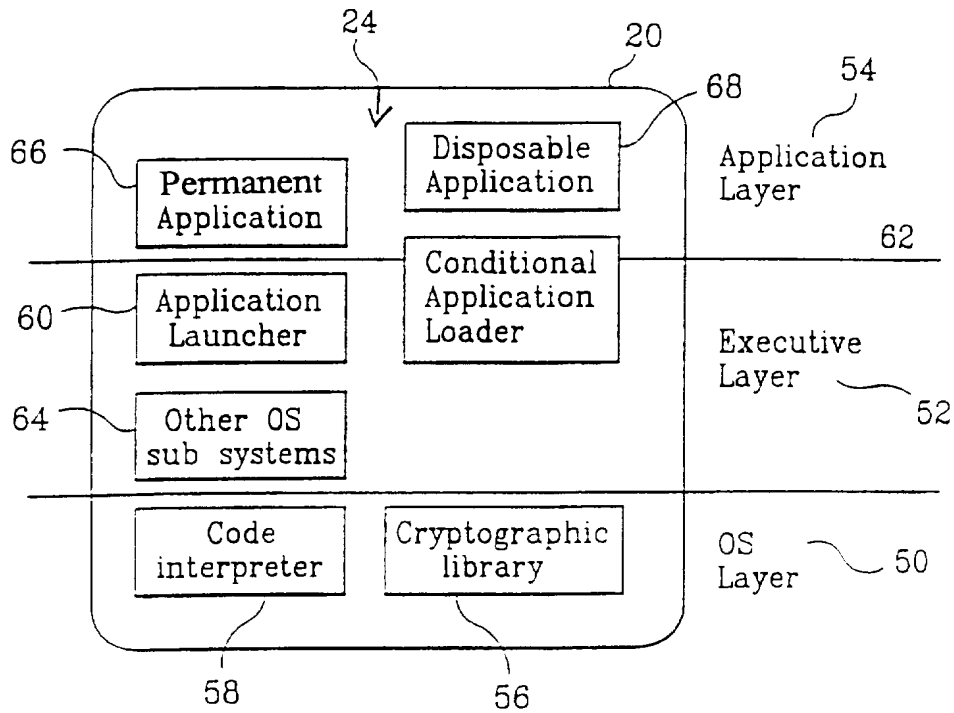
1           12. The smart card apparatus of Claim 11, where said second  
2 application has equivalent use rights to the first use rights, the equivalent use  
3 rights having a refreshed state, and wherein storing means further comprises  
4 means for replacing the first application in said memory with said second  
5 application having refreshed use rights so that the use rights of the application  
6 located within the memory of the smart card are replenished.



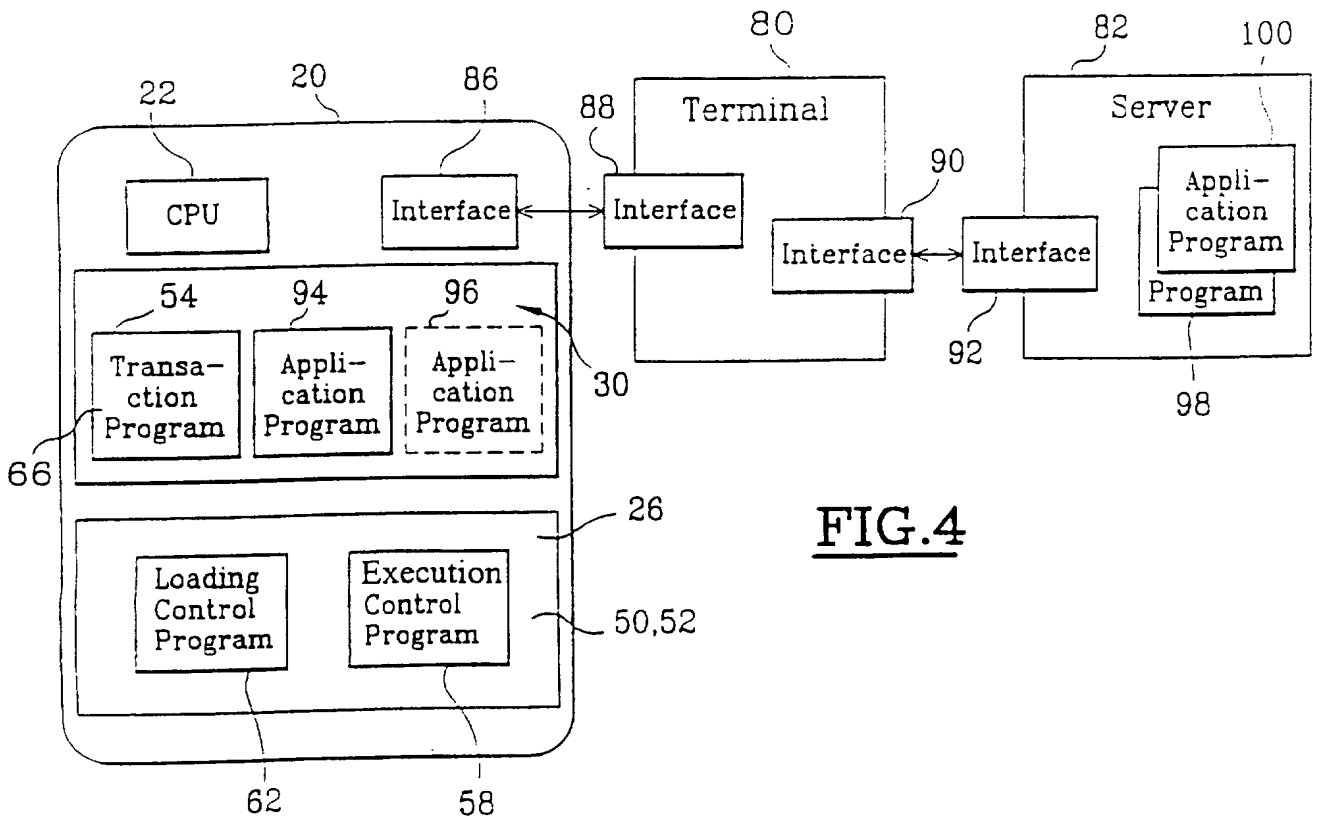
**FIG. 1**



**FIG. 2**

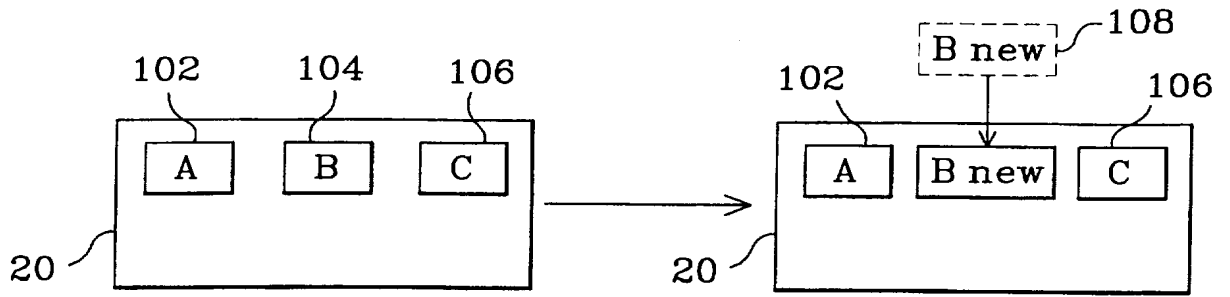


**FIG. 3**

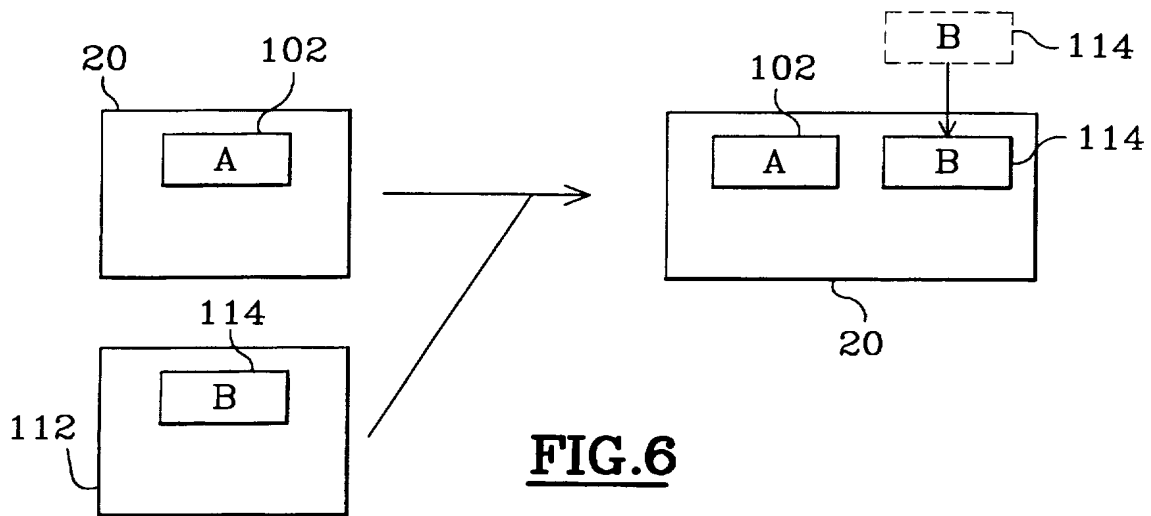


**FIG. 4**

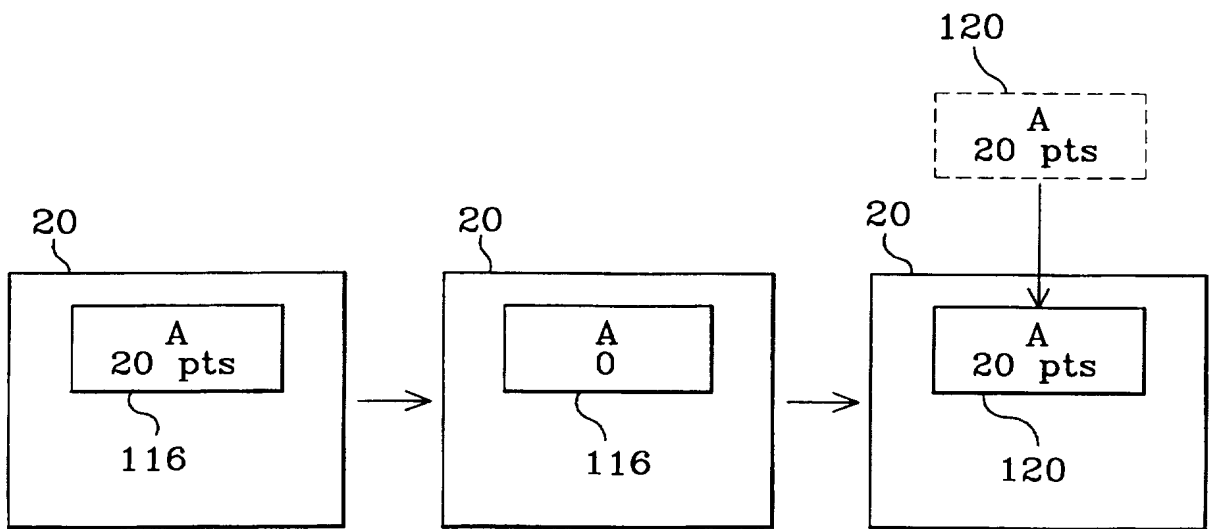
3/5



**FIG.5**

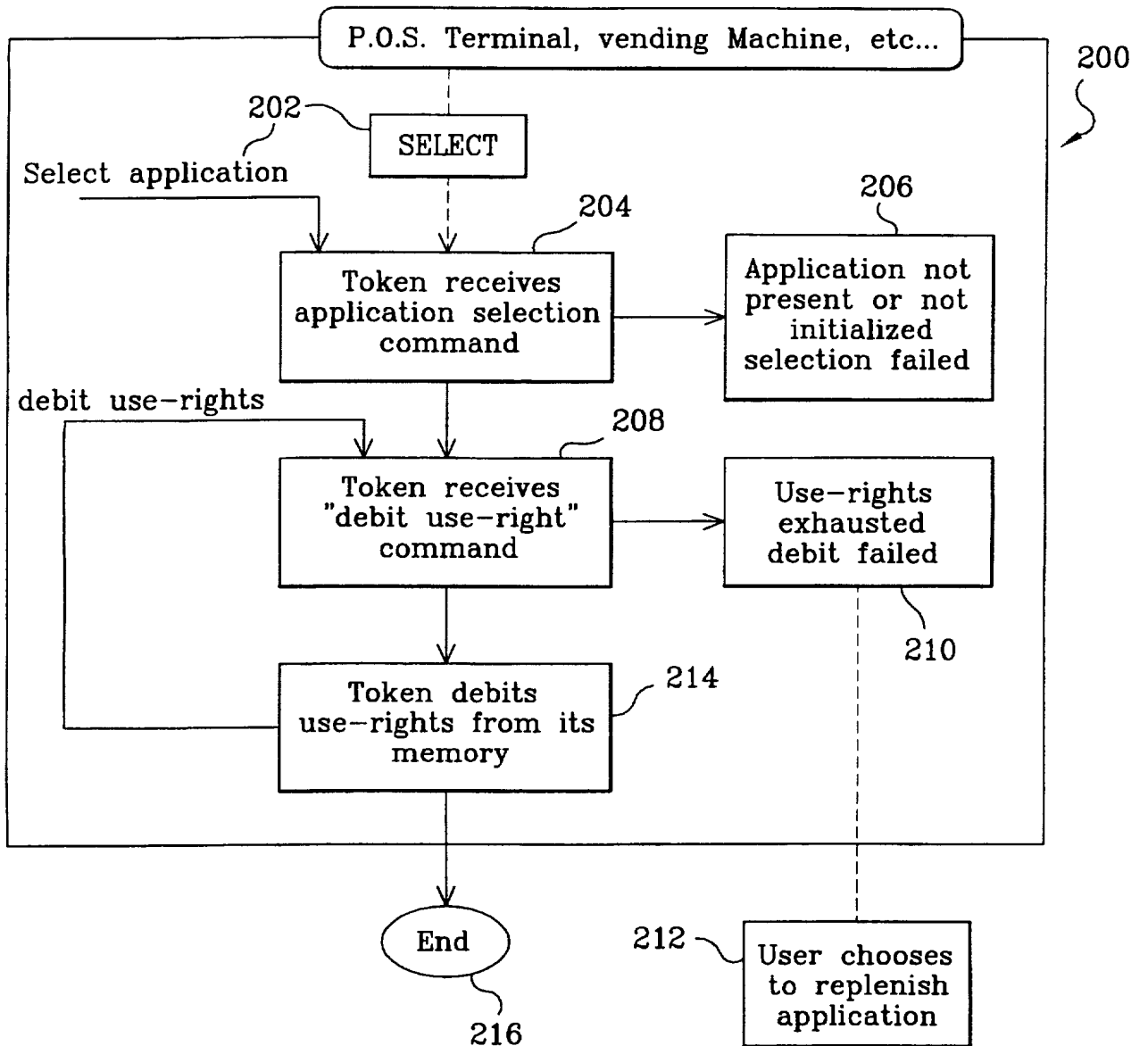


**FIG.6**

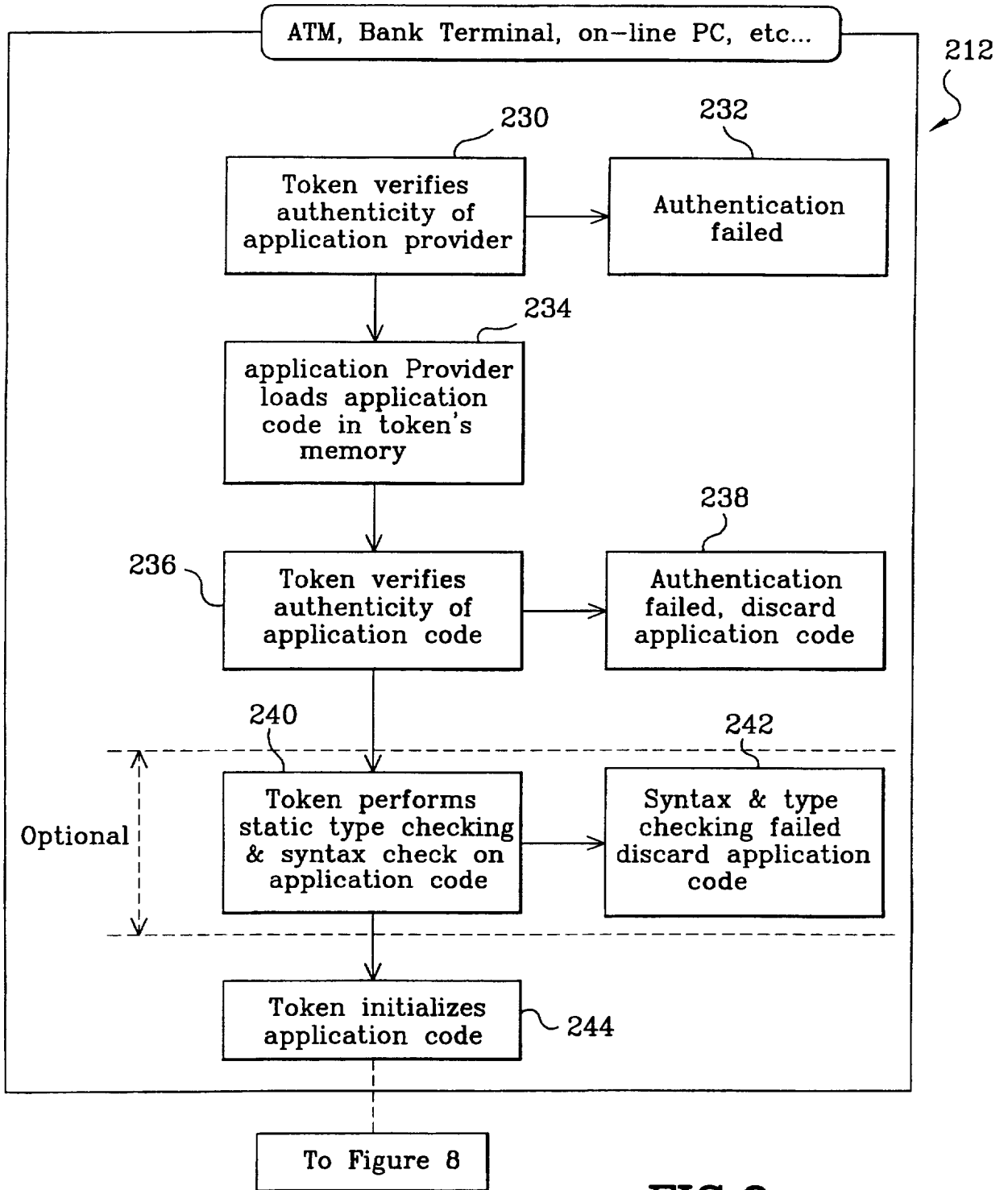


**FIG.7**





**FIG.8**



**FIG.9**



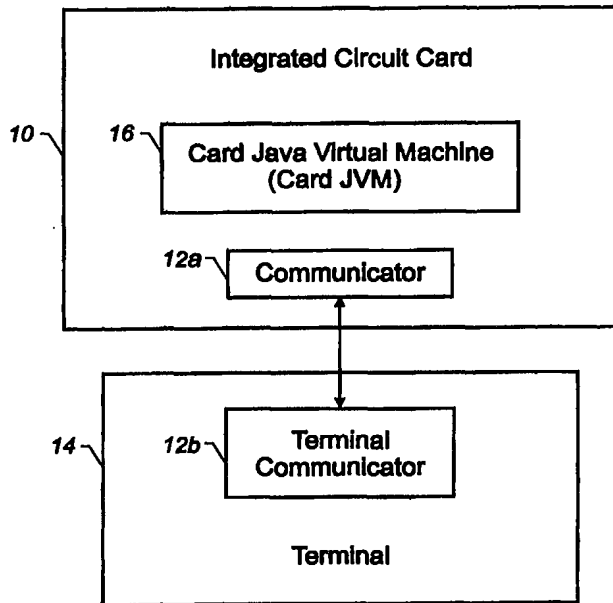
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>G06F 9/46, G07F 7/10</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 98/19237</b> (43) International Publication Date: 7 May 1998 (07.05.98)</p>
<p>(21) International Application Number: PCT/US97/18999 (22) International Filing Date: 22 October 1997 (22.10.97) (30) Priority Data: 60/029,057 25 October 1996 (25.10.96) US (71) Applicant: SCHLUMBERGER TECHNOLOGIES, INC. [US/US]; 8311 North R.R. 620, Austin, TX 78726 (US). (72) Inventors: WILKINSON, Timothy, J.; 6 Drumna House, 20 Oakleigh Park South, Whetstone, London M20 9JU (GB). GUTHERY, Scott, B.; 19 Foster Road, Belmont, MA 02178-3736 (US). KRISHNA, Ksheerabdh; 2831 Little Elm Trail, Cedar Park, TX 78613 (US). MONTGOMERY, Michael, A.; 906 Nelson Ranch Road, Cedar Park, TX 78613 (US). (74) Agents: PRUNER, Fred, G., Jr. et al.; Fish &amp; Richardson P.C., Suite 1200, One Riverway, Houston, TX 77056 (US).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> <i>With international search report.</i></p>

(54) Title: USING A HIGH LEVEL PROGRAMMING LANGUAGE WITH A MICROCONTROLLER

(57) Abstract

An integrated circuit card is used with a terminal. The integrated circuit card includes a memory that stores an interpreter and an application that has a high level programming language format. A processor of the card is configured to use the interpreter to interpret the application for execution and to use a communicator of the card to communicate with the terminal.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AL</b>	Albania	<b>ES</b>	Spain	<b>LS</b>	Lesotho	<b>SI</b>	Slovenia
<b>AM</b>	Armenia	<b>FI</b>	Finland	<b>LT</b>	Lithuania	<b>SK</b>	Slovakia
<b>AT</b>	Austria	<b>FR</b>	France	<b>LU</b>	Luxembourg	<b>SN</b>	Senegal
<b>AU</b>	Australia	<b>GA</b>	Gabon	<b>LV</b>	Latvia	<b>SZ</b>	Swaziland
<b>AZ</b>	Azerbaijan	<b>GB</b>	United Kingdom	<b>MC</b>	Monaco	<b>TD</b>	Chad
<b>BA</b>	Bosnia and Herzegovina	<b>GE</b>	Georgia	<b>MD</b>	Republic of Moldova	<b>TG</b>	Togo
<b>BB</b>	Barbados	<b>GH</b>	Ghana	<b>MG</b>	Madagascar	<b>TJ</b>	Tajikistan
<b>BE</b>	Belgium	<b>GN</b>	Guinea	<b>MK</b>	The former Yugoslav Republic of Macedonia	<b>TM</b>	Turkmenistan
<b>BF</b>	Burkina Faso	<b>GR</b>	Greece	<b>ML</b>	Mali	<b>TR</b>	Turkey
<b>BG</b>	Bulgaria	<b>HU</b>	Hungary	<b>MN</b>	Mongolia	<b>TT</b>	Trinidad and Tobago
<b>BJ</b>	Benin	<b>IE</b>	Ireland	<b>MR</b>	Mauritania	<b>UA</b>	Ukraine
<b>BR</b>	Brazil	<b>IL</b>	Israel	<b>MR</b>	Mauritania	<b>UG</b>	Uganda
<b>BY</b>	Belarus	<b>IS</b>	Iceland	<b>MW</b>	Malawi	<b>US</b>	United States of America
<b>CA</b>	Canada	<b>IT</b>	Italy	<b>MX</b>	Mexico	<b>UZ</b>	Uzbekistan
<b>CF</b>	Central African Republic	<b>JP</b>	Japan	<b>NE</b>	Niger	<b>VN</b>	Viet Nam
<b>CG</b>	Congo	<b>KE</b>	Kenya	<b>NL</b>	Netherlands	<b>YU</b>	Yugoslavia
<b>CH</b>	Switzerland	<b>KG</b>	Kyrgyzstan	<b>NO</b>	Norway	<b>ZW</b>	Zimbabwe
<b>CI</b>	Côte d'Ivoire	<b>KP</b>	Democratic People's Republic of Korea	<b>NZ</b>	New Zealand		
<b>CM</b>	Cameroon	<b>KR</b>	Republic of Korea	<b>PL</b>	Poland		
<b>CN</b>	China	<b>KZ</b>	Kazakhstan	<b>PT</b>	Portugal		
<b>CU</b>	Cuba	<b>LC</b>	Saint Lucia	<b>RO</b>	Romania		
<b>CZ</b>	Czech Republic	<b>LI</b>	Liechtenstein	<b>RU</b>	Russian Federation		
<b>DE</b>	Germany	<b>LK</b>	Sri Lanka	<b>SD</b>	Sudan		
<b>DK</b>	Denmark	<b>LR</b>	Liberia	<b>SE</b>	Sweden		
<b>EE</b>	Estonia			<b>SG</b>	Singapore		

- 1 -

USING A HIGH LEVEL PROGRAMMING LANGUAGE  
WITH A MICROCONTROLLER

5           A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and  
10 Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

          Under 35 U.S.C. § 119(e), this application claims benefit of prior U.S. provisional application Serial No. 60/029,057, filed October 25, 1996.

15                           Background of the Invention

          This invention relates in general to the field of programming, and more particularly to using a high level programming language with a smart card or a microcontroller.

20           Software applications written in the Java high-level programming language have been so designed that an application written in Java can be run on many different computer brands or computer platforms without change. This is accomplished by the following procedure.  
25 When a Java application is written, it is compiled into "Class" files containing byte codes that are instructions for a hypothetical computer called a Java Virtual Machine. An implementation of this virtual machine is written for each platform that is supported. When a user  
30 wishes to run a particular Java application on a selected platform, the class files compiled from the desired application is loaded onto the selected platform. The Java virtual machine for the selected platform is run, and interprets the byte codes in the class file, thus  
35 effectively running the Java application.

- 2 -

Java is described in the following references which are hereby incorporated by reference: (1) Arnold, Ken, and James Gosling, "The Java Programming Language," Addison-Wesley, 1996; (2) James Gosling, Bill Joy, and  
5 Guy Steele, "The Java Language Specification," Sun Microsystems, 1996, (web site: [http://java.sun.com/doc/language\\_specification](http://java.sun.com/doc/language_specification)); (3) James Gosling and Henry McGilton, "The Java Language Environment: A White Paper," Sun Microsystems, 1995 (web  
10 site: [http://java.sun.com/doc/language\\_environment/](http://java.sun.com/doc/language_environment/)); and (4) Tim Lindholm and Frank Yellin, "The Java Virtual Machine Specification," Addison-Wesley, 1997. These texts among many others describe how to program using Java.

15 In order for a Java application to run on a specific platform, a Java virtual machine implementation must be written that will run within the constraints of the platform, and a mechanism must be provided for loading the desired Java application on the platform,  
20 again keeping within the constraints of this platform.

Conventional platforms that support Java are typically microprocessor-based computers, with access to relatively large amounts of memory and hard disk storage space. Such microprocessor implementations frequently  
25 are used in desktop and personal computers. However, there are no conventional Java implementations on microcontrollers, as would typically be used in a smart card.

Microcontrollers differ from microprocessors in  
30 many ways. For example, a microprocessor typically has a central processing unit that requires certain external components (e.g., memory, input controls and output controls) to function properly. A typical microprocessor can access from a megabyte to a gigabyte  
35 of memory, and is capable of processing 16, 32, or 64

- 3 -

bits of information or more with a single instruction. In contrast to the microprocessor, a microcontroller includes a central processing unit, memory and other functional elements, all on a single semiconductor substrate, or integrated circuit (e.g., a "chip"). As compared to the relatively large external memory accessed by the microprocessor, the typical microcontroller accesses a much smaller memory. A typical microcontroller can access one to sixty-four kilobytes of built-in memory, with sixteen kilobytes being very common.

There are generally three different types of memory used: random access memory (RAM), read only memory (ROM), and electrically erasable programmable read only memory (EEPROM). In a microcontroller, the amount of each kind of memory available is constrained by the amount of space on the integrated circuit used for each kind of memory. Typically, RAM takes the most space, and is in shortest supply. ROM takes the least space, and is abundant. EEPROM is more abundant than RAM, but less than ROM.

Each kind of memory is suitable for different purposes. Although ROM is the least expensive, it is suitable only for data that is unchanging, such as operating system code. EEPROM is useful for storing data that must be retained when power is removed, but is extremely slow to write. RAM can be written and read at high speed, but is expensive and data in RAM is lost when power is removed.

A microprocessor system typically has relatively little ROM and EEPROM, and has 1 to 128 megabytes of RAM, since it is not constrained by what will fit on a single integrated circuit device, and often has access to an external disk memory system that serves as a large writable, non-volatile storage area at a lower cost that

- 4 -

EEPROM. However, a microcontroller typically has a small RAM of 0.1 to 2.0 K, 2K to 8K of EEPROM, and 8K - 56K of ROM.

Due to the small number of external components  
5 required and their small size, microcontrollers  
frequently are used in integrated circuit cards, such as  
smart cards. Such smart cards come in a variety of  
forms, including contact-based cards, which must be  
inserted into a reader to be used, and contactless cards,  
10 which need not be inserted. In fact, microcontrollers  
with contactless communication are often embedded into  
specialized forms, such as watches and rings, effectively  
integrating the functionality of a smart card in an  
ergonomically attractive manner.

15 Because of the constrained environment,  
applications for smart cards are typically written in a  
low level programming language (e.g., assembly language)  
to conserve memory.

The integrated circuit card is a secure, robust,  
20 tamper-resistant and portable device for storing data.  
The integrated circuit card is the most personal of  
personal computers because of its small size and because  
of the hardware and software data security features  
unique to the integrated circuit card.

25 The primary task of the integrated circuit card  
and the microcontroller on the card is to protect the  
data stored on the card. Consequently, since its  
invention in 1974, integrated circuit card technology has  
been closely guarded on these same security grounds. The  
30 cards were first used by French banks as debit cards. In  
this application, before a financial transaction based on  
the card is authorized, the card user must demonstrate  
knowledge of a 4-digit personal identification number  
(PIN) stored in the card in addition to being in  
35 possession of the card. Any information that might



- 5 -

contribute to discovering the PIN number on a lost or stolen card was blocked from public distribution. In fact, since nobody could tell what information might be useful in this regard, virtually all information about  
5 integrated circuit cards was withheld.

Due to the concern for security, applications written for integrated circuit cards have unique properties. For example, each application typically is identified with a particular owner or identity. Because  
10 applications typically are written in a low-level programming language, such as assembly language, the applications are written for a particular type of microcontroller. Due to the nature of low level programming languages, unauthorized applications may  
15 access data on the integrated circuit card. Programs written for a integrated circuit card are identified with a particular identity so that if two identities want to perform the same programming function there must be two copies of some portions of the application on the  
20 microcontroller of the integrated circuit card.

Integrated circuit card systems have historically been closed systems. An integrated circuit card contained a dedicated application that was handcrafted to work with a specific terminal application. Security  
25 checking when an integrated circuit card was used consisted primarily of making sure that the card application and the terminal application were a matched pair and that the data on the card was valid.

As the popularity of integrated circuit cards  
30 grew, it became clear that integrated circuit card users would be averse to carrying a different integrated circuit card for each integrated circuit card application. Therefore, multiple cooperating applications began to be provided on single provider  
35 integrated circuit cards. Thus, for example, an

- 6 -

automated teller machine (ATM) access card and a debit card may coexist on a single integrated circuit card platform. Nevertheless, this was still a closed system since all the applications in the terminal and the card  
5 were built by one provider having explicit knowledge of the other providers.

The paucity of information about integrated circuit cards -- particularly information about how to communicate with them and how to program them -- has  
10 impeded the general application of the integrated circuit card. However, the advent of public digital networking (e.g., the Internet and the World Wide Web) has opened new domains of application for integrated circuit cards. In particular, this has lead to a need to load new  
15 applications on the card that do not have explicit knowledge of the other providers, but without the possibility of compromising the security of the card. However, typically, this is not practical with conventional cards that are programmed using low level  
20 languages.

#### Summary of the Invention

In general, in one aspect, the invention features an integrated circuit card for use with a terminal. The integrated circuit card includes a memory that stores an  
25 interpreter and an application that has a high level programming language format. A processor of the card is configured to use the interpreter to interpret the application for execution and to use a communicator of the card to communicate with the terminal.

30 Among the advantages of the invention are one or more of the following. New applications may be downloaded to a smart card without compromising the security of the smart card. These applications may be provided by different companies loaded at different times

- 7 -

using different terminals. Security is not comprised since the applications are protected against unauthorized access of any application code or data by the security features provided by the Java virtual machine. Smart  
5 card applications can be created in high level languages such as Java and Eiffel, using powerful mainstream program development tools. New applications can be quickly prototyped and downloaded to a smart card in a matter of hours without resorting to soft masks.

10 Embedded systems using microcontrollers can also gain many of these advantages for downloading new applications, high level program development, and rapid prototyping by making use of this invention.

Implementations of the invention may include one  
15 or more of the following. The high level programming language format of the application may have a class file format and may have a Java programming language format. The processor may be a microcontroller. At least a portion of the memory may be located in the processor.

20 The application may have been processed from a second application that has a string of characters, and the string of characters may be represented in the first application by an identifier (e.g., an integer).

The processor may be also configured to receive a  
25 request from a requester (e.g., a processor or a terminal) to access an element (e.g., an application stored in the memory, data stored in the memory or the communicator) of the card, after receipt of the request, interact with the requester to authenticate an identity  
30 of the requester, and based on the identity, selectively grant access to the element.

The memory may also store an access control list for the element. The access control list furnishes an indication of types of access to be granted to the  
35 identity, and based on the access control list, the

- 8 -

processor selectively grants specific types of access (e.g., reading data, writing data, appending data, creating data, deleting data or executing an application) to the requester.

5           The application may be one of a several applications stored in the memory. The processor may be further configured to receive a request from a requester to access one of the plurality of applications; after receipt of the request, determine whether said one of the  
10 plurality of applications complies with a predetermined set of rules; and based on the determination, selectively grant access to the requester to said one of the plurality of applications. The predetermined rules provide a guide for determining whether said one of the  
15 plurality of applications accesses a predetermined region of the memory. The processor may be further configured to authenticate an identity of the requester and grant access to said one of the plurality of applications based on the identity.

20           The processor may be also configured to interact with the terminal via the communicator to authenticate an identity; determine if the identity has been authenticated; and based on the determination, selectively allow communication between the terminal and  
25 the integrated circuit card.

The communicator and the terminal may communicate via communication channels. The processor may also be configured to assign one of the communication channels to the identity when the processor allows the communication  
30 between the terminal and the integrated circuit card. The processor may also be configured to assign a session key to the assigned communication channel and use the session key when the processor and the terminal communicate via the assigned communication channel.

- 9 -

The terminal may have a card reader, and the communicator may include a contact for communicating with the card reader. The terminal may have a wireless communication device, and the communicator may include a wireless transceiver for communicating with the wireless communication device. The terminal may have a wireless communication device, and the communicator may include a wireless transmitter for communicating with the wireless communication device.

10 In general, in another aspect, the invention features a method for use with an integrated circuit card and a terminal. The method includes storing an interpreter and at least one application having a high level programming language format in a memory of the integrated circuit card. A processor of the integrated circuit card uses the interpreter to interpret the at least one application for execution, and the processor uses a communicator of the card when communicating between the processor and the terminal.

20 In general, in another aspect, the invention features a smart card. The smart card includes a memory that stores a Java interpreter and a processor that is configured to use the interpreter to interpret a Java application for execution.

25 In general, in another aspect, the invention features a microcontroller that has a semiconductor substrate and a memory located in the substrate. A programming language interpreter is stored in the memory and is configured to implement security checks. A central processing unit is located in the substrate and is coupled to the memory.

30 Implementations of the invention may include one or more of the following. The interpreter may be a Java byte code interpreter. The security checks may include

- 10 -

establishing firewalls and may include enforcing a sandbox security model.

In general, in another aspect, the invention features a smart card that has a programming language interpreter stored in a memory of the card. The  
5 interpreter is configured to implement security check. A central processing unit of the card is coupled to the memory.

In general, in another aspect, the invention  
10 features an integrated circuit card that is used with a terminal. The card includes a communicator and a memory that stores an interpreter and first instructions of a first application. The first instructions have been converted from second instructions of a second  
15 application. The integrated circuit card includes a processor that is coupled to the memory and is configured to use the interpreter to execute the first instructions and to communicate with the terminal via the communicator.

20 Implementations of the invention may include one or more of the following. The first and/or second applications may have class file format(s). The first and/or second applications may include byte codes, such as Java byte codes. The first instructions may be  
25 generalized or renumbered versions of the second instructions. The second instructions may include constant references, and the first instructions may include constants that replace the constant references of the second instructions. The second instructions may  
30 include references, and the references may shift location during the conversion of the second instructions to the first instructions. The first instructions may be relinked to the references after the shifting. The first instructions may include byte codes for a first type of  
35 virtual machine, and the second instructions may include

- 11 -

byte codes for a second type of virtual machine. The first type is different from the second type.

In general, in another aspect, the invention features a method for use with an integrated circuit  
5 card. The method includes converting second instructions of a second application to first instructions of a first application; storing the first instructions in a memory of the integrated circuit card; and using an interpreter of the integrated circuit card to execute the first  
10 instructions.

In general, in another aspect, the invention features an integrated circuit for use with a terminal. The integrated circuit card has a communicator that is configured to communicate with the terminal and a memory  
15 that stores a first application that has been processed from a second application having a string of characters. The string of characters are represented in the first application by an identifier. The integrated circuit card includes a processor that is coupled to the memory.  
20 The processor is configured to use the interpreter to interpret the first application for execution and to use the communicator to communicate with the terminal.

In general, in another aspect, the invention features a method for use with an integrated circuit card  
25 and a terminal. The method includes processing a second application to create a first application. The second application has a string of characters. The string of characters is represented by an identifier in the second application. An interpreter and the first application  
30 are stored in a memory of the integrated circuit card. A processor uses an interpreter to interpret the first application for execution.

In general, in another aspect, the invention features a microcontroller that includes a memory which  
35 stores an application and an interpreter. The

- 12 -

application has a class file format. A processor of the microcontroller is coupled to the memory and is configured to use the interpreter to interpret the application for execution.

5 In implementations of the invention, the microcontroller may also include a communicator that is configured to communicate with a terminal.

In general, in another aspect, the invention features a method for use with an integrated circuit  
10 card. The method includes storing a first application in a memory of the integrated circuit card, storing a second application in the memory of the integrated circuit card, and creating a firewall that isolates the first and  
15 second applications so that the second application cannot access either the first application or data associated with the first application.

In general, in another aspect, the invention features an integrated circuit card for use with a  
20 terminal. The integrated circuit card includes a communicator that is configured to communicate with the terminal, a memory and a processor. The memory stores applications, and each application has a high level programming language format. The memory also stores an  
25 interpreter. The processor is coupled to the memory and is configured to: a.) use the interpreter to interpret the applications for execution, b.) use the interpreter to create a firewall to isolate the applications from each other, and c.) use the communicator to communicate with the terminal.

30 Other advantages and features will become apparent from the following description and from the claims.

Brief Description of the Drawing



- 13 -

Fig. 1 is a block diagram of an integrated card system.

Fig. 2 is a flow diagram illustrating the preparation of Java applications to be downloaded to an  
5 integrated circuit card.

Fig. 3 is a block diagram of the files used and generated by the card class file converter.

Fig. 4 is a block diagram illustrating the transformation of application class file(s) into a card  
10 class file.

Fig. 5 is a flow diagram illustrating the working of the class file converter.

Fig. 6 is a flow diagram illustrating the modification of the byte codes.

Fig. 7 is a block diagram illustrating the transformation of specific byte codes into general byte  
15 codes.

Fig. 8 is a block diagram illustrating the replacement of constant references with constants.

Fig. 9 is a block diagram illustrating the replacement of references with their updated values.  
20

Fig. 10 is a block diagram illustrating renumbering of original byte codes.

Fig. 11 is a block diagram illustrating translation of original byte codes for a different  
25 virtual machine architecture.

Fig 12 is a block diagram illustrating loading applications into an integrated circuit card.

Fig. 13 is a block diagram illustrating executing  
30 applications in an integrated circuit card.

Fig. 14 is a schematic diagram illustrating memory organization for ROM, RAM and EEPROM.

Fig. 15 is a flow diagram illustrating the overall architecture of the Card Java virtual machine.

- 14 -

Fig. 16 is a flow diagram illustrating method execution in the Card Java virtual machine with the security checks.

Fig. 17 is a flow diagram illustrating byte code execution in the Card Java virtual machine.

Fig. 18 is a flow diagram illustrating method execution in the Card Java virtual machine without the security checks.

Fig. 19 is a block diagram illustrating the association between card applications and identities.

Fig. 20 is a block diagram illustrating the access rights of a specific running application.

Fig. 21 is a perspective view of a microcontroller on a smart card.

Fig. 22 is a perspective view of a microcontroller on a telephone.

Fig. 23 is a perspective view of a microcontroller on a key ring.

Fig. 24 is a perspective view of a microcontroller on a ring.

Fig. 25 is a perspective view of a microcontroller on a circuit card of an automobile.

#### Detailed Description of the Preferred Embodiments

Referring to Fig. 1, an integrated circuit card 10 (e.g., a smart card) is constructed to provide a high level, Java-based, multiple application programming and execution environment. The integrated circuit card 10 has a communicator 12a that is configured to communicate with a terminal communicator 12b of a terminal 14. In some embodiments, the integrated circuit card 10 is a smart card with an 8 bit microcontroller, 512 bytes of RAM, 4K bytes of EEPROM, and 20K of ROM; the terminal communicator 12b is a conventional contact smart card reader; and the terminal 14 is a conventional personal

- 15 -

computer running the Windows NT operating system supporting the personal computer smart card (PC/SC) standard and providing Java development support.

In some embodiments, the microcontroller, memory  
5 and communicator are embedded in a plastic card that has substantially the same dimensions as a typical credit card. In other embodiments, the microcontroller, memory and communicator are mounted within bases other than a plastic card, such as jewelry (e.g., watches, rings or  
10 bracelets), automotive equipment, telecommunication equipment (e.g., subscriber identity module (SIM) cards), security devices (e.g., cryptographic modules) and appliances.

The terminal 14 prepares and downloads Java  
15 applications to the integrated circuit card 10 using the terminal communicator 12b. The terminal communicator 12b is a communications device capable of establishing a communications channel between the integrated circuit card 10 and the terminal 14. Some communication options  
20 include contact card readers, wireless communications via radio frequency or infrared techniques, serial communication protocols, packet communication protocols, ISO 7816 communication protocol, to name a few.

The terminal 14 can also interact with  
25 applications running in the integrated circuit card 10. In some cases, different terminals may be used for these purposes. For example, one kind of terminal may be used to prepare applications, different terminals could be used to download the applications, and yet other  
30 terminals could be used to run the various applications. Terminals can be automated teller machines (ATM)s, point-of-sale terminals, door security systems, toll payment systems, access control systems, or any other system that communicates with an integrated circuit card or  
35 microcontroller.

- 16 -

The integrated circuit card 10 contains a card Java virtual machine (Card JVM) 16, which is used to interpret applications which are contained on the card 10.

5 Referring to Fig. 2, the Java application 20 includes three Java source code files A.java 20a, B.java 20b, and C.java 20c. These source code files are prepared and compiled in a Java application development environment 22. When the Java application 20 is compiled  
10 by the development environment 22, application class files 24 are produced, with these class files A.class 24a, B.class 24b, and C.class 24c corresponding to their respective class Java source code 20a, 20b, and 20c. The application class files 24 follow the standard class file  
15 format as documented in chapter 4 of the Java virtual machine specification by Tim Lindholm and Frank Yellin, "The Java Virtual Machine Specification," Addison-Wesley, 1996. These application class files 24 are fed into the card class file converter 26, which consolidates and  
20 compresses the files, producing a single card class file 27. The card class file 27 is loaded to the integrated circuit card 10 using a conventional card loader 28.

Referring to Fig. 3, the card class file converter 26 is a class file postprocessor that processes a set of  
25 class files 24 that are encoded in the standard Java class file format, optionally using a string to ID input map file 30 to produce a Java card class file 27 in a card class file format. One such card class file format is described in Appendix A which is hereby incorporated  
30 by reference. In addition, in some embodiments, the card class file converter 26 produces a string to ID output map file 32 that is used as input for a subsequent execution of the card class file converter.

In some embodiments, in order for the string to ID  
35 mapping to be consistent with a previously generated card

- 17 -

class file (in the case where multiple class files  
reference the same strings), the card class file  
converter 26 can accept previously defined string to ID  
mappings from a string to ID input map file 30. In the  
5 absence of such a file, the IDs are generated by the card  
class file converter 26. Appendix B, which is hereby  
incorporated by reference, describes one possible way of  
implementing and producing the string to ID input map  
file 30 and string to ID output map file 32 and  
10 illustrates this mapping via an example.

Referring to Fig. 4, a typical application class  
file 24a includes class file information 41; a class  
constant pool 42; class, fields created, interfaces  
referenced, and method information 43; and various  
15 attribute information 44, as detailed in aforementioned  
Java Virtual Machine Specification. Note that much of  
the attribute information 44 is not needed for this  
embodiment and is eliminated 45 by the card class file  
converter 26. Eliminated attributes include SourceFile,  
20 ConstantValue, Exceptions, LineNumberTable,  
LocalVariableTable, and any optional vendor attributes.  
The typical card class file 27 as described in Appendix A  
is derived from the application class files 24 in the  
following manner. The card class file information 46 is  
25 derived from the aggregate class file information 41 of  
all application class files 24a, 24b, and 24c. The card  
class file constant pool 47 is derived from the aggregate  
class constant pool 42 of all application class files  
24a, 24b, and 24c. The card class, fields created,  
30 interfaces referenced, and method information 48 is  
derived from the aggregate class, fields created,  
interfaces referenced, and method information 43 of all  
application class files 24a, 24b, and 24c. The card  
attribute information 49 in this embodiment is derived  
35 from only the code attribute of the aggregate attribute

- 18 -

information 44 of all application class files 24a, 24b, and 24c.

To avoid dynamic linking in the card, all the information that is distributed across several Java class file 24a, 24b, and 24c that form the application 24, are  
5 coalesced into one card class file 27 by the process shown in the flowchart in Fig. 5. The first class file to be processed is selected 51a. The constant pool 42 is compacted 51b in the following manner. All objects,  
10 classes, fields, methods referenced in a Java class file 24a are identified by using strings in the constant pool 42 of the class file 24a. The card class file converter 26 compacts the constant pool 42 found in the Java class file 24a into an optimized version. This compaction is  
15 achieved by mapping all the strings found in the class file constant pool 42 into integers (the size of which is microcontroller architecture dependent). These integers are also referred to as IDs. Each ID uniquely identifies a particular object, class, field or method in the  
20 application 20. Therefore, the card class file converter 26 replaces the strings in the Java class file constant pool 42 with its corresponding unique ID. Appendix B shows an example application HelloSmartCard.java, with a table below illustrating the IDs corresponding to the  
25 strings found in the constant pool of the class file for this application. The IDs used for this example are 16-bit unsigned integers.

Next, the card class file converter 26 checks for unsupported features 51c in the Code attribute of the  
30 input Java class file 24a. The Card JVM 16 only supports a subset of the full Java byte codes as described in Appendix C, which is hereby incorporated by reference. Hence, the card class file converter 26 checks for unsupported byte codes in the Code attribute of the Java  
35 class file 24a. If any unsupported byte codes are found

- 19 -

52, the card class file converter flags an error and stops conversion 53. The program code fragment marked "A" in APPENDIX D shows how these spurious byte codes are apprehended. Another level of checking can be performed 5 by requiring the standard Java development environment 22 to compile the application 20 with a '-g' flag. Based on the aforementioned Java virtual machine specification, this option requires the Java compiler to place information about the variables used in a Java 10 application 20 in the LocalVariableTable attribute of the class file 24a. The card class file converter 26 uses this information to check if the Java class file 24a references data types not supported by the Java card.

Next, the card class file converter 26 discards 15 all the unnecessary parts 51c of the Java class file 24a not required for interpretation. A Java class file 24a stores information pertaining to the byte codes in the class file in the Attributes section 44 of the Java class file. Attributes that are not required for 20 interpretation by the card JVM 16, such as SourceFile, ConstantValue, Exceptions, LineNumberTable, and LocalVariableTable may be safely discarded 45. The only attribute that is retained is the Code attribute. The Code attribute contains the byte codes that correspond to 25 the methods in the Java class file 24a.

Modifying the byte codes 54 involves examining the Code attribute information 44 for each method in the class file, and modifying the operands of byte codes that refer to entries in the Java class file constant pool 42 30 to reflect the entries in the card class file constant pool 47. In some embodiments, the byte codes are also modified, as described below.

Modifying the byte codes 54 involves five passes (with two optional passes) as described by the flowchart 35 in Fig. 6. The original byte codes 60 are found in the

- 20 -

Code attribute 44 of the Java class file 24a being processed. The first pass 61 records all the jumps and their destinations in the original byte codes. During later byte code translation, some single byte code may be translated to dual or triple bytes. Fig. 7 illustrates an example wherein byte code ILOAD\_0 is replaced with two bytes, byte code ILOAD and argument 0. When this is done, the code size changes, requiring adjustment of any jump destinations which are affected. Therefore, before these transformations are made, the original byte codes 60 are analyzed for any jump byte codes and a note made of their position and current destination. The program code fragment marked "B" in Appendix D shows how these jumps are recorded. Appendix D is hereby incorporated by reference.

Once the jumps are recorded, if the optional byte code translation is not being performed 62, the card class file converter 26 may proceed to the third pass 64.

Otherwise, the card class file converter converts specific byte codes into generic byte codes. Typically, the translated byte codes are not interpreted in the Card JVM 16 but are supported by converting the byte codes into equivalent byte codes that can be interpreted by the Card JVM 16 (see Fig. 7). The byte codes 70 may be replaced with another semantically equivalent but different byte codes 72. This generally entails the translation of short single specific byte codes such as ILOAD\_0 into their more general versions. For example, ILOAD\_0 may be replaced by byte code ILOAD with an argument 0. This translation is done to reduce the number of byte codes translated by the Card JVM 16, consequently reducing the complexity and code space requirements for the Card JVM 16. The program code fragment marked "C" in Appendix D shows how these translations are made. Note that such translations



- 21 -

increase the size of the resulting byte code and force the re-computation of any jumps which are affected.

In the third pass 64, the card class file converter rebuilds constant references via elimination of the strings used to denote these constants. Fig. 8 shows an example wherein the byte code LDC 80 referring to constant "18" found via an index in the Java class file 24a constant pool 42 may be translated into BIPUSH byte code 82. In this pass the card class file converter 26 modifies the operands to all the byte codes that refer to entries in the Java class file constant pool 42 to reflect their new location in the card class file constant pool 47. Fig. 9 shows an example wherein the argument to a byte code, INVOKESTATIC 90, refers to an entry in the Java class file constant pool 42 that is modified to reflect the new location of that entry in the card class file constant pool 47. The modified operand 94 shows this transformation. The program code fragment marked "D" in Appendix D shows how these modifications are made.

Once the constant references are relinked, if the optional byte code modification is not being performed, the card class file converter may proceed to the fifth and final pass 67.

Otherwise, the card class file converter modifies the original byte codes into a different set of byte codes supported by the particular Card JVM 16 being used. One potential modification renumbers the original byte codes 60 into Card JVM 16 byte codes (see Fig. 10). This renumbering causes the byte codes 100 in the original byte codes 60 to be modified into a renumbered byte codes 102. Byte code ILOAD recognized by value 21 may be renumbered to be recognized by value 50. This modification may be done for optimizing the type tests (also known in prior art as Pass 3 checks) in the Card

- 22 -

JVM 16. The program code fragment marked "E" in Appendix D shows an implementation of this embodiment. This modification may be done in order to reduce the program space required by the Card JVM 16 to interpret the byte code. Essentially this modification regroups the byte codes into Card JVM 16 byte codes so that byte codes with similar operands, results are grouped together, and there are no gaps between Card JVM 16 byte codes. This allows the Card JVM 16 to efficiently check Card JVM 16 byte codes and validate types as it executes.

In some embodiments, the card class file converter modifies the original byte codes 60 into a different set of byte codes designed for a different virtual machine architecture, as shown in Fig. 11. The Java byte code ILOAD 112 intended for use on a word stack 114 may be replaced by Card JVM 16 byte code ILOAD\_B 116 to be used on a byte stack 118. An element in a word stack 114 requires allocating 4 bytes of stack space, whereas an element in the byte stack 118 requires only one byte of stack space. Although this option may provide an increase in execution speed, it risks losing the security features available in the original byte codes.

Since the previous steps 63, 64 or 66 may have changed the size of the byte codes 60 the card class file converter 26 has to relink 67 any jumps which have been effected. Since the jumps were recorded in the first step 61 of the card class file converter 26, this adjustment is carried out by fixing the jump destinations to their appropriate values. The program code fragment marked "F" in Appendix D shows how these jumps are fixed.

The card class file converter now has modified byte codes 68 that is equivalent to the original byte codes 60 ready for loading. The translation from the Java class file 24a to the card class file 27 is now complete.

- 23 -

Referring back to Fig. 5, if more class files 24 remain to be processed 55 the previous steps 51a, 51b, 51c, 52 and 54 are repeated for each remaining class file. The card class file converter 26 gathers 56 the  
5 maps and modified byte codes for the classes 24 that have been processed, places them as an aggregate and generates 57 a card class file 27. If required, the card class file converter 26 generates a string to ID output map file 32, that contains a list of all the new IDs  
10 allocated for the strings encountered in the constant pool 42 of the Java class files 24 during the translation.

Referring to Fig. 12, the card loader 28 within the terminal 14 sends a card class file to the loading  
15 and execution control 120 within the integrated circuit card 10 using standard ISO 7816 commands. The loading and execution control 120 with a card operating system 122, which provides the necessary system resources, including support for a card file system 124, which can  
20 be used to store several card applications 126. Many conventional card loaders are written in low level languages, supported by the card operating system 122. In the preferred embodiment, the bootstrap loader is written in Java, and the integrated circuit card 10  
25 includes a Java virtual machine to run this application. A Java implementation of the loading and execution control 120 is illustrated in Appendix E which is hereby incorporated by reference. The loading and execution control 120 receives the card class file 26 and produces  
30 a Java card application 126x stored in the card file system 126 in the EEPROM of the integrated circuit card 10. Multiple Java card applications 126x, 126y, and 126z can be stored in a single card in this manner. The loading and execution control 120 supports commands  
35 whereby the terminal 14 can select which Java card

- 24 -

application to run immediately, or upon the next card reset.

Referring to Fig. 13, upon receiving a reset or an execution command from the loading and execution control  
5 120, the Card Java Virtual Machine (Card JVM) 16 begins execution at a predetermined method (for example, main) of the selected class in the selected Java Card application 126z. The Card JVM 16 provides the Java card application 126z access to the underlying card operating  
10 system 122, which provides capabilities such as I/O, EEPROM support, file systems, access control, and other system functions using native Java methods as illustrated in Appendix F which is hereby incorporated by reference.

The selected Java card application 126z  
15 communicates with an appropriate application in the terminal 14 using the communicator 12a to establish a communication channel to the terminal 14. Data from the communicator 12a to the terminal 14 passes through a communicator driver 132 in the terminal, which is  
20 specifically written to handle the communications protocol used by the communicator 12a. The data then passes to an integrated circuit card driver 134, which is specifically written to address the capabilities of the particular integrated circuit card 10 being used, and  
25 provides high level software services to the terminal application 136. In the preferred embodiment, this driver would be appropriate PC/SC Smartcard Service Provider (SSP) software. The data then passes to the terminal application 136, which must handle the  
30 capabilities provided by the particular card application 126z being run. In this manner, commands and responses pass back and forth between the terminal application 136 and the selected card application 126z. The terminal application interacts with the user, receiving commands

- 25 -

from the user, some of which are passed to the selected Java card application 126z, and receiving responses from the Java card application 126z, which are processed and passed back to the user.

5 Referring to Fig. 14, the Card JVM 16 is an interpreter that interprets a card application 126x. The memory resources in the microcontroller that impact the Card JVM 16 are the Card ROM 140, Card RAM 141 and the Card EEPROM 142. The Card ROM 140 is used to store the  
10 Card JVM 16 and the card operating system 122. Card ROM 140 may also be used to store fixed card applications 140a and class libraries 140b. Loadable applications 141a, 141b and libraries 141c may also be stored in Card RAM 141. The Card JVM 16 interprets a card application  
15 141a, 141b, or 140a. The Card JVM 16 uses the Card RAM to store the VM stack 144a and system state variables 144b. The Card JVM 16 keeps track of the operations performed via the VM stack 144a. The objects created by the Card JVM 16 are either on the RAM heap 144c, in the  
20 EEPROM heap 146a, or in the file system 147.

All of the heap manipulated by the Card JVM 16 may be stored in the Card RAM 141 as a RAM Heap 144c, or it may be distributed across to the Card EEPROM 142 as a EEPROM Heap 146a. Card RAM 141 is also used for  
25 recording the state of the system stack 148 that is used by routines written in the native code of the microcontroller. The Card JVM 16 uses the Card EEPROM 142 to store application data either in the EEPROM heap 146a or in the file system 147. Application data stored  
30 in a file may be manipulated via an interface to the card operating system 122. This interface is provided by a class library 140b stored in Card ROM 140, by a loadable class library 141c stored in Card EEPROM 142. One such interface is described in Appendix F. Applications and

- 26 -

data in the card are isolated by a firewall mechanism  
149.

To cope with the limited resources available on  
microcontrollers, the Card JVM 16 implements a strict  
5 subset of the Java programming language. Consequently, a  
Java application 20 compiles into a class file that  
contains a strict subset of Java byte codes. This  
enables application programmers to program in this strict  
subset of Java and still maintain compatibility with  
10 existing Java Virtual Machines. The semantics of the  
Java byte codes interpreted by the Card JVM 16 are  
described in the aforementioned Java Virtual Machine  
Specification. The subset of byte codes interpreted by  
the Card JVM 16 can be found in Appendix C. The card  
15 class file converter 26 checks the Java application 20 to  
ensure use of only the features available in this subset  
and converts into a form that is understood and  
interpreted by the Card JVM 16.

In other embodiments, the Card JVM 16 is designed  
20 to interpret a different set or augmented set of byte  
codes 116. Although a different byte code set might lead  
to some performance improvements, departing from a strict  
Java subset may not be desirable from the point of view  
of security that is present in the original Java byte  
25 codes or compatibility with mainstream Java development  
tools.

All Card JVM 16 applications 126 have a defined  
entry point denoted by a class and a method in the class.  
This entry point is mapped in the string to ID input map  
30 30 and assigned by the card class file converter 26.  
Classes, methods and fields within a Java application 20  
are assigned IDs by the card class file converter 26.  
For example, the ID corresponding to the main application  
class may be defined as F001 and the ID corresponding to

- 27 -

its main method, such as "main()V" could be defined as F002.

The overall execution architecture of the Card JVM is described by the flowchart in Fig. 15. Execution of the Card JVM 16 begins at the execution control 120, which chooses a card application 126z to execute. It proceeds by finding and assigning an entry point 152 (a method) in this card application for the Card JVM 16 to interpret. The Card JVM 16 interprets the method 153. If the interpretation proceeds successfully 154, the Card JVM 16 reports success 155 returning control back to the execution control 120. If in the course of interpretation 153 the Card JVM 16 encounters an unhandled error or exception (typically a resource limitation or a security violation), the Card JVM 16 stops 156 and reports the appropriate error to the terminal 14.

An essential part of the Card JVM 16 is a subroutine that handles the execution of the byte codes. This subroutine is described by the flowchart in Fig. 16. Given a method 160 it executes the byte codes in this method. The subroutine starts by preparing for the parameters of this method 161. This involves setting the VM stack 144a pointer, VM stack 144a frame limits, and setting the program counter to the first byte code of the method.

Next, the method flags are checked 162. If the method is flagged native, then the method is actually a call to native method code (subroutine written in the microcontroller's native processor code). In this case, the Card JVM 16 prepares for an efficient call 163 and return to the native code subroutine. The parameters to the native method may be passed on the VM stack 144a or via the System stack 148. The appropriate security checks are made and the native method subroutine is

- 28 -

called. On return, the result (if any) of the native method subroutine is placed on the VM stack 144a so that it may be accessed by the next byte code to be executed.

The dispatch loop 164 of the Card JVM 16 is then entered. The byte code dispatch loop is responsible for preparing, executing, and retiring each byte code. The loop terminates when it finishes interpreting the byte codes in the method 160, or when the Card JVM 16 encounters a resource limitation or a security violation.

10 If a previous byte code caused a branch to be taken 165 the Card JVM prepares for the branch 165a. The next byte code is retrieved 165b. In order to keep the cost of processing each byte code down, as many common elements such as the byte code arguments, length, type  
15 are extracted and stored.

To provide the security offered by the security model of the programming language, byte codes in the class file must be verified and determined conformant to this model. These checks are typically carried out in  
20 prior art by a program referred to as the byte code verifier, which operates in four passes as described in the Java Virtual Machine Specification. To offer the run-time security that is guaranteed by the byte code verifier, the Card JVM 16 must perform the checks that  
25 pertain to the Pass 3 and Pass 4 of the verifier. This checking can be bypassed by the Card JVM 16 if it can be guaranteed (which is almost impossible to do) that the byte codes 60 interpreted by the Card JVM 16 are secure. At the minimum, code security can be maintained as long  
30 as object references cannot be faked and the VM stack 144a and local variable bounds are observed. This requires checking the state of the VM stack 144a with respect to the byte code being executed.

To enforce the security model of the programming  
35 language, a 256-byte table is created as shown in



- 29 -

Appendix G which is hereby incorporated by reference. This table is indexed by the byte code number. This table contains the type and length information associated with the indexing byte code. It is encoded with the first 5 bits representing type, and the last 3 bits representing length. The type and length of the byte code is indexed directly from the table by the byte code number. This type and length is then used for checking as shown in Appendix H which is hereby incorporated by reference. In Appendix H, the checking process begins by decoding the length and type from the table in Appendix G which is hereby incorporated by reference. The length is used to increment the program counter. The type is used first for pre-execution checking, to insure that the data types on the VM stack 144a are correct for the byte code that is about to be executed. The 256 bytes of ROM for table storage allows the original Java byte codes to be run in the Card JVM 16 and minimizes the changes required to the Java class file to be loaded in the card. Additional Java byte codes can be easily supported since it is relatively easy to update the appropriate table entries.

In other embodiments, as shown in Fig. 10, the Java byte codes in the method are renumbered in such a manner that the byte code type and length information stored in the table in Appendix H is implicit in the reordering. Appendix H is hereby incorporated by reference. Consequently, the checks that must be performed on the state of the VM stack 144a and the byte code being processed does not have to involve a table look up. The checks can be performed by set of simple comparisons as shown in Appendix I which is hereby incorporated by reference. This embodiment is preferable when ROM space is at a premium, since it eliminates a 256-byte table. However adding new byte codes to the set

- 30 -

of supported byte codes has to be carefully thought out since the new byte codes have to fit in the implicit numbering scheme of the supported byte codes.

In another embodiment, the Card JVM 16 chooses not to perform any security checks in favor of Card JVM 16 execution speed. This is illustrated in the flowchart in Fig. 18. The flow chart in Fig. 18 is the same as that of Fig. 16 with the security checks removed. This option is not desirable from the point of view of security, unless it can be guaranteed that the byte codes are secure.

The Card JVM 16 may enforce other security checks as well. If the byte code may reference a local variable, the Card JVM 16 checks if this reference is valid, throwing an error if it is not. If the reference is valid, the Card JVM 16 stores the type of the local variable for future checking. The VM stack 144a pointer is checked to see if it is still in a valid range. If not an exception is thrown. The byte code number is checked. If it is not supported, an exception is thrown.

Finally, the byte code itself is dispatched 165d. The byte codes translated by the Card JVM 16 are listed in Appendix C. The semantics of the byte codes are described in the aforementioned Java Virtual Machine Specification with regard to the state of the VM stack 144a before and after the dispatch of the byte code. Note also that some byte codes (the byte codes, INVOKESTATIC, INVOKESPECIAL, INVOKENONVIRTUAL and INVOKEVIRTUAL) may cause reentry into the Card JVM 16, requiring processing to begin at the entry of the subroutine 161. Fig. 17 shows the flowchart of the byte code execution routine. The routine is given a byte code 171 to execute. The Card JVM 16 executes 172 the instructions required for the byte code. If in the course of executing the Card JVM 16 encounters a resource

- 31 -

limitation 173, it returns an error 156. This error is returned to the terminal 16 by the Card JVM 16. If the byte code executes successfully, it returns a success 175.

5           After execution, the type of the result is used to set the VM stack 144a state correctly 165e, properly flagging the data types on the VM stack 144a. The byte code information gathered previously 165b from the byte code info table is used to set the state of the VM stack  
10 144a in accordance with the byte code that just executed.

          In other embodiments, setting the output state of the VM stack 144a with respect to the byte code executed is simplified if the byte code is renumbered. This is shown in Appendix I which is hereby incorporated by  
15 reference.

          In yet another embodiment, the Card JVM 16 may bypass setting the output state of the VM stack 144a in favor of Card JVM 16 execution speed. This option is not desirable from the point of view of security, unless it  
20 can be guaranteed that the byte codes are secure.

          After the byte code has been executed, the byte code is retired 165f. This involves popping arguments off the VM stack 144a. Once byte code processing is completed, the loop 164 is repeated for the next byte  
25 code for the method.

          Once the dispatch loop 164 terminates, the VM stack 144a is emptied 166. This prevents any object references filtering down to other Card JVM 16 invocations and breaking the Card JVM's 16 security.  
30 Termination 167 of the byte code dispatch loop 164 indicates that the Card JVM 16 has completed executing the requested method.

          To isolate data and applications in the integrated circuit card 10 from each other, the integrated circuit

card 10 relies on the firewall mechanism 149 provided by the Card JVM 16. Because the Card JVM implements the standard pass 3 and pass 4 verifier checks, it detects any attempt by an application to reference the data or code space used by another application, and flag a security error 156. For example, conventional low level applications can cast non-reference data types into references, thereby enabling access to unauthorized memory space, and violating security. With this invention, such an attempt by a card application 126z to use a non-reference data type as a reference will trigger a security violation 156. In conventional Java, this protected application environment is referred to as the sandbox application-interpretation environment.

However, these firewall facilities do not work independently. In fact, the facilities are overlapping and mutually reinforcing with conventional access control lists and encryption mechanisms shown in the following table:

	Access Control Lists	Virtual Machine	Encryption
Data Protection	access control before operation	access only to own namespace	data to another program encrypted
Program Protection	access control before execution	execution only on correct types	data encrypted in program's namespace

	Access Control Lists	Virtual Machine	Encryption
Communication Protection	access control on channels	channel controls in own namespace	only mutually authenticated parties can communicate

Taken together, these facilities isolate both data and applications on the integrated circuit card 10 and ensure that each card application 126 can access only the authorized resources of the integrated circuit card 10.

Referring to Fig. 19, card applications 126x, 126y, 126z can be endowed with specific privileges when the card applications 126 execute. These privileges determine, for example, which data files the card applications 126 can access and what operations the card applications 126 can perform on the file system 147. The privileges granted to the card applications 126 are normally set at the time that a particular card application 126z is started by the user, typically from the terminal 14.

The integrated circuit card 10 uses cryptographic identification verification methods to associate an identity 190 (e.g., identities 190a, 190b and 190c) and hence, a set of privileges to the execution of the card application 126. The association of the specific identity 190c to the card application 126z is made when the card application 126z begins execution, thus creating a specific running application 200, as shown in Fig. 20. The identity 190 is a unique legible text string reliably associated with an identity token. The identity token (e.g., a personal identification number (PIN) or a RSA private key) is an encryption key.

- 34 -

Referring to Fig. 20, in order to run a specific card application 126z, the identity 190c of the card application 126z must be authenticated. The identity 190c is authenticated by demonstrating knowledge of the identity token associated with the identity 190c. Therefore, in order to run the card application 126z, an agent (e.g., a card holder or another application wishing to run the application) must show that it possesses or knows the application's identity-defining encryption key.

One way to demonstrate possession of an encryption key is simply to expose the key itself. PIN verification is an example of this form of authentication. Another way to demonstrate the possession of an encryption key without actually exposing the key itself is to show the ability to encrypt or decrypt plain text with the key.

Thus, a specific running application 200 on the integrated circuit card 10 includes a card application 126z plus an authenticated identity 190c. No card application 126 can be run without both of these elements being in place. The card application 126z defines data processing operations to be performed, and the authenticated identity 190c determines on what computational objects those operations may be performed. For example, a specific application 126z can only access identity C's files 202 in the file system 147 associated with the specific identity 190c, and the specific card application 126z cannot access other files 204 that are associated with identities other than the specific identity 190c.

The integrated circuit card 10 may take additional steps to ensure application and data isolation. The integrated circuit card 10 furnishes three software features sets: authenticated-identity access control lists; a Java-based virtual machine; and one-time session encryption keys to protect data files, application

- 35 -

execution, and communication channels, respectively. Collectively, for one embodiment, these features sets provide the application data firewalls 149 for one embodiment. The following discusses each software  
5 feature set and then shows how the three sets work together to insure application and data isolation on the integrated circuit card 10.

An access control list (ACL) is associated with every computational object (e.g., a data file or a  
10 communication channel) on the integrated circuit card 10 that is to be protected, i.e., to which access is to be controlled. An entry on an ACL (for a particular computational object) is in a data format referred to as an e-tuple:

15 type:identity:permissions

The type field indicates the type of the following identity (in the identity field), e.g., a user (e.g., "John Smith"), or a group. The permissions field indicates a list of operations (e.g., read, append and  
20 update) that can be performed by the identity on the computational object.

As an example, for a data file that has the ACL entry:

USER:AcmeAirlines:RAU,

25 any application whose identity is "AcmeAirlines" can read ("R"), append ("A") and update ("U") the data file. In addition, the ACL may be used selectively to permit the creation and deletion of data files. Furthermore, the ACL may be used selectively to permit execution of an  
30 application.

Whenever a computational object is accessed by a running application 200, the access is intercepted by the Card JVM 16 and passed to the card operating system 122, which determines if there is an ACL associated with the  
35 object. If there is an associated ACL, then the identity

- 36 -

190c associated with the running application 200 is matched on the ACL. If the identity is not found or if the identity is not permitted for the type of access that is being requested, then the access is denied.

5 Otherwise, the access is allowed to proceed.

Referring to Fig. 13, to prevent the potential problems due to the single data path between the integrated circuit card 10 and the terminal 14, communication channel isolation is accomplished by  
10 including in the identity authentication process the exchange of a one-time session key 209 between the a card application 126z and the terminal application 136. The key 209 is then used to encrypt subsequent traffic between the authenticating terminal application 136 and  
15 the authenticated card application 126z. Given the one-time session key 209, a rogue terminal application can neither "listen in" on an authenticated communication between the terminal 14 and the integrated circuit card 10, nor can the rogue terminal application "spooft" the  
20 card application into performing unauthorized operations on its behalf.

Encryption and decryption of card/terminal traffic can be handled either by the card operating system 122 or by the card application itself 126z. In the former case,  
25 the communication with the terminal 14 is being encrypted transparently to the application, and message traffic arrives decrypted in the data space of the application. In the latter case, the card application 126z elects to perform encryption and decryption to provide an extra  
30 layer of security since the application could encrypt data as soon as it was created and would decrypt data only when it was about to be used. Otherwise, the data would remain encrypted with the session key 209.

Thus, the application firewall includes three  
35 mutually reinforcing software sets. Data files are



- 37 -

protected by authenticated-identity access control lists. Application execution spaces are protected by the Card JVM 16. Communication channels are protected with one-time session encryption keys 209.

5           In other embodiments, the above-described techniques are used with a microcontroller (such as the processor 12) may control devices (e.g., part of an automobile engine) other than an integrated circuit card. In these applications, the microcontroller provides a  
10 small platform (i.e., a central processing unit, and a memory, both of which are located on a semiconductor substrate) for storing and executing high level programming languages. Most existing devices and new designs that utilize a microcontroller could use this  
15 invention to provide the ability to program the microcontroller using a high level language, and application of this invention to such devices is specifically included.

          The term application includes any program, such as  
20 Java applications, Java applets, Java aglets, Java servlets, Java comlets, Java components, and other non-Java programs that can result in class files as described below.

          Class files may have a source other than Java  
25 program files. Several programming languages other than Java also have compilers or assemblers for generating class files from their respective source files. For example, the programming language Eiffel can be used to generate class files using Pirmin Kalberer's "J-Eiffel",  
30 an Eiffel compiler with JVM byte code generation (web site: <http://www.spin.ch/~kalberer/jive/index.htm>). An Ada 95 to Java byte code translator is described in the following reference (incorporated herein by reference): Taft, S. Tucker, "Programming the Internet in Ada 95",  
35 proceedings of Ada Europe '96, 1996. Jasmin is a Java

- 38 -

byte code assembler that can be used to generate class files, as described in the following reference (incorporated herein by reference): Meyer, Jon and Troy Downing, "Java Virtual Machine", O'Reilly, 1997.

5 Regardless of the source of the class files, the above description applies to languages other than Java to generate codes to be interpreted.

Fig. 21 shows an integrated circuit card, or smart card, which includes a microcontroller 210 that is  
10 mounted to a plastic card 212. The plastic card 212 has approximately the same form factor as a typical credit card. The communicator 12a can use a contact pad 214 to establish a communication channel, or the communicator 12a can use a wireless communication system.

15 In other embodiments, a microcontroller 210 is mounted into a mobile or fixed telephone 220, effectively adding smart card capabilities to the telephone, as shown in Fig. 22. In these embodiments, the microcontroller 210 is mounted on a module (such as a Subscriber Identity  
20 Module (SIM)), for insertion and removal from the telephone 220.

In other embodiments, a microcontroller 210 is added to a key ring 230 as shown in Fig. 23. This can be used to secure access to an automobile that is equipped  
25 to recognize the identity associated with the microcontroller 210 on the key ring 230.

Jewelry such as a watch or ring 240 can also house a microcontroller 210 in an ergonomic manner, as shown in Fig. 24. Such embodiments typically use a wireless  
30 communication system for establishing a communication channel, and are a convenient way to implement access control with a minimum of hassle to the user.

Fig. 25 illustrates a microcontroller 210 mounted in an electrical subsystem 252 of an automobile 254. In  
35 this embodiment, the microcontroller is used for a

- 39 -

variety of purposes, such as to controlling access to the automobile, (e.g. checking identity or sobriety before enabling the ignition system of the automobile), paying tolls via wireless communication, or interfacing with a  
5 global positioning system (GPS) to track the location of the automobile, to name a few.

While specific embodiments of the present invention have been described, various modifications and substitutions will become apparent to one skilled in the  
10 art by this disclosure. Such modifications and substitutions are within the scope of the present invention, and are intended to be covered by the appended claims.

## APPENDIX A

### Card Class File Format For Preferred Embodiment

#### Introduction

The card class file is a compressed form of the original class file(s). The card class file contains only the semantic information required to interpret Java programs from the original class files. The indirect references in the original class file are replaced with direct references resulting in a compact representation.

The card class file format is based on the following principles:

***Stay close to the standard class file format.*** The card class file format should remain as close to the standard class file format as possible. The Java byte codes in the class file remain unaltered. Not altering the byte codes ensures that the structural and static constraints on them remain verifiably intact.

***Ease of implementation:*** The card class file format should be simple enough to appeal to Java Virtual Machine implementers. It must allow for different yet behaviorally equivalent implementations.

***Feasibility:*** The card class file format must be compact in order to accommodate smart card technology. It must meet the constraints of today's technology while not losing sight of tomorrow's innovations.

This document is based on Chapter 4, "The class file format", in the book titled "The Java™ Virtual Machine Specification"[1], henceforth referred to as the Red book. Since the document is based on the standard class file format described in the Red book, we only present information that is different. The Red book serves as the final authority for any clarification.

The primary changes from the standard class file format are:

The constant pool is optimized to contain only 16-bit identifiers and, where possible, indirection is replaced by a direct reference.

Attributes in the original class file are eliminated or regrouped.

#### **The Java Card class File Format**

This section describes the Java Card class file format. Each card class file contains one

or many Java types, where a type may be a class or an interface.

A card class file consists of a stream of 8-bit bytes. All 16-bit, 32-bit, and 64-bit quantities are constructed by reading in two, four, and eight consecutive 8-bit bytes, respectively. Multi-byte data items are always stored in big-endian order, where the high bytes come first. In Java, this format is supported by interfaces `java.io.DataInput` and `java.io.DataOutput` and classes such as `java.io.DataInputStream` and `java.io.DataOutputStream`.

We define and use the same set of data types representing Java class file data: The types `u1`, `u2`, and `u4` represent an unsigned one-, two-, or four-byte quantity, respectively. In Java, these types may be read by methods such as `readUnsignedByte`, `readUnsignedShort`, and `readInt` of the interface `java.io.DataInput`.

The card class file format is presented using pseudo-structures written in a C-like structure notation. To avoid confusion with the fields of Java Card Virtual Machine classes and class instances, the contents of the structures describing the card class file format are referred to as items. Unlike the fields of a C structure, successive items are stored in the card class file sequentially, without padding or alignment.

Variable-sized tables, consisting of variable-sized items, are used in several class file structures. Although we will use C-like array syntax to refer to table items, the fact that tables are streams of varying-sized structures means that it is not possible to directly translate a table index into a byte offset into the table.

Where we refer to a data structure as an array, it is literally an array.

In order to distinguish between the card class file structure and the standard class file structure, we add capitalization; for example, we rename `field_info` in the original class file to `FieldInfo` in the card class file.

### **Card Class File**

A card class file contains a single `CardClassFile` structure:

```
CardClassFile {
    u1 major_version;
    u1 minor_version;
    u2 name_index;
    u2 const_size;
    u2 max_class;
    CpInfo constant_pool[const_size];
    ClassInfo class[max_class];
}
```

The items in the CardClassFile structure are as follows:

**minor\_version, major\_version**

The values of the minor\_version and major\_version items are the minor and major version numbers of the off-card Java Card Virtual Machine that produced this card class file. An implementation of the Java Card Virtual Machine normally supports card class files having a given major version number and minor version numbers 0 through some particular minor\_version.

Only the Java Card Forum may define the meaning of card class file version numbers.

**name\_index**

The value of the name\_index item must represent a valid Java class name. The Java class name represented by name\_index must be exactly the same Java class name that corresponds to the main application that is to run in the card. A card class file contains several classes or interfaces that constitute the application that runs in the card. Since Java allows each class to contain a main method there must be a way to distinguish the class file containing the main method which corresponds to the card application.

**const\_size**

The value of const\_size gives the number of entries in the card class file constant pool. A constant\_pool index is considered valid if it is greater than or equal to zero and less than const\_size.

**max\_class**

This value refers to the number of classes present in the card class file. Since the name resolution and linking in the Java Card are done by the off-card Java Virtual Machine all the class files or classes required for an application are placed together in one card class file.

**constant\_pool[]**

The constant\_pool is a table of variable-length structures () representing various string constants, class names, field names, and other constants that are referred to within the CardClassFile structure and its substructures.

The first entry in the card class file is constant\_pool[0].

Each of the constant\_pool table entries at indices 0 through const\_size is a variable-length structure ().

**class[]**

The class is a table of max\_class classes that constitute the application loaded onto the card.

### Constant Pool

All constant\_pool table entries have the following general format:

```
CpInfo {
    u1 tag;
    u1 info[];
}
```

Each item in the constant\_pool table must begin with a 1-byte tag indicating the kind of cp\_info entry. The contents of the info array varies with the value of tag. The valid tags and their values are the same as those specified in the Red book.

Each tag byte must be followed by two or more bytes giving information about the specific constant. The format of the additional information varies with the tag value. Currently the only tags that need to be included are CONSTANT\_Class, CONSTANT\_FieldRef, CONSTANT\_MethodRef and CONSTANT\_InterfaceRef. Support for other tags be added as they are included in the specification.

#### CONSTANT\_Class

The CONSTANT\_Class\_info structure is used to represent a class or an interface:

```
CONSTANT_ClassInfo {
    u1 tag;
    u2 name_index;
}
```

The items of the CONSTANT\_Class\_info structure are the following:

#### tag

The tag item has the value CONSTANT\_Class (7).

#### name\_index

The value of the name\_index item must represent a valid Java class name. The Java class name represented by name\_index must be exactly the same Java class name that is described by the corresponding CONSTANT\_Class entry in the constant\_pool of the original class file.

CONSTANT\_Fieldref, CONSTANT\_Methodref, and CONSTANT\_InterfaceMethodref Fields, methods, and interface methods are represented by similar structures:

```
CONSTANT_FieldrefInfo {
    u1 tag;
    u2 class_index;
    u2 name_sig_index;
}
```

```

    CONSTANT_MethodrefInfo {
        u1 tag;
        u2 class_index;
        u2 name_sig_index;
    }
    CONSTANT_InterfaceMethodrefInfo {
        u1 tag;
        u2 class_index;
        u2 name_sig_index;
    }

```

The items of these structures are as follows:

**tag**

The tag item of a CONSTANT\_FieldrefInfo structure has the value CONSTANT\_Fieldref (9).

The tag item of a CONSTANT\_MethodrefInfo structure has the value CONSTANT\_Methodref (10).

The tag item of a CONSTANT\_InterfaceMethodrefInfo structure has the value CONSTANT\_InterfaceMethodref (11).

**class\_index**

The value of the class\_index item must represent a valid Java class or interface name. The name represented by class\_index must be exactly the same name that is described by the corresponding CONSTANT\_Class\_info entry in the constant\_pool of the original class file.

**name\_sig\_index**

The value of the name\_sig\_index item must represent a valid Java name and type. The name and type represented by name\_sig\_index must be exactly the same name and type described by the CONSTANT\_NameAndType\_info entry in the constant\_pool structure of the original class file.

**Class**

Each class is described by a fixed-length ClassInfo structure. The format of this structure is:

```

ClassInfo {
    u2 name_index;
    u1 max_field;
    u1 max_sfield;

```



```

    u1 max_method;
    u1 max_interface;
    u2 superclass;
    u2 access_flags;
    FieldInfo field[max_field+max_sfield];
    InterfaceInfo interface[max_interface];
    MethodInfo method[max_method];
}

```

The items of the ClassInfo structure are as follows:

**name\_index**

The value of the name\_index item must represent a valid Java class name. The Java class name represented by name\_index must be exactly the same Java class name that is described in the corresponding ClassFile structure of the original class file.

**max\_field**

The value of the max\_field item gives the number of FieldInfo () structures in the field table that represent the instance variables, declared by this class or interface type. This value refers to the number of non-static the fields in the card class file. If the class represents an interface the value of max\_field is 0.

**max\_sfield**

The value of the max\_sfield item gives the number of FieldInfo structures in the field table that represent the class variables, declared by this class or interface type. This value refers to the number of static the fields in the card class file.

**max\_method**

The value of the max\_method item gives the number of MethodInfo () structures in the method table.

**max\_interface**

The value of the max\_interface item gives the number of direct superinterfaces of this class or interface type.

**superclass**

For a class, the value of the superclass item must represent a valid Java class name. The Java class name represented by superclass must be exactly the same Java class name that is described in the corresponding ClassFile structure of the original class file. Neither the superclass nor any of its superclasses may be a final class. If the value of superclass is 0, then this class must represent the class java.lang.Object, the only class or interface without a superclass.

For an interface, the value of superclass must always represent the Java class `java.lang.Object`.

#### **access\_flags**

The value of the `access_flags` item is a mask of modifiers used with class and interface declarations. The `access_flags` modifiers and their values are the same as the `access_flags` modifiers in the corresponding `ClassFile` structure of the original class file.

#### **field[]**

Each value in the field table must be a fixed-length `FieldInfo` () structure giving a complete description of a field in the class or interface type. The field table includes only those fields that are declared by this class or interface. It does not include items representing fields that are inherited from superclasses or superinterfaces.

#### **interface[]**

Each value in the interface array must represent a valid interface name. The interface name represented by each entry must be exactly the same interface name that is described in the corresponding interface array of the original class file.

#### **method[]**

Each value in the method table must be a variable-length `MethodInfo` () structure giving a complete description of and Java Virtual Machine code for a method in the class or interface.

The `MethodInfo` structures represent all methods, both instance methods and, for classes, class (static) methods, declared by this class or interface type. The method table only includes those methods that are explicitly declared by this class. Interfaces have only the single method `<clinit>`, the interface initialization method. The methods table does not include items representing methods that are inherited from superclasses or superinterfaces.

#### **Fields**

Each field is described by a fixed-length `field_info` structure. The format of this structure is

```
FieldInfo {
    u2 name_index;
    u2 signature_index;
    u2 access_flags;
}
```

The items of the `FieldInfo` structure are as follows:

#### **name\_index**

The value of the name\_index item must represent a valid Java field name. The Java field name represented by name\_index must be exactly the same Java field name that is described in the corresponding field\_info structure of the original class file.

#### **signature\_index**

The value of the signature\_index item must represent a valid Java field descriptor. The Java field descriptor represented by signature index must be exactly the same Java field descriptor that is described in the corresponding field\_info structure of the original class file.

#### **access\_flags**

The value of the access\_flags item is a mask of modifiers used to describe access permission to and properties of a field. The access\_flags modifiers and their values are the same as the access\_flags modifiers in the corresponding field\_info structure of the original class file.

#### **Methods**

Each method is described by a variable-length MethodInfo structure. The MethodInfo structure is a variable-length structure that contains the Java Virtual Machine instructions and auxiliary information for a single Java method, instance initialization method, or class or interface initialization method. The structure has the following format:

```
MethodInfo {
    u2 name_index;
    u2 signature_index;
    u1 max_local;
    u1 max_arg;
    u1 max_stack;
    u1 access_flags;
    u2 code_length;
    u2 exception_length;
    u1 code[code_length];
    {
        u2 start_pc;
        u2 end_pc;
        u2 handler_pc;
        u2 catch_type;
    } einfo[exception_length];
}
```

The items of the MethodInfo structure are as follows:

**name\_index**

The value of the name\_index item must represent either one of the special internal method names, either <init> or <clinit>, or a valid Java method name. The Java method name represented by name\_index must be exactly the same Java method name that is described in the corresponding method\_info structure of the original class file.

**signature\_index**

The value of the signature\_index item must represent a valid Java method descriptor. The Java method descriptor represented by signature\_index must be exactly the same Java method descriptor that is described in the corresponding method\_info structure of the original class file.

**max\_local**

The value of the max\_locals item gives the number of local variables used by this method, excluding the parameters passed to the method on invocation. The index of the first local variable is 0. The greatest local variable index for a one-word value is max\_locals-1.

**max\_arg**

The value of the max\_arg item gives the maximum number of arguments to this method.

**max\_stack**

The value of the max\_stack item gives the maximum number of words on the operand stack at any point during execution of this method.

**access\_flags**

The value of the access\_flags item is a mask of modifiers used to describe access permission to and properties of a method or instance initialization method. . The access\_flags modifiers and their values are the same as the access\_flags modifiers in the corresponding method\_info structure of the original class file.

**code\_length**

The value of the code\_length item gives the number of bytes in the code array for this method. The value of code\_length must be greater than zero; the code array must not be empty.

**exception\_length**

The value of the exception\_length item gives the number of entries in the exception\_info table.

**code[]**

The code array gives the actual bytes of Java Virtual Machine code that implement the method. When the code array is read into memory on a byte addressable machine, if the first byte of the array is aligned on a 4-byte boundary, the tableswitch and lookupswitch 32-bit offsets will be 4-byte aligned; refer to the descriptions of those instructions for more information on the consequences of code array alignment. The detailed constraints on the contents of the code array are extensive and are the same as described in the Java Virtual Machine Specification.

**info[]**

Each entry in the info array describes one exception handler in the code array. Each info entry contains the following items:

**start\_pc, end\_pc**

The values of the two items start\_pc and end\_pc indicate the ranges in the code array at which the exception handler is active.

The value of start\_pc must be a valid index into the code array of the opcode of an instruction. The value of end\_pc either must be a valid index into the code array of the opcode of an instruction, or must be equal to code\_length, the length of the code array. The value of start\_pc must be less than the value of end\_pc.

The start\_pc is inclusive and end\_pc is exclusive; that is, the exception handler must be active while the program counter is within the interval [start\_pc, end\_pc).

**handler\_pc**

The value of the handler\_pc item indicates the start of the exception handler. The value of the item must be a valid index into the code array, must be the index of the opcode of an instruction, and must be less than the value of the code\_length item.

**catch\_type**

If the value of the catch\_type item is nonzero, it must represent a valid Java class type. The Java class type represented by catch\_type must be exactly the same as the Java class type that is described by the catch\_type in the corresponding method\_info structure of the original class file. This class must be the class Throwable or one of its subclasses. The exception handler will be called only if the thrown exception is an instance of the given class or one of its subclasses.

If the value of the catch\_type item is zero, this exception handler is called for all exceptions. This is used to implement finally.

**Attributes**

Attributes used in the original class file are either eliminated or regrouped for compaction.

The predefined attributes `SourceFile`, `ConstantValue`, `Exceptions`, `LineNumberTable`, and `Local-VariableTable` may be eliminated without sacrificing any information required for Java byte code interpretation.

The predefined attribute `Code` which contains all the byte codes for a particular method are moved in the corresponding `MethodInfo` structure.

### **Constraints on Java Card Virtual Machine Code**

The Java Card Virtual Machine code for a method, instance initialization method, or class or interface initialization method is stored in the array `code` of the `MethodInfo` structure of a card class file. Both the static and the structural constraints on this code array are the same as those described in the Red book.

Limitations of the Java Card Virtual Machine and Java Card class File Format

The following limitations in the Java Card Virtual Machine are imposed by this version of the Java Card Virtual Machine specification:

The per-card class file constant pool is limited to 65535 entries by the 16-bit `const_size` field of the `CardClassFile` structure (). This acts as an internal limit on the total complexity of a single card class file. This count also includes the entries corresponding to the constant pool of the class hierarchy available to the application in the card.

The amount of code per method is limited to 65535 bytes by the sizes of the indices in the `MethodInfo` structure.

The number of local variables in a method is limited to 255 by the size of the `max_local` item of the `MethodInfo` structure ().

The number of fields of a class is limited to 510 by the size of the `max_field` and the `max_sfield` items of the `ClassInfo` structure ().

The number of methods of a class is limited to 255 by the size of the `max_method` item of the `ClassInfo` structure ().

The size of an operand stack is limited to 255 words by the `max_stack` field of the `MethodInfo` structure ().

### **Bibliography**

[1] Tim Lindholm and Frank Yellin, *The Java Virtual Machine Specification*, Addison-Wesley, 1996.

**APPENDIX B****String To ID Input And Output**

For the correct operation of Card JVM it is very important that the declared and generated IDs are correctly managed. This management is controlled by the definitions in the string to ID input file **String-ID INMap**. This textual file, the basis for which is shown below, declares which areas of the namespace can be used for what purposes. One possible arrangement of this map may reserve some IDs for internal use by the Card JVM interpreter, and the rest is allocated to Card JVM applications.

```
#
# String-ID INMap file.
#
# 4000 - 7FFF Available for application use.
# F000 - FFFE Reserved for Card JVM's internal use.
#
constantBase F000 # The area from F000 to FFFF is reserved for
                  # Card JVM's internal use.
                  #
MainApplication # F000 - Name of the startup class
                # (changes for each application)
main()V        # F001 - Name of the startup method
                # (may change for each application)
java/lang/Object # F002
java/lang/String # F003
<init>()V       # F004
<clinit>()V     # F005
[L              # F006
[I              # F007
[C              # F008
[B              # F009
[S              # F000A
#
constantBase FFF0 # This area is reserved for simple return types.
L              # FFF0
```

V		# FFF1
I		# FFF2
S		# FFF3
C		# FFF4
B		# FFF5
Z		# FFF6
#		
constantBase	4000	# From here on this space is application dependent.

Essentially, all applications which are to be loaded into a smart card are allocated their own IDs within the 0x4000 to 0x7FFF. This space is free for each application since no loaded application is permitted to access other applications.

Care must be taken on managing the IDs for preloaded class libraries. The management of these IDs is helped by the (optional) generation of the string to ID output file **String-ID OUTMap** file. This map is the **String-ID INMap** augmented with the new String-ID bindings. These bindings may be produced when the Card Class File Converter application terminates. The **String-ID OUTMap** is generated for support libraries and OS interfaces loaded on the card. This map may be used as the **String-ID INMap** for smart card applications using the support libraries and OS interfaces loaded on the card. When building new applications this file can generally be discarded.



As an example consider the following Java program, HelloSmartCard.java. When compiled it generates a class file HelloSmartCard.class. This class file has embedded in it strings that represent the class name, methods and type information. On the basis of the **String-ID INMap** described above Card Class File Converter generates a card class file that replaces the strings present in the class file with IDs allocated by Card Class File Converter. Table 1 lists the strings found in the constant pool of HelloSmartCard.class with their respective Card Class File Converter assigned IDs. Note that some strings (like "java/lang/Object") have a pre-assigned value (F002) and some strings (like "()V") get a new value (4004).

Program : HelloSmartCard.java

```
public class HelloSmartCard {  
    public byte aVariable;  
  
    public static void main() {  
        HelloSmartCard h = new HelloSmartCard();  
        h.aVariable = (byte)13;  
    }  
}
```

**Relevant entries of String-ID OUTMap**

## APPENDIX C

## Byte codes supported by the Card JVM in the preferred embodiment

AALOAD	AASTORE	ACONST_NULL
ALOAD	ALOAD_0	ALOAD_1
ALOAD_2	ALOAD_3	ARETURN
ARRAYLENGTH	ASTORE	ASTORE_0
ASTORE_1	ASTORE_2	ASTORE_3
ATHROW	BALOAD	BASTORE
CHECKCAST	DUP	DUP2
DUP2_X1	DUP2_X2	DUP_X1
DUP_X2	GETFIELD	GETSTATIC
GOTO	IADD	ILOAD
IAND	IASTORE	ICONST_0
ICONST_1	ICONST_2	ICONST_3
ICONST_4	ICONST_5	ICONST_M1
IDIV	IFEQ	IFGE
IFGT	IFLE	IFLT
IFNE	IFNONNULL	IFNULL
IF_ACMPEQ	IF_ACMPEQ	IF_ICMPEQ
IF_ICMPGE	IF_ICMPGT	IF_ICMPLE
IF_ICMPLT	IF_ICMPNE	IINC
ILOAD	ILOAD_0	ILOAD_1
ILOAD_2	ILOAD_3	IMUL
INEG	INSTANCEOF	INT2BYTE
INT2CHAR	INT2SHORT	INVOKEINTERFACE
INVOKENONVIRTUAL	INVOKESTATIC	INVOKEVIRTUAL
IOR	IREM	IRETURN
ISHL	ISHR	ISTORE
ISTORE_0	ISTORE_1	ISTORE_2
ISTORE_3	ISUB	IUSHR
IXOR	JSR	LDC1
LDC2	LOOKUPSWITCH	NEW
NEWARRAY	NOP	POP
POP2	PUTFIELD	PUTSTATIC
RET	RETURN	SALOAD
SASTORE	SIPUSH	SWAP
TABLESWITCH	BIPUSH	

**Standard Java byte codes numbers for the byte codes supported in the preferred embodiment**

```
package util;
```

```
/*
```

```
* List of actual Java Bytecodes handled by this JVM
```

```
* ref. Lindohlm and Yellin.
```

```
*
```

```
* Copyright (c) 1996 Schlumberger Austin Products Center,
```

```
* Schlumberger, Austin, Texas, USA.
```

```
*/
```

```
public interface BytecodeDefn {
```

```
    public static final byte j_NOP = (byte)0;
```

```
    public static final byte ACONST_NULL = (byte)1;
```

```
    public static final byte ICONST_M1 = (byte)2;
```

```
    public static final byte ICONST_0 = (byte)3;
```

```
    public static final byte ICONST_1 = (byte)4;
```

```
    public static final byte ICONST_2 = (byte)5;
```

```
    public static final byte ICONST_3 = (byte)6;
```

```
    public static final byte ICONST_4 = (byte)7;
```

```
    public static final byte ICONST_5 = (byte)8;
```

```
    public static final byte BIPUSH = (byte)16;
```

```
    public static final byte SIPUSH = (byte)17;
```

```
    public static final byte LDC1 = (byte)18;
```

```
    public static final byte LDC2 = (byte)19;
```

```
    public static final byte ILOAD = (byte)21;
```

```
    public static final byte ALOAD = (byte)25;
```

```
    public static final byte ILOAD_0 = (byte)26;
```

```
    public static final byte ILOAD_1 = (byte)27;
```

```
    public static final byte ILOAD_2 = (byte)28;
```

```
    public static final byte ILOAD_3 = (byte)29;
```

```
    public static final byte ALOAD_0 = (byte)42;
```

```
    public static final byte ALOAD_1 = (byte)43;
```

```
public static final byte ALOAD_2 = (byte)44;
public static final byte ALOAD_3 = (byte)45;
public static final byte IALOAD = (byte)46;
public static final byte AALOAD = (byte)50;
public static final byte BALOAD = (byte)51;
public static final byte CALOAD = (byte)52;
public static final byte ISTORE = (byte)54;
public static final byte ASTORE = (byte)58;
public static final byte ISTORE_0 = (byte)59;
public static final byte ISTORE_1 = (byte)60;
public static final byte ISTORE_2 = (byte)61;
public static final byte ISTORE_3 = (byte)62;
public static final byte ASTORE_0 = (byte)75;
public static final byte ASTORE_1 = (byte)76;
public static final byte ASTORE_2 = (byte)77;
public static final byte ASTORE_3 = (byte)78;
public static final byte IASTORE = (byte)79;
public static final byte AASTORE = (byte)83;
public static final byte BASTORE = (byte)84;
public static final byte CASTORE = (byte)85;
public static final byte POP = (byte)87;
public static final byte POP2 = (byte)88;
public static final byte DUP = (byte)89;
public static final byte DUP_X1 = (byte)90;
public static final byte DUP_X2 = (byte)91;
public static final byte DUP2 = (byte)92;
public static final byte DUP2_X1 = (byte)93;
public static final byte DUP2_X2 = (byte)94;
public static final byte SWAP = (byte)95;
public static final byte IADD = (byte)96;
public static final byte ISUB = (byte)100;
public static final byte IMUL = (byte)104;
public static final byte IDIV = (byte)108;
public static final byte IREM = (byte)112;
public static final byte INEG = (byte)116;
```

```
public static final byte ISHL = (byte)120;
public static final byte ISHR = (byte)122;
public static final byte IUSHR = (byte)124;
public static final byte IAND = (byte)126;
public static final byte IOR = (byte)128;
public static final byte IXOR = (byte)130;
public static final byte IINC = (byte)132;
public static final byte INT2BYTE = (byte)145;
public static final byte INT2CHAR = (byte)146;
public static final byte INT2SHORT = (byte)147;
public static final byte IFEQ = (byte)153;
public static final byte IFNE = (byte)154;
public static final byte IFLT = (byte)155;
public static final byte IFGE = (byte)156;
public static final byte IFGT = (byte)157;
public static final byte IFLE = (byte)158;
public static final byte IF_ICMPEQ = (byte)159;
public static final byte IF_ICMPNE = (byte)160;
public static final byte IF_ICMPLT = (byte)161;
public static final byte IF_ICMPGE = (byte)162;
public static final byte IF_ICMPGT = (byte)163;
public static final byte IF_ICMPLE = (byte)164;
public static final byte IF_ACMPEQ = (byte)165;
public static final byte IF_ACMUNE = (byte)166;
public static final byte GOTO = (byte)167;
public static final byte j_JSR = (byte)168;
public static final byte RET = (byte)169;
public static final byte TABLESWITCH = (byte)170;
public static final byte LOOKUPSWITCH = (byte)171;
public static final byte IRETURN = (byte)172;
public static final byte ARETURN = (byte)176;
public static final byte RETURN = (byte)177;
public static final byte GETSTATIC = (byte)178;
public static final byte PUTSTATIC = (byte)179;
public static final byte GETFIELD = (byte)180;
```

```
public static final byte PUTFIELD = (byte)181;
public static final byte INVOKEVIRTUAL = (byte)182;
public static final byte INVOKENONVIRTUAL = (byte)183;
public static final byte INVOKESTATIC = (byte)184;
public static final byte INVOKEINTERFACE = (byte)185;
public static final byte NEW = (byte)187;
public static final byte NEWARRAY = (byte)188;
public static final byte ARRAYLENGTH = (byte)190;
public static final byte ATHROW = (byte)191;
public static final byte CHECKCAST = (byte)192;
public static final byte INSTANCEOF = (byte)193;
public static final byte IFNULL = (byte)198;
public static final byte IFNONNULL = (byte)199;
}
```

**APPENDIX D****Card Class File Converter byte code conversion process**

```
/*
 * Reprocess code block.
 */
static
void
reprocessMethod(iMethod* imeth)
{
    int pc;
    int npc;
    int align;
    bytecode* code;
    int codelen;
    int i;
    int opad;
    int npad;
    int apc;
    int high;
    int low;

    /* codeinfo is a table that keeps track of the valid Java bytecodes and their
     * corresponding translation
     */
    code = imeth->external->code;
    codelen = imeth->external->code_length;

    jumpPos = 0;
    align = 0;

    /* Scan for unsupported opcodes */
    for (pc = 0; pc < codelen; pc = npc) {
        if (codeinfo[code[pc]].valid == 0) {
            error("Unsupported opcode %d", code[pc]);
        }
    }
}
```

```

    }
    npc = nextPC(pc, code);
}

/* Scan for jump instructions an insert into jump table */
for (pc = 0; pc < codelen; pc = npc) {
    npc = nextPC(pc, code);

    if (codeinfo[code[pc]].valid == 3) {
        insertJump(pc+1, pc, (int16)((code[pc+1] << 8)|code[pc+2]));
    }
    else if (codeinfo[code[pc]].valid == 4) {
        apc = pc & -4;
        low = (code[apc+8] << 24) | (code[apc+9] << 16)
            | (code[apc+10] << 8) | code[apc+11];
        high = (code[apc+12] << 24) | (code[apc+13] << 16)
            | (code[apc+14] << 8) | code[apc+15];
        for (i = 0; i < high-low+1; i++) {
            insertJump(apc+(i*4)+18, pc,
                (int16)((code[apc+(i*4)+18] << 8) | code[apc+(i*4)+19]));
        }
        insertJump(apc+6, pc, (int16)((code[apc+6] << 8) | code[apc+7]));
    }
    else if (codeinfo[code[pc]].valid == 5) {
        apc = pc & -4;
        low = (code[apc+8] << 24) | (code[apc+9] << 16)
            | (code[apc+10] << 8) | code[apc+11];
        for (i = 0; i < low; i++) {
            insertJump(apc+(i*8)+18, pc,
                (int16)((code[apc+(i*8)+18] << 8) | code[apc+(i*8)+19]));
        }
        insertJump(apc+6, pc, (int16)((code[apc+6] << 8) | code[apc+7]));
    }
}

```



```
#ifdef TRANSLATE_BYTECODE
/* Translate specific opcodes to general ones */
for (pc = 0; pc < codelen; pc = npc) {
/* This is a translation code */
if (codeinfo[code[pc]].valid == 2) {
switch (code[pc]) {
case ILOAD_0:
case ILOAD_1:
case ILOAD_2:
case ILOAD_3:
insertSpace(code, &codelen, pc, 1);
align += 1;
code[pc+1] = code[pc] - ILOAD_0;
code[pc+0] = ILOAD;
break;

case ALOAD_0:
case ALOAD_1:
case ALOAD_2:
case ALOAD_3:
insertSpace(code, &codelen, pc, 1);
align += 1;
code[pc+1] = code[pc] - ALOAD_0;
code[pc+0] = ALOAD;
break;

case ISTORE_0:
case ISTORE_1:
case ISTORE_2:
case ISTORE_3:
insertSpace(code, &codelen, pc, 1);
align += 1;
code[pc+1] = code[pc] - ISTORE_0;
code[pc+0] = ISTORE;

```

```
break;

case ASTORE_0:
case ASTORE_1:
case ASTORE_2:
case ASTORE_3:
    insertSpace(code, &codelen, pc, 1);
    align += 1;
    code[pc+1] = code[pc] - ASTORE_0;
    code[pc+0] = ASTORE;
    break;

case ICONST_M1:
    insertSpace(code, &codelen, pc, 2);
    align += 2;
    code[pc+2] = 255;
    code[pc+1] = 255;
    code[pc+0] = SIPUSH;
    break;

case ICONST_0:
case ICONST_1:
case ICONST_2:
case ICONST_3:
case ICONST_4:
case ICONST_5:
    insertSpace(code, &codelen, pc, 2);
    align += 2;
    code[pc+2] = code[pc] - ICONST_0;
    code[pc+1] = 0;
    code[pc+0] = SIPUSH;
    break;

case LDC1:
    insertSpace(code, &codelen, pc, 1);
```

```
align += 1;  
code[pc+1] = 0;  
code[pc+0] = LDC2;  
break;
```

```

case BIPUSH:
    insertSpace(code, &codelen, pc, 1);
    align += 1;
    if ((int8)code[pc+2] >= 0) {
        code[pc+1] = 0;
    }
    else {
        code[pc+1] = 255;
    }
    code[pc+0] = SIPUSH;
    break;

case INT2SHORT:
    removeSpace(code, &codelen, pc, 1);
    align -= 1;
    npc = pc;
    continue;

}
}
else if (codeinfo[code[pc]].valid == 4 || codeinfo[code[pc]].valid == 5) {
    /* Switches are aligned to 4 byte boundaries. Since we are inserting and
    * removing bytecodes, this may change the alignment of switch instructions.
    * Therefore, we must readjust the padding in switches to compensate.
    */
    opad = (4 - (((pc+1) - align) % 4)) % 4; /* Current switch padding */
    npad = (4 - ((pc+1) % 4)) % 4; /* New switch padding */
    if (npad > opad) {
        insertSpace(code, &codelen, pc+1, npad - opad);
        align += (npad - opad);
    }
    else if (npad < opad) {
        removeSpace(code, &codelen, pc+1, opad - npad);
        align -= (opad - npad);
    }
}
}

```

```
    }

    npc = nextPC(pc, code);
}
#endif

/* Relink constants */
for (pc = 0; pc < codelen; pc = npc) {
    npc = nextPC(pc, code);
    i = (uint16)((code[pc+1] << 8) + code[pc+2]);

    switch (code[pc]) {
    case LDC2:
        /* 'i' == general index */
        switch (cltem(i).type) {
        case CONSTANT_Integer:
            i = cltem(i).v.tint;
            code[pc] = SIPUSH;
            break;

        case CONSTANT_String:
            i = buildStringIndex(i);
            break;

        default:
            error("Unsupported loading of constant type");
            break;
        }
        break;

    case NEW:
    case INSTANCEOF:
    case CHECKCAST:
        /* 'i' == class index */
```

```
    i = buildClassIndex(i);
    break;

case GETFIELD:
case PUTFIELD:
    /* 'i' == field index */
    /* i = buildFieldSignatureIndex(i); */
    i = buildStaticFieldSignatureIndex(i);
    break;

case GETSTATIC:
case PUTSTATIC:
    /* 'i' == field index */
    i = buildStaticFieldSignatureIndex(i);
    break;

case INVOKEVIRTUAL:
case INVOKENONVIRTUAL:
case INVOKESTATIC:
case INVOKEINTERFACE:
    /* 'i' == method signature index */
    i = buildSignatureIndex(i);
    break;
}

/* Insert application constant reference */
code[pc+1] = (i >> 8) & 0xFF;
code[pc+2] = i & 0xFF;
}

#ifdef MODIFY_BYTECODE
/* Translate codes */
for (pc = 0; pc < codelen; pc = npc) {
    npc = nextPC(pc, code);
}
```

```
    code[pc] = codeinfo[code[pc]].translation;
}
#endif
```

```
/* Relink jumps */
```

```
for (i = 0; i < jumpPos; i++) {
    apc = jumpTable[i].at;
    pc = jumpTable[i].from;
    npc = jumpTable[i].to - pc;
```

```
    code[apc+0] = (npc >> 8) & 0xFF;
    code[apc+1] = npc & 0xFF;
```

```
}
```

```
/* Fixup length */
```

```
imeth->external->code_length = codelen;
imeth->esize = (SIZEOFMETHOD + codelen + 3) & -4;
```

```
}
```

**APPENDIX E****Example Loading And Execution Control Program**

```
public class Bootstrap {

    // Constants used throughout the program
    static final byte BUFFER_LENGTH      = 32;
    static final byte ACK_SIZE          = (byte)1;
    static final byte ACK_CODE          = (byte)0;
    static final byte OS_HEADER_SIZE    = (byte)0x10;
    static final byte GPOS_CREATE_FILE  = (byte)0xE0;

    static final byte ST_INVALID_CLASS  = (byte)0xC0;
    static final byte ST_INVALID_PARAMETER = (byte)0xA0;
    static final byte ST_INS_NOT_SUPPORTED = (byte)0xB0;
    static final byte ST_SUCCESS        = (byte)0x00;

    static final byte ISO_COMMAND_LENGTH = (byte)5;
    static final byte ISO_READ_BINARY    = (byte)0xB0;
    static final byte ISO_UPDATE_BINARY  = (byte)0xD6;
    static final byte ISO_INIT_APPLICATION = (byte)0xF2;
    static final byte ISO_VERIFY_KEY     = (byte)0x2A;
    static final byte ISO_SELECT_FILE    = (byte)0xA4;

    static final byte ISO_CLASS          = (byte)0xC0;
    static final byte ISO_APP_CLASS      = (byte)0xF0;

    public static void main () {

        byte pBuffer[] = new byte[ISO_COMMAND_LENGTH];
        byte dbuffer[] = new byte[BUFFER_LENGTH];
        byte ackByte[] = new byte[ACK_SIZE];
        //short fileId;
        short offset;
```



```
byte bReturnStatus;

// Initialize Communications
_OS.SendATR();

do {
    // Retrieve the command header
    _OS.GetMessage(pbuffer, ISO_COMMAND_LENGTH, ACK_CODE);

    // Verify class of the message - Only ISO + Application
    if ((pbuffer[0] != ISO_APP_CLASS)
        && (pbuffer[0] != ISO_CLASS)) {
        _OS.SendStatus(ST_INVALID_CLASS);
    }
    else {
        // go through the switch
        // Send the acknowledge code

        // Verify if data length too large
        if (pbuffer[4] > BUFFER_LENGTH) {
            bReturnStatus = ST_INVALID_PARAMETER;
        }
        else
        {
            switch (pbuffer[1]) {
            case ISO_SELECT_FILE:
                // we always assume that length is 2
                if (pbuffer[4] != 2) {
                    bReturnStatus = ST_INVALID_PARAMETER;
                }
                else
                {
                    // get the fileId(offset) in the data buffer
                    _OS.GetMessage(dbuffer, (byte)2, pbuffer[1]);
                    // cast dbuffer[0..1] into a short
                }
            }
        }
    }
}
```

- 69/2 -

```
        offset = (short) ((dbuffer[0] << 8) | (dbuffer[1] & 0x00FF));
        bReturnStatus = _OS.SelectFile(offset);
    }
    break;

case ISO_VERIFY_KEY:
    // Get the Key from the terminal
    _OS.GetMessage(dbuffer, pBuffer[4], pBuffer[1]);

    bReturnStatus = _OS.VerifyKey(pBuffer[3],
                                   dbuffer,
                                   pBuffer[4]);

    break;

case ISO_INIT_APPLICATION:
    // Should send the id of a valid program file
    _OS.GetMessage(dbuffer, (byte)1, pBuffer[1]);
    // compute fileId(offset) from pBuffer[2..3] via casting
    offset = (short) ((pBuffer[2] << 8) | (pBuffer[3] & 0x00FF));
    bReturnStatus = _OS.Execute(offset,
                                   dbuffer[0]);

    break;

case GPOS_CREATE_FILE:
    if (pBuffer[4] != OS_HEADER_SIZE) {
        bReturnStatus = ST_INVALID_PARAMETER;
        break;
    }
    // Receive The data
    _OS.GetMessage(dbuffer, pBuffer[4], pBuffer[1]);
    bReturnStatus = _OS.CreateFile(dbuffer);
    break;

case ISO_UPDATE_BINARY:
    _OS.GetMessage(dbuffer, pBuffer[4], pBuffer[1]);
    // compute offset from pBuffer[2..3] via casting
```

```
    offset = (short) ((pbuffer[2] << 8) | (pbuffer[3] & 0x00FF));
    // assumes that a file is already selected
    bReturnStatus = _OS.WriteBinaryFile (offset,
                                         pbuffer[4],
                                         dbuffer);

    break;
case ISO_READ_BINARY:
    // compute offset from pbuffer[2..3] via casting
    offset = (short) ((pbuffer[2] << 8) | (pbuffer[3] & 0x00FF));
    // assumes that a file is already selected
    bReturnStatus = _OS.ReadBinaryFile (offset,
                                         pbuffer[4],
                                         dbuffer);

    // Send the data if successful
    ackByte[0] = pbuffer[1];
    if (bReturnStatus == ST_SUCCESS) {
        _OS.SendMessage(ackByte, ACK_SIZE);
        _OS.SendMessage(dbuffer, pbuffer[4]);
    }
    break;
default:
    bReturnStatus = ST_INS_NOT_SUPPORTED;
}
}
_OS.SendStatus(bReturnStatus);
}
}
while (true);
}
}
```

**APPENDIX F****Methods For Accessing Card Operating System Capabilities In The Preferred Embodiment**

```
public class _OS {

    static native byte    SelectFile    (short file_id);
    static native byte    SelectParent  ();
    static native byte    SelectCD     ();
    static native byte    SelectRoot   ();

    static native byte    CreateFile   (byte file_hdr[]);
    static native byte    DeleteFile   (short file_id);

    // General File Manipulation
    static native byte    ResetFile    ();
    static native byte    ReadByte     (byte offset);
    static native short   ReadWord     (byte offset);

    // Header Manipulation
    static native byte    GetFileInfo   (byte file_hdr[]);

    // Binary File support
    static native byte    ReadBinaryFile (short offset,
                                         byte data_length,
                                         byte buffer[]);
    static native byte    WriteBinaryFile (short offset,
                                         byte data_length,
                                         byte buffer[]);

    // Record File support
    static native byte    SelectRecord  (byte record_nb,
                                         byte mode);
    static native byte    NextRecord   ();
    static native byte    PreviousRecord ();
}
```

```
static native byte    ReadRecord      (byte record_data[],
                                       byte record_nb,
                                       byte offset,
                                       byte length);

static native byte    WriteRecord     (byte buffer[],
                                       byte record_nb,
                                       byte offset,
                                       byte length);

// Cyclic File Support
static native byte    LastUpdatedRec  ();

// Messaging Functions
static native byte    GetMessage     (byte buffer[],
                                       byte expected_length,
                                       byte ack_code);

static native byte    SendMessage    (byte buffer[],
                                       byte data_length);

static native byte    SetSpeed       (byte speed);

// Identity Management
static native byte    CheckAccess     (byte ac_action);
static native byte    VerifyKey       (byte key_number,
                                       byte key_buffer[],
                                       byte key_length);

static native byte    VerifyCHV      (byte CHV_number,
                                       byte CHV_buffer[],
                                       byte unblock_flag);

static native byte    ModifyCHV      (byte CHV_number,
                                       byte old_CHV_buffer[],
                                       byte new_CHV_buffer[],
                                       byte unblock_flag);
```

```
static native byte   GetFileStatus   ();
static native byte   SetFileStatus   (byte file_status);

static native byte   GrantSupervisorMode ();
static native byte   RevokeSupervisorMode();

static native byte   SetFileACL      (byte file_acl[]);
static native byte   GetFileACL      (byte file_acl[]);

// File context manipulation
static native void   InitFileStatus   ();
static native void   BackupFileStatus ();
static native void   RestoreFileStatus ();

// Utilities
static native byte   CompareBuffer    (byte pattern_length,
                                       byte buffer_1[],
                                       byte buffer_2[]);
static native short  AvailableMemory ();
static native void   ResetCard        (byte mode);
static native byte   SendATR          ();
static native byte   SetDefaultATR    (byte buffer[],
                                       byte length);
static native byte   Execute          (short file_id,
                                       byte flag);

// Global state variable functions
static native byte   GetIdentity      ();
static native byte   GetRecordNb     ();
static native short  GetApplicationId ();
static native byte   GetRecordLength ();
static native byte   GetFileType     ();
static native short  GetFileLength   ();
static native void   SendStatus      (byte status);
```

}

## APPENDIX G

### Byte Code Attributes Tables

#### Dividing Java byte codes into type groups

Each bytecode is assigned a 5 bit type associated with it. This is used to group the codes into similarly behaving sets. In general this behaviour reflects how the types of byte codes operate on the stack, but types 0, 13, 14, and 15 reflect specific kinds of instructions as denoted in the comments section.

The table below illustrates the state of the stack before and after each type of instruction is executed.

<u>Type</u>	<u>Before execution</u>	<u>After execution</u>	<u>Comment</u>
0			Illegal instruction
1	stk0==int stk1==int	pop(1)	
2	stk0==int	pop(1)	
3	stk0==int stk1==int	pop(2)	
4			
5	push(1)		
6	stk0==int stk1==int	pop(3)	
7	stk0==int	pop(1)	
8	stk0==ref	pop(1)	
9	stk0==int	pop(1)	
10	push(1)	stk0<-int	
11	push(1)	stk0<-ref	
12	stk0==ref	stk0<-int	
13			DUPs, SWAP instructions
14			INVOKE instructions
15			FIELDS instructions
16		stk0<-ref	



### Using Standard Java Byte Code (without reordering) - Attribute Lookup Table

```

/*
 * Table of bytecode decode information. This contains a bytecode type
 * and a bytecode length. We currently support all standard bytecodes
 * (ie. no quicks) which gives us codes 0 to 201 (202 codes in all).
 */

#define      T_      0
#define      T3      1
#define      T6      2
#define      T1      3
#define      T2      4
#define      T7      5
#define      T9      6
#define      T8      7
#define      T12     8
#define      T10     9
#define      T5      10
#define      T11     11
#define      T16     12
#define      T4      13
#define      T13     14
#define      T14     15
#define      T15     16

#define      D(T,L)
#define      _BUILD_ITYPE_AND_ILENGTH(T, L)
#define      _BUILD_ITYPE_AND_ILENGTH(T,L)
(_BUILD_ITYPE(T)|_BUILD_ILENGTH(L))
#define      _BUILD_ITYPE(T)          ((T) << 3)
#define      _BUILD_ILENGTH(L)       (L)
#define      _GET_ITYPE(I)            ((I) & 0xF8)
#define      _GET_ILENGTH(I)         ((I) & 0x07)

```

```

const uint8 _SCODE_decodeinfo[256] = {
    D( T4 , 1 ),      /* NOP          */
    D( T11 , 1 ),    /* ACONST_NULL */
    D( T10 , 1 ),    /* ICONST_M1   */
    D( T10 , 1 ),    /* ICONST_0    */
    D( T10 , 1 ),    /* ICONST_1    */
    D( T10 , 1 ),    /* ICONST_2    */
    D( T10 , 1 ),    /* ICONST_3    */
    D( T10 , 1 ),    /* ICONST_4    */
    D( T10 , 1 ),    /* ICONST_5    */
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T10 , 2 ),    /* BIPUSH     */
    D( T10 , 3 ),    /* SIPUSH     */
    D( T_ , 2 ),     /* LDC1       */
    D( T11 , 3 ),    /* LDC2       */
    D( T_ , 3 ),
    D( T5 , 2 ),     /* ILOAD      */
    D( T_ , 2 ),
    D( T_ , 2 ),
    D( T_ , 2 ),
    D( T5 , 2 ),     /* ALOAD      */
    D( T5 , 1 ),     /* ILOAD_0    */
    D( T5 , 1 ),     /* ILOAD_1    */
    D( T5 , 1 ),     /* ILOAD_2    */
    D( T5 , 1 ),     /* ILOAD_3    */
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T_ , 1 ),
    D( T_ , 1 ),

```

```
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T5 , 1),      /* ALOAD_0 */
D(T5 , 1),      /* ALOAD_1 */
D(T5 , 1),      /* ALOAD_2 */
D(T5 , 1),      /* ALOAD_3 */
D(T_ , 1),      /* IALOAD */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),      /* AALOAD */
D(T7 , 1),      /* BALOAD */
D(T_ , 1),      /* CALOAD */
D(T7 , 1),      /* SALOAD */
D(T2 , 2),      /* ISTORE */
D(T_ , 2),
D(T_ , 2),
D(T_ , 2),
D(T8 , 2),      /* ASTORE */
D(T2 , 1),      /* ISTORE_0 */
D(T2 , 1),      /* ISTORE_1 */
D(T2 , 1),      /* ISTORE_2 */
D(T2 , 1),      /* ISTORE_3 */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
```

```

D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T8 , 1),      /* ASTORE_0      */
D(T8 , 1),      /* ASTORE_1      */
D(T8 , 1),      /* ASTORE_2      */
D(T8 , 1),      /* ASTORE_3      */
D(T_ , 1),      /* IASTORE */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),      /* AASTORE      */
D(T6 , 1),      /* BASTORE      */
D(T_ , 1),      /* CASTORE      */
D(T6 , 1),      /* SASTORE      */
D(T2 , 1),      /* POP          */
D(T3 , 1),      /* POP2         */
D(T13 , 1),     /* DUP          */
D(T13 , 1),     /* DUP_X1      */
D(T13 , 1),     /* DUP_X2      */
D(T13 , 1),     /* DUP2        */
D(T13 , 1),     /* DUP2_X1     */
D(T13 , 1),     /* DUP2_X2     */
D(T13 , 1),     /* SWAP        */
D(T1 , 1),      /* IADD        */
D(T_ , 1),
D(T_ , 1),
D(T1 , 1),
D(T_ , 1),      /* ISUB        */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),

```

```
D(T1 , 1),      /* IMUL      */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T1 , 1),      /* IDIV      */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T1 , 1),      /* IREM      */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T9 , 1),      /* INEG      */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T1 , 1),      /* ISHL      */
D(T_ , 1),
D(T1 , 1),      /* ISHR      */
D(T_ , 1),
D(T1 , 1),      /* IUSHR     */
D(T_ , 1),
D(T1 , 1),      /* IAND      */
D(T_ , 1),
D(T1 , 1),      /* IOR       */
D(T_ , 1),
D(T1 , 1),      /* IXOR      */
D(T_ , 1),
D(T4 , 3),      /* IINC      */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
```

```

D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T9 , 1),      /* INT2BYTE      */
D(T9 , 1),      /* INT2CHAR       */
D(T_ , 1),      /* INT2SHORT      */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T2 , 3),      /* IFEQ           */
D(T2 , 3),      /* IFNE           */
D(T2 , 3),      /* IFLT           */
D(T2 , 3),      /* IFGE           */
D(T2 , 3),      /* IFGT           */
D(T2 , 3),      /* IFLT           */
D(T3 , 3),      /* IF_ICMPEQ     */
D(T3 , 3),      /* IF_ICMPNE     */
D(T3 , 3),      /* IF_ICMPLT     */
D(T3 , 3),      /* IF_ICMPGE     */
D(T3 , 3),      /* IF_ICMPGT     */
D(T3 , 3),      /* IF_ICMPLE     */
D(T3 , 3),      /* IF_ACMPEQ     */
D(T3 , 3),      /* IF_ACMPNE     */
D(T4 , 3),      /* GOTO           */
D(T_ , 3),      /* JSR            */
D(T_ , 2),      /* RET            */
D(T2 , 0),      /* TABLESWITCH  */
D(T2 , 0),      /* LOOKUPSWITCH*/
D(T2 , 1),      /* IRETURN      */
D(T_ , 1),

```

```

D(T_ , 1),
D(T_ , 1),
D(T8 , 1),      /* ARETURN      */
D(T4 , 1),      /* RETURN      */
D(T15 , 3),     /* GETSTATIC   */
D(T15 , 3),     /* PUTSTATIC   */
D(T15 , 3),     /* GETFIELD    */
D(T15 , 3),     /* PUTFIELD    */
D(T14 , 3),     /* INVOKEVIRTUAL */
D(T14 , 3),     /* INVOKESPECIAL */
D(T14 , 3),     /* INVOKESTATIC */
D(T14 , 5),     /* INVOKEINTERFACE */
D(T_ , 1),
D(T11 , 3),     /* NEW          */
D(T16 , 2),     /* NEWARRAY     */
D(T_ , 3),
D(T12 , 1),     /* ARRAYLENGTH */
D(T8 , 1),      /* ATHROW      */
D(T16 , 3),     /* CHECKCAST   */
D(T12 , 3),     /* INSTANCEOF  */
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 4),
D(T8 , 3),      /* IFNULL      */
D(T8 , 3),      /* IFNONNULL   */
D(T_ , 5),
D(T_ , 5),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),
D(T_ , 1),

```





D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),  
D(T\_ , 1),

};

## APPENDIX H

### Checks Done On Java Byte Codes By Type

Decoding the instruction. This gives us the length to generate the next PC, and the instruction type:

```
pcarg1 = _GET_ILENGTH(_decodeinfo[insn]);
itype = _GET_ITYPE(_decodeinfo[insn]);
```

Implement some pre-execution checks based on this:

```
/* Check the input stack state based on the instruction type */
if (itype <= ITYPE9) {
    if (itype <= ITYPE1) {
        check_stack_int(1);
    }
    check_stack_int(0);
}
else if (itype <= ITYPE12) {
    check_stack_ref(0);
}
else if (itype < ITYPE11) {
    push(1);
}
}
```

Finally, implement some post execution checks:

```
/* Set the output state */
if (itype <= ITYPE8) {
    if (itype <= ITYPE6) {
        if (itype >= ITYPE6) {
            pop(1);
        }
    }
}
```

```
        pop(1);
    }
    pop(1);
}
else if (itype <= ITYPE10) {
    set_stack_int(0);
}
else if (itype >= ITYPE11 && itype <= ITYPE16) {
    set_stack_ref(0);
}
```

## APPENDIX I

### Checks Done On Renumbered Java Byte Codes

Get the instruction. The numeric value of the instruction implicitly contains the instruction type:

```
insn = getpc(-1);
```

Implement some pre-execution checks based on this:

```
/*
 * Check input stack state. By renumbering the byte codes we can
 * perform the necessary security checks by testing if the value of the
 * byte code (and hence the byte code) belongs to the correct group
 */
if (insn <= TYPE9_END) {
    if (insn <= TYPE1_END) {
        check_stack_int(1);
    }
    check_stack_int(0);
}
else if (insn <= TYPE12_END) {
    check_stack_ref(0);
}
else if (insn <= TYPE11_END) {
    push(1)
}
}
```

Finally, implement some post execution checks:

```
/*
```

```
* Set output stack state.  
*/  
if (insn <= TYPE8_END) {  
    if (insn <= TYPE6_END) {  
        if (insn >= TYPE6_START) {  
            pop(1);  
        }  
        pop(1);  
    }  
    pop(1);  
}  
else if (insn <= TYPE10_END) {  
    set_stack_int(0);  
}  
else if (insn >= TYPE11_START && insn <= TYPE16_END) {  
    set_stack_ref(0);  
}
```

**Reordering of supported Java byte codes by type**

```
/* TYPE 3 */
```

```
#define s_POP2      0
#define s_IF_ICMPEQ  1
#define s_IF_ICMPNE  2
#define s_IF_ICMPLT  3
#define s_IF_ICMPGE  4
#define s_IF_ICMPGT  5
#define s_IF_ICMPLE  6
#define s_IF_ACMPEQ  7
#define s_IF_ACMPNE  8
```

```
/* TYPE 6 */
```

```
#define TYPE6_START  9

#define s_SASTORE    9
#define s_AASTORE    10
#define s_BASTORE    11

#define TYPE6_END    12
```

```
/* TYPE 1 */
```

```
#define s_IADD      13
#define s_ISUB      14
#define s_IMUL      15
#define s_IDIV      16
#define s_IREM      17
#define s_ISHL      18
#define s_ISHR      19
#define s_IUSHR     20
#define s_IAND      21
```

```
#define s_IOR      22
#define s_IXOR    23

#define TYPE1_END  23

/* TYPE 2 */

#define s_ISTORE  24
#define s_POP     25
#define s_IFEQ    26
#define s_IFNE    27
#define s_IFLT    28
#define s_IFGE    29
#define s_IFGT    30
#define s_IFLE    31
#define s_TABLESWITCH  32
#define s_LOOKUPSWITCH 33
#define s_IRETURN  34

/* TYPE 7 */

#define s_SALOAD  35
#define s_AALOAD  36
#define s_BALOAD  37

/* TYPE 9 */

#define s_INEG    39
#define s_INT2BYTE 40
#define s_INT2CHAR 41

#define TYPE9_END 41

/* TYPE 8 */
```

```
#define s_ASTORE      42
#define s_ARETURN    43
#define s_ATHROW     44
#define s_IFNULL     45
#define s_IFNONNULL  46

#define TYPE8_END    46

/* TYPE 12 */

#define s_ARRAYLENGTH 47
#define s_INSTANCEOF 48

#define TYPE12_END   48

/* TYPE 10 */

#define s_SIPUSH     49

#define TYPE10_END   49

/* TYPE 5 */

#define s_ILOAD      50
#define s_ALOAD      51

/* TYPE 11 */

#define TYPE11_START 52

#define s_ACONST_NULL 52
#define s_LDC2         53
#define s_JSR          54
#define s_NEW          55
```



```
#define TYPE11_END    55
```

```
/* TYPE 16 */
```

```
#define s_NEWARRAY    56
```

```
#define s_CHECKCAST   57
```

```
#define TYPE16_END    57
```

```
/* TYPE 13 */
```

```
#define s_DUP          58
```

```
#define s_DUP_X1       59
```

```
#define s_DUP_X2       60
```

```
#define s_DUP2         61
```

```
#define s_DUP2_X1      62
```

```
#define s_DUP2_X2      63
```

```
#define s_SWAP         64
```

```
/* TYPE 14 */
```

```
#define s_INVOKEVIRTUAL 65 /* 01000001 */
```

```
#define s_INVOKENONVIRTUAL 66 /* 01000010 */
```

```
#define s_INVOKESTATIC  67 /* 01000011 */
```

```
#define s_INVOKEINTERFACE 68 /* 01000100 */
```

```
/* TYPE 15 */
```

```
#define s_GETSTATIC     69
```

```
#define s_PUTSTATIC     70
```

```
#define s_GETFIELD      71
```

```
#define s_PUTFIELD      72
```

```
/* TYPE 4 */
```

```
#define s_NOP      73
#define s_IINC     74
#define s_GOTO     75
#define s_RET      76
#define s_RETURN   77
```

What is claimed is:

1. An integrated circuit card for use with a terminal, comprising:
  - a communicator configured to communicate with  
5 the terminal;
  - a memory storing:
    - an application having a high level programming language format, and
    - an interpreter; and
  - 10 a processor coupled to the memory, the processor configured to use the interpreter to interpret the application for execution and to use the communicator to communicate with the terminal.
2. The integrated circuit card of claim 1,  
15 wherein the high level programming language format comprises a class file format.
3. The integrated circuit card of claim 1 wherein the processor comprises a microcontroller.
4. The integrated circuit card of claim 1  
20 wherein at least a portion of the memory is located in the processor.
5. The integrated circuit card of claim 1 wherein the high level programming language format comprises a Java programming language format.

6. The integrated circuit card of claim 1,  
wherein

the application has been processed from a  
second application having a string of characters, and  
5 the string of characters is represented in  
the first application by an identifier.

7. The integrated circuit card of claim 6,  
wherein the identifier comprises an integer.

8. The integrated circuit card of claim 1  
10 wherein the processor is further configured to:  
receive a request from a requester to access  
an element of the card;  
after receipt of the request, interact with  
the requester to authenticate an identity of the  
15 requester; and  
based on the identity, selectively grant  
access to the element.

9. The integrated circuit card of claim 8,  
wherein the requester comprises the processor.

20 10. The integrated circuit card of claim 8,  
wherein the requester comprises the terminal.

11. The integrated circuit card of claim 8,  
wherein  
the element comprises the application stored  
25 in the memory, and  
once access is allowed, the requester is  
configured to use the application.

12. The integrated circuit card of claim 8,  
wherein

the element comprises another application stored in the memory.

13. The integrated circuit card of claim 8, wherein the element includes data stored in the memory.

5 14. The integrated circuit card of claim 8 wherein the element comprises the communicator.

15 15. The integrated circuit card of claim 8, wherein the memory also stores an access control list for the element, the access control list furnishing an  
10 indication of types of access to be granted to the identity, the processor further configured to:  
based on the access control list,  
selectively grant specific types of access to the requester.

15 16. The integrated circuit card of claim 15 wherein the types of access include reading data.

17. The integrated circuit card of claim 15 wherein the types of access include writing data.

20 18. The integrated circuit card of claim 15 wherein the types of access include appending data.

19. The integrated circuit card of claim 15 wherein the types of access include creating data.

20. The integrated circuit card of claim 15 wherein the types of access include deleting data.

25 21. The integrated circuit card of claim 15 wherein the types of access include executing an application.

22. The integrated circuit card of claim 1, wherein the application is one of a plurality of applications stored in the memory, the processor is further configured to:

5                   receive a request from a requester to access one of the plurality of applications;  
                  after receipt of the request, determine whether said one of the plurality of applications complies with a predetermined set of rules; and  
10                   based on the determination, selectively grant access to the requester to said one of the plurality of applications.

23. The integrated circuit card of claim 22, wherein the predetermined rules provide a guide for  
15 determining whether said one of the plurality of applications accesses a predetermined region of the memory.

24. The integrated circuit card of claim 22, wherein the processor is further configured to:  
20                   authenticate an identity of the requester; and  
                  grant access to said one of the plurality of applications based on the identity.

25. The integrated circuit card of claim 1, wherein the processor is further configured to:  
25                   interact with the terminal via the communicator to authenticate an identity; and  
                  determine if the identity has been authenticated; and  
                  based on the determination, selectively allow  
30 communication between the terminal and the integrated circuit card.

26. The integrated circuit card of claim 25,  
wherein the communicator and the terminal communicate via  
communication channels, the processor further configured  
to assign one of the communication channels to the  
5 identity when the processor allows the communication  
between the terminal and the integrated circuit card.

27. The integrated circuit card of claim 26,  
wherein the processor is further configured to:  
assign a session key to said one of the  
10 communication channels, and  
use the session key when the processor and the  
terminal communicate via said one of the communication  
channels.

28. The integrated circuit card of claim 1,  
15 wherein the terminal has a card reader and the  
communicator comprises a contact for communicating with  
the card reader.

29. The integrated circuit card of claim 1,  
wherein the terminal has a wireless communication device  
20 and the communicator a wireless transceiver for  
communicating with the wireless communication device.

30. The integrated circuit card of claim 1,  
wherein the terminal has a wireless communication device  
and the communicator comprises a wireless transmitter for  
25 communicating with the wireless communication device.

31. A method for use with an integrated circuit card and a terminal, comprising:

storing an interpreter and an application having a high level programming language format in a

5 memory of the integrated circuit card; and

using a processor of the integrated circuit card to use the interpreter to interpret the application for execution; and

10 using a communicator of the card when communicating between the processor and the terminal.

32. The method of claim 31, wherein the high level programming language format comprises a class file format.

33. The method of claim 31, wherein the processor  
15 comprises a microcontroller.

34. The method of claim 31, wherein at least a portion of the memory is located in the processor.

35. The method of claim 31, wherein the high level programming language format comprises a Java  
20 programming language format.

36. The method of claim 1, wherein  
the application has been processed from a second application having a string of characters, further comprising:  
25 representing the string of characters in the first application by an identifier.

37. The method of claim 36, wherein the identifier includes an integer.



38. The method of claim 31, further comprising:  
receiving a request from a requester to  
access an element of the card;

5 after receipt of the request, interacting  
with the requester to authenticate an identity of the  
requester; and

based on the identity, selectively granting  
access to the element.

39. The method of claim 38, wherein the requester  
10 comprises the processor.

40. The method of claim 38, wherein the requester  
comprises the terminal.

41. The method of claim 38, wherein the element  
comprises the application stored in the memory, further  
15 comprising:

once access is allowed, using the application  
with the requester.

42. The method of claim 38, wherein the element  
comprises another application stored in the memory.

20 43. The method of claim 38, wherein the element  
includes data stored in the memory.

44. The method of claim 38, wherein the element  
comprises the communicator.

45. The method of claim 38, wherein the memory also stores an access control list for the element, the access control list furnishing an indication of types of access to be granted to the identity, further comprising:

5 based on the access control list, using the processor to selectively grant specific types of access to the requester.

46. The method of claim 45, wherein the types of access include reading data.

10 47. The method of claim 45, wherein the types of access include writing data.

48. The method of claim 45, wherein the types of access include appending data.

15 49. The method of claim 45, wherein the types of access include creating data.

50. The method of claim 45, wherein the types of access include deleting data.

51. The method of claim 45, wherein the types of access including executing an application.

52. The method of claim 31, wherein the application is one of a plurality of applications stored in the memory, further comprising:

receiving a request from a requester to access one  
5 of the applications stored in the memory;

upon receipt of the request, determining whether said one of the plurality of applications complies with a predetermined set of rules; and

based on the determining, selectively  
10 granting access to the said one of the plurality of applications.

53. The method of claim 52, wherein the predetermined rules provide a guide for determining whether said one of the plurality of applications  
15 accesses a predetermined region of the memory.

54. The method of claim 52, further comprising:  
authenticating an identity of the requester; and  
based on the identity, granting access to said  
one of the plurality of applications.

20 55. The method of claim 31, further comprising:  
communicating with the terminal to  
authenticate an identity;

determining if the identity has been  
authenticated; and

25 based on the determining, selectively  
allowing communication between the terminal and the  
integrated circuit card.

56. The method of claim 55, further comprising:  
communicating between the terminal and the  
processor via communication channels; and  
assigning one of the communication channels  
5 to the identity when the allowing allows communication  
between the card reader and the integrated circuit card.

57. The method of claim 56, further comprising:  
assigning a session key to said one of the  
communication channels; and  
10 using the session key when the processor and  
the terminal communicate via said one of the  
communication channels.

58. A smart card comprising:  
a memory storing a Java interpreter; and  
a processor configured to use the interpreter  
to interpret a Java application for execution.

5 59. A microcontroller comprising:  
a semiconductor substrate;  
a memory located in the substrate;  
a programming language interpreter stored in  
the memory and configured to implement security checks;  
10 and  
a central processing unit located in the  
substrate and coupled to the memory.

60. The microcontroller of claim 59, wherein the  
interpreter comprises a Java byte code interpreter.

15 61. The microcontroller of claim 59, wherein the  
security checks comprise establishing firewalls.

62. The microcontroller of claim 59, wherein the  
security checks comprise enforcing a sandbox security  
model.

20 63. A smart card comprising:  
a memory;  
a programming language interpreter stored in  
the memory and configured to implement security checks;  
and  
25 a central processing unit coupled to the  
memory.

64. The smart card of claim 63, wherein the  
interpreter comprises a Java byte code interpreter.

65. The smart card of claim 63, wherein the security checks comprise establishing firewalls.

66. The smart card of claim 63, wherein the security checks comprise enforcing a sandbox security  
5 model.

67. An integrated circuit card for use with a terminal, comprising:  
a communicator;  
a memory storing an interpreter and first  
10 instructions of a first application, the first instructions having been converted from second instructions of a second application; and  
a processor coupled to the memory and  
configured to use the interpreter to execute the first  
15 instructions and to communicate with the terminal via the communicator.

68. The integrated circuit card of claim 67, wherein the first application has a class file format.

69. The integrated circuit card of claim 67,  
20 wherein the second application has a class file format.

70. The integrated circuit card of claim 67, wherein the first instructions comprise byte codes.

71. The integrated circuit card of claim 67, wherein the second instructions comprise byte codes.

25 72. The integrated circuit card of claim 67, wherein the first instructions comprise Java byte codes.

73. The integrated circuit card of claim 67,  
wherein the second instructions comprise Java byte codes.

74. The integrated circuit card of claim 67,  
wherein the first instructions comprise generalized  
5 versions of the second instructions.

75. The integrated circuit card of claim 67,  
wherein the first instructions comprise renumbered  
versions of the second instructions.

76. The integrated circuit card of claim 67,  
10 wherein  
the second instructions include constant  
references, and  
the first instructions include constants that  
replace the constant references of the second  
15 instructions.

77. The integrated circuit card of claim 67,  
wherein  
the second instructions include references, the  
references shifting location during the conversion of the  
20 second instructions to the first instructions, and  
the first instructions are relinked to the  
references after the shifting.

78. The integrated circuit card of claim 67,  
wherein  
25 the first instructions comprise byte codes for a  
first type of virtual machine, and  
the second instructions comprise byte codes for a  
second type of virtual machine, the first type being  
different from the second type.

79. A method for use with an integrated circuit card, comprising:

converting second instructions of a second application to first instructions of a first application;

5 storing the first instructions in a memory of the integrated circuit card; and

using an interpreter of the integrated circuit card to execute the first instructions.

80. The method of claim 79, wherein the first  
10 application has a class file format.

81. The method of claim 79, wherein the second application has a class file format.

82. The method of claim 79, wherein the first instructions comprise byte codes.

15 83. The method of claim 79, wherein the second instructions comprise byte codes.

84. The method of claim 79, wherein the first instructions comprise Java byte codes.

20 85. The method of claim 79, wherein the second instructions comprise Java byte codes.

86. The method of claim 79, wherein the first instructions are generalized versions of the second instructions.

25 87. The method of claim 79, wherein the converting includes renumbering the second instructions to form first instructions.



88. The method of claim 79, wherein the second instructions include constant references, and the converting includes replacing the constant references of the second instructions with constants.

5 89. The method of claim 79, wherein the second instructions include references and the converting includes shifting location of the references, further comprising:

10 relinking the first instructions to the references after the converting.

90. The method of claim 79, wherein the first instructions comprise byte codes for a first type of virtual machine, and the second instructions comprise byte codes for a second type of virtual machine, the first type being different from the second type.

91. An integrated circuit for use with a terminal, comprising:

a communicator configured to communicate with the terminal;

5 a memory storing a first application that has been processed from a second application having a string of characters, the string of characters being represented in the first application by an identifier; and

10 a processor coupled to the memory, the processor configured to use the interpreter to interpret the first application for execution and to use the communicator to communicate with the terminal.

92. The integrated circuit card of claim 91, wherein the identifier comprises an integer.

15 93. A method for use with an integrated circuit card and a terminal comprising:

processing a second application to create a first application, the second application having a string of characters;

20 representing the string of characters of the first application by an identifier in the second application;

storing an interpreter and the first application in a memory of the integrated circuit card; and

25 using a processor of the integrated circuit card to use an interpreter to interpret the first application for execution.

94. The method of claim 93, wherein the identifier includes an integer.

95. A microcontroller comprising:  
a memory storing:  
an application having a class file  
format, and  
5 an interpreter; and  
a processor coupled to the memory, the  
processor configured to use the interpreter to interpret  
the application for execution.

96. The microcontroller of claim 95, further  
10 comprising:  
a communicator configured to communicate with a  
terminal.

97. The microcontroller of claim 96, wherein the  
terminal has a card reader and the communicator comprises  
15 a contact for communicating with the card reader.

98. The microcontroller of claim 96, wherein the  
terminal has a wireless communication device and the  
communicator a wireless transceiver for communicating with  
the wireless communication device.

20 99. The microcontroller of claim 96, wherein the  
terminal has a wireless communication device and the  
communicator comprises a wireless transmitter for  
communicating with the wireless communication device.

100. The microcontroller of claim 95, wherein the  
25 class file format comprises a Java class file format.

101. A method for use with an integrated circuit card, comprising:

storing a first application in a memory of the integrated circuit card;

5 storing a second application in the memory of the integrated circuit card; and

creating a firewall that isolates the first and second applications so that the second application cannot access either the first application or data associated  
10 with the first application.

102. The method of claim 101, wherein the first and second applications comprise Java byte codes.

103. The method of claim 100, wherein the creating includes using a Java interpreter.

15 104. The method of claim 101, wherein the storing of the first application is performed in association with manufacture of the integrated circuit card; and  
the storing of the second application is performed  
20 at a later time after the manufacture is completed.

105. An integrated circuit card for use with a terminal, comprising:

a communicator configured to communicate with the terminal;

5 a memory storing:

applications, each application having a high level programming language format, and

an interpreter; and

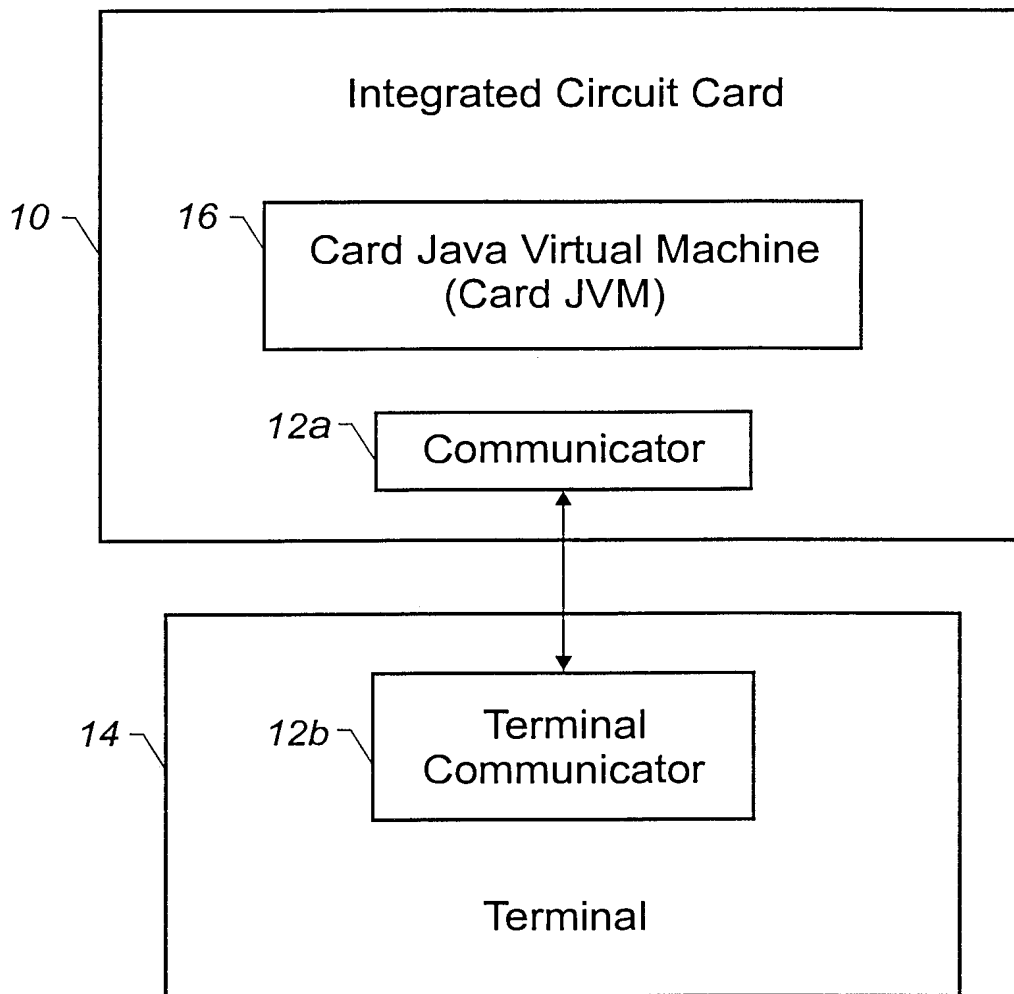
10 a processor coupled to the memory, the processor configured to:

a.) use the interpreter to interpret the applications for execution,

b.) use the interpreter to create a firewall to isolate the applications from each other, and

15 c.) use the communicator to communicate with the terminal.

1/23



**FIGURE 1**

2/23

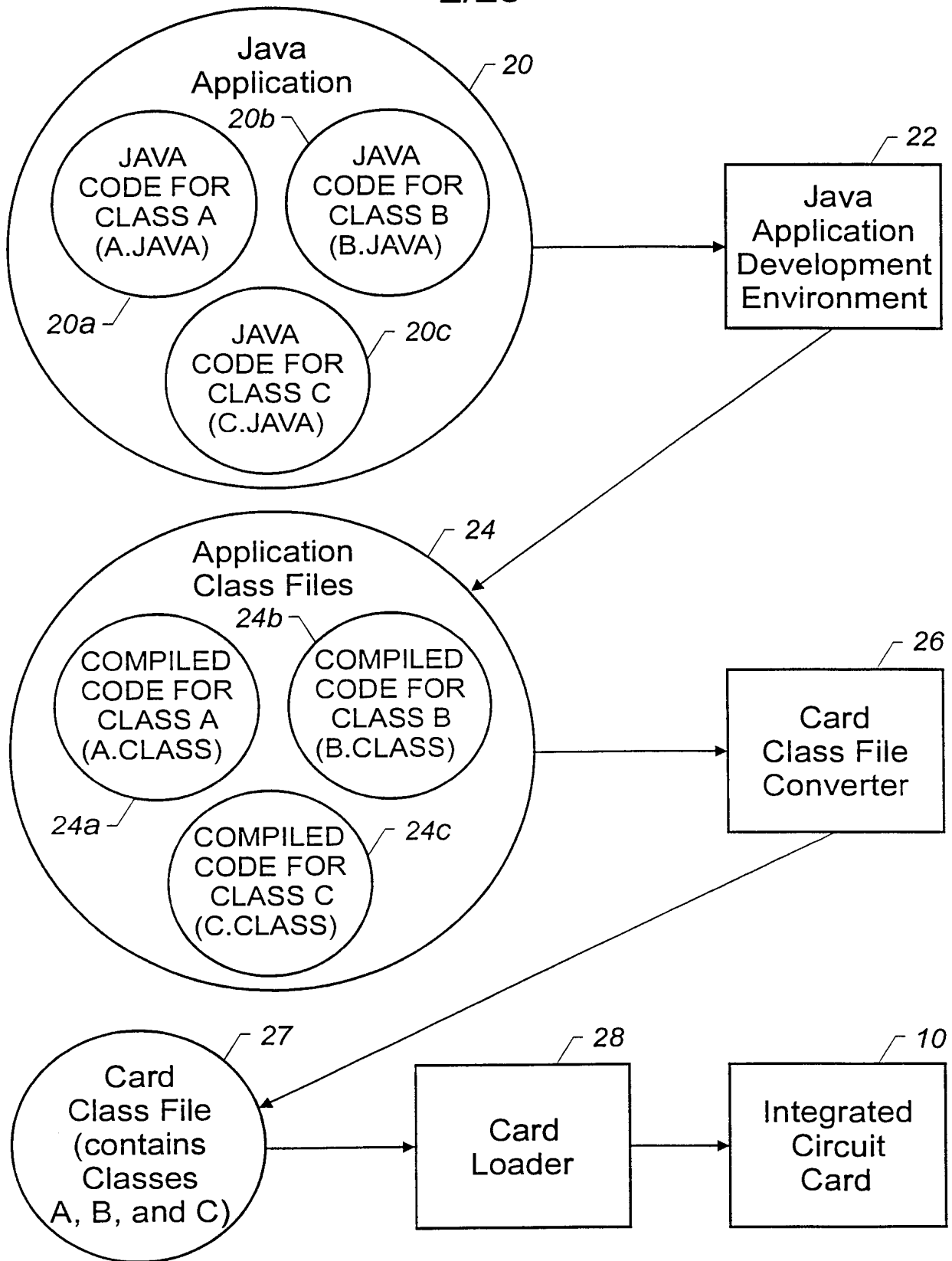


FIGURE 2

3/23

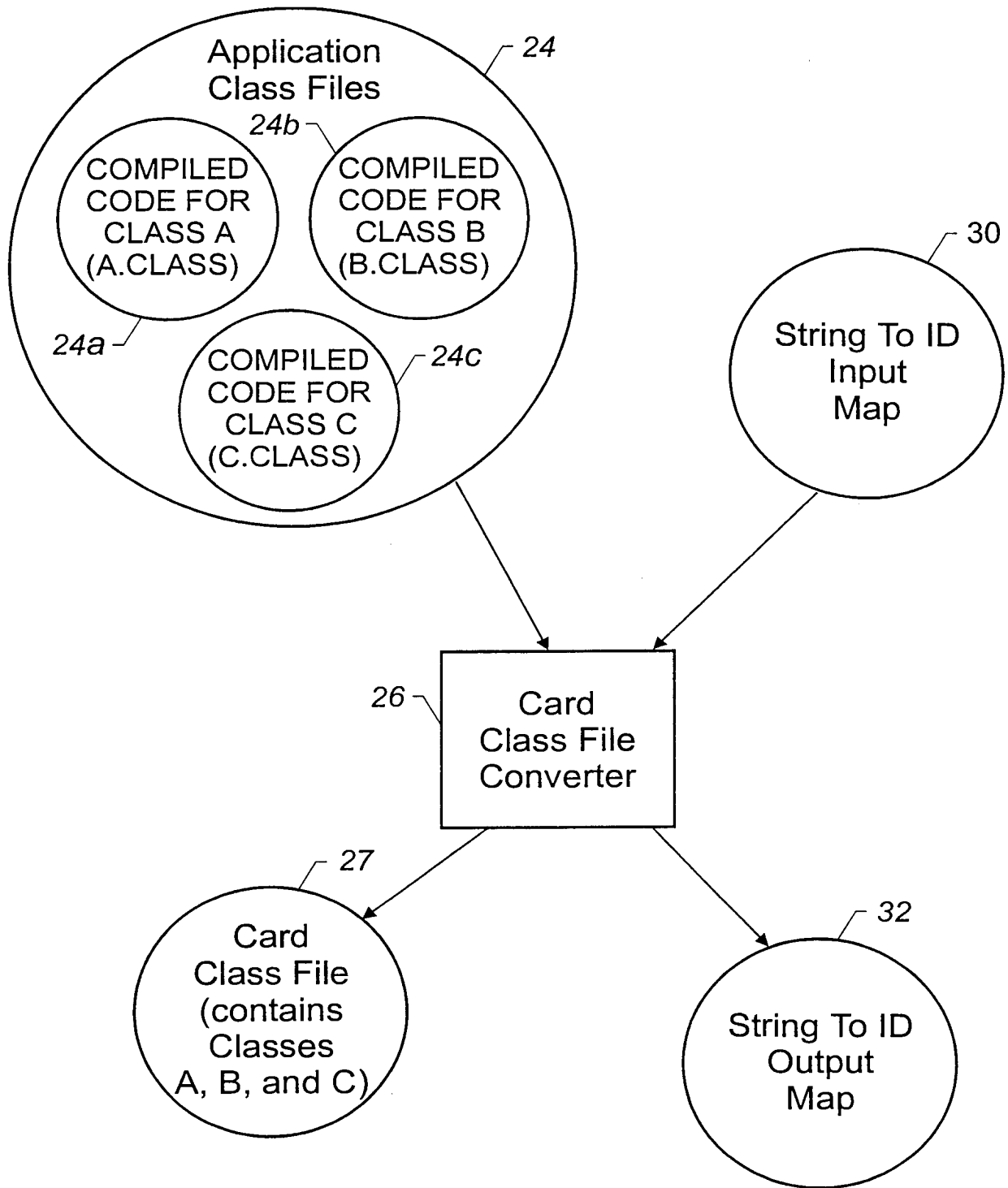


FIGURE 3



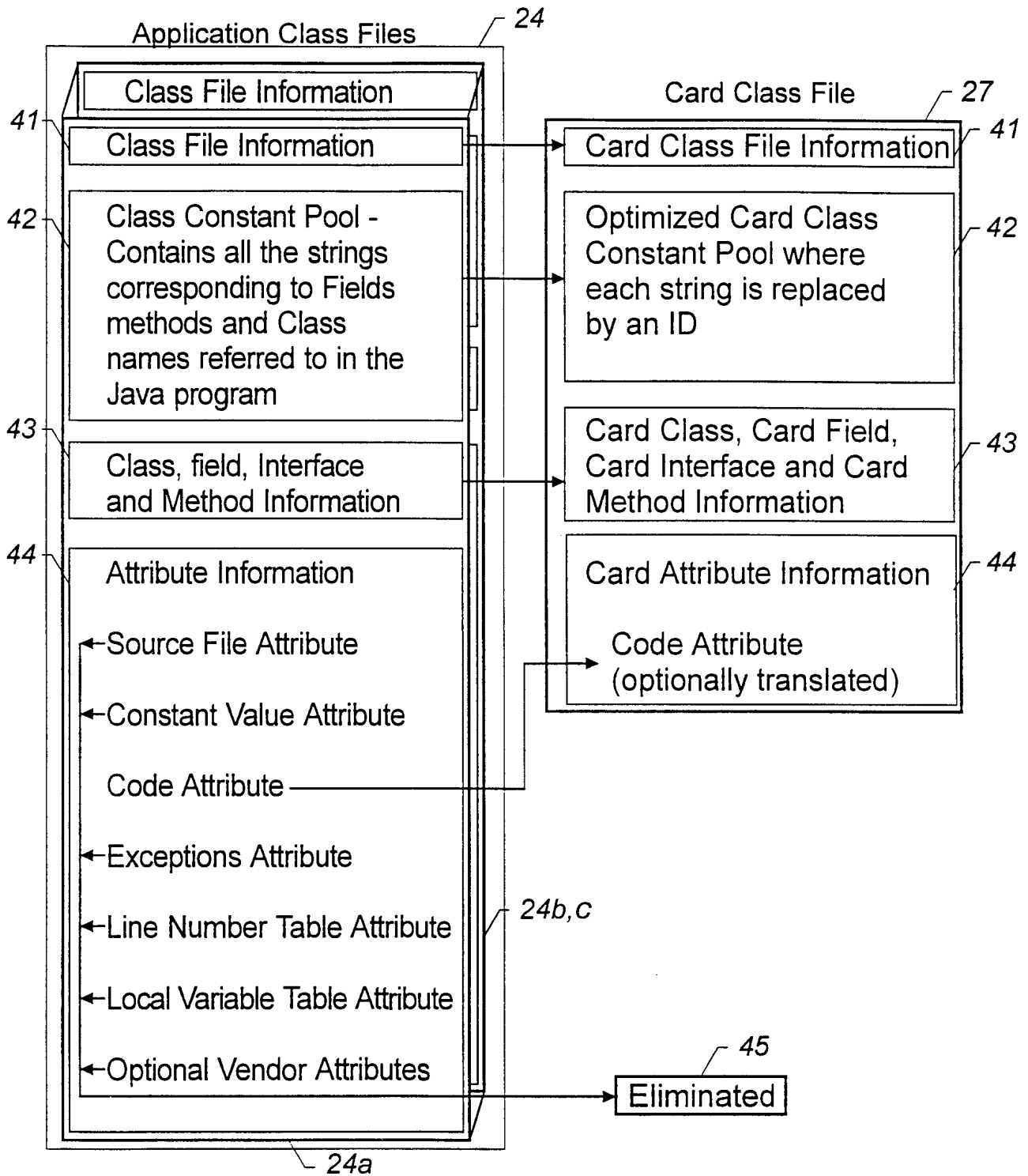


FIGURE 4

5/23

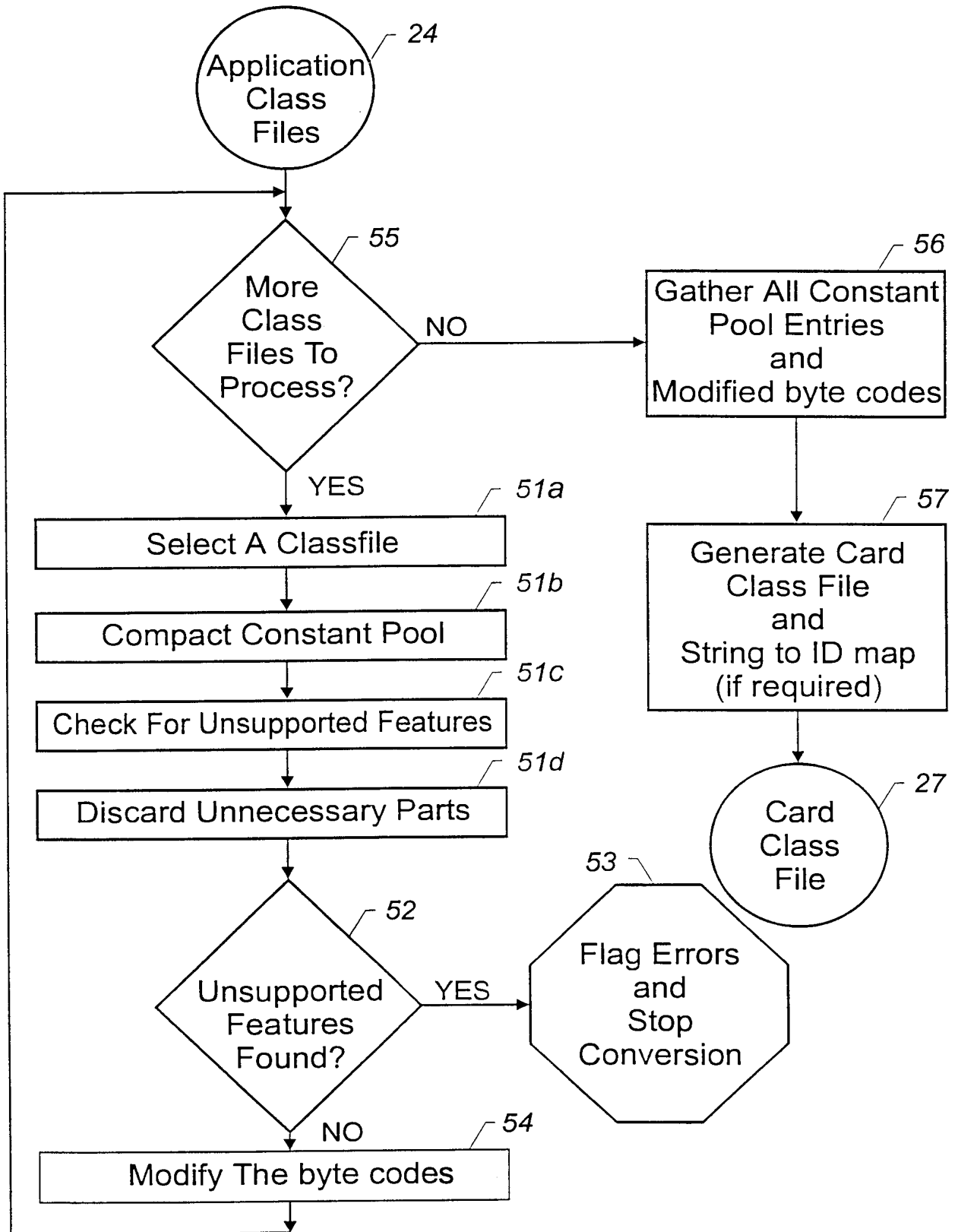


FIGURE 5

6/23

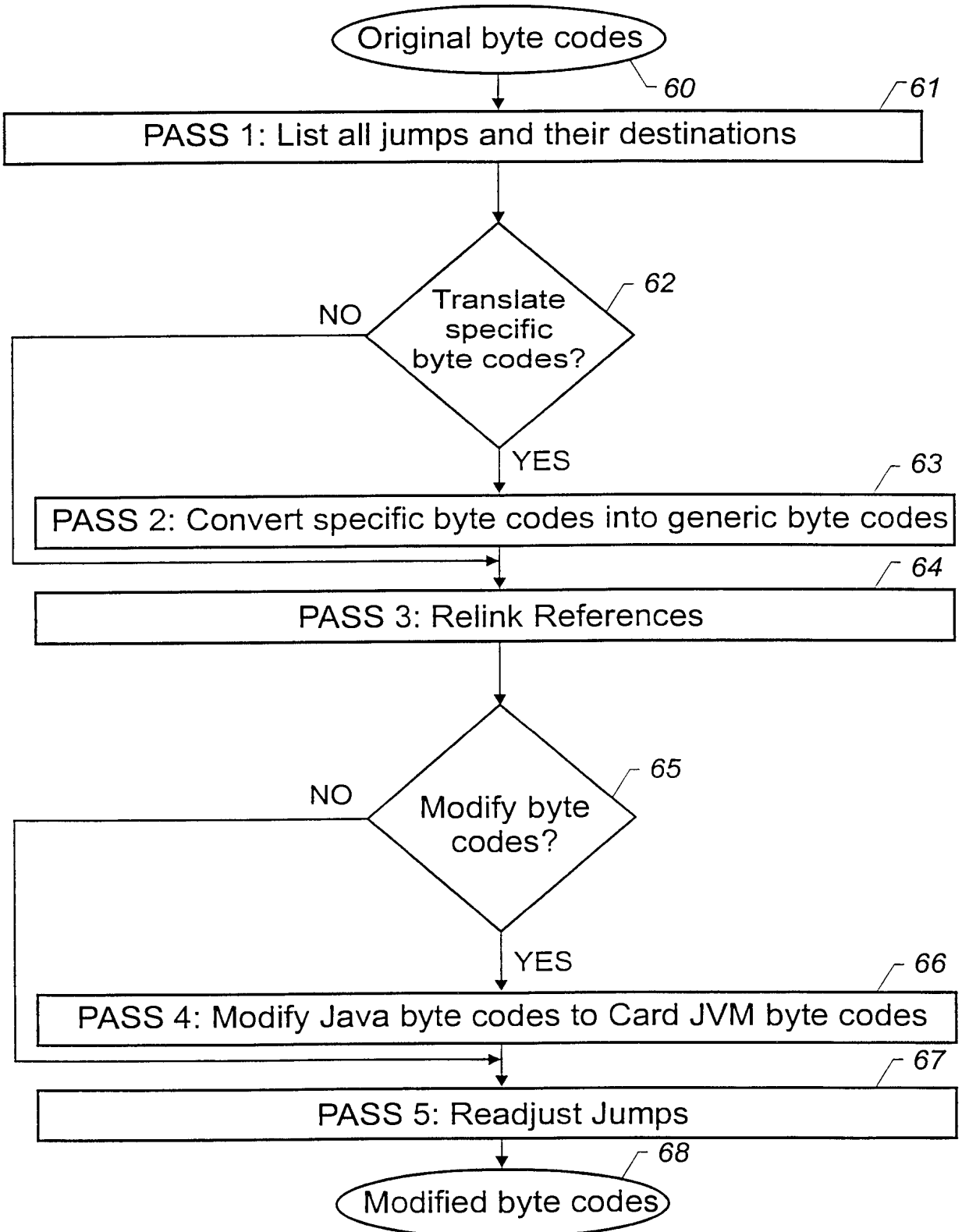


FIGURE 6

7/23

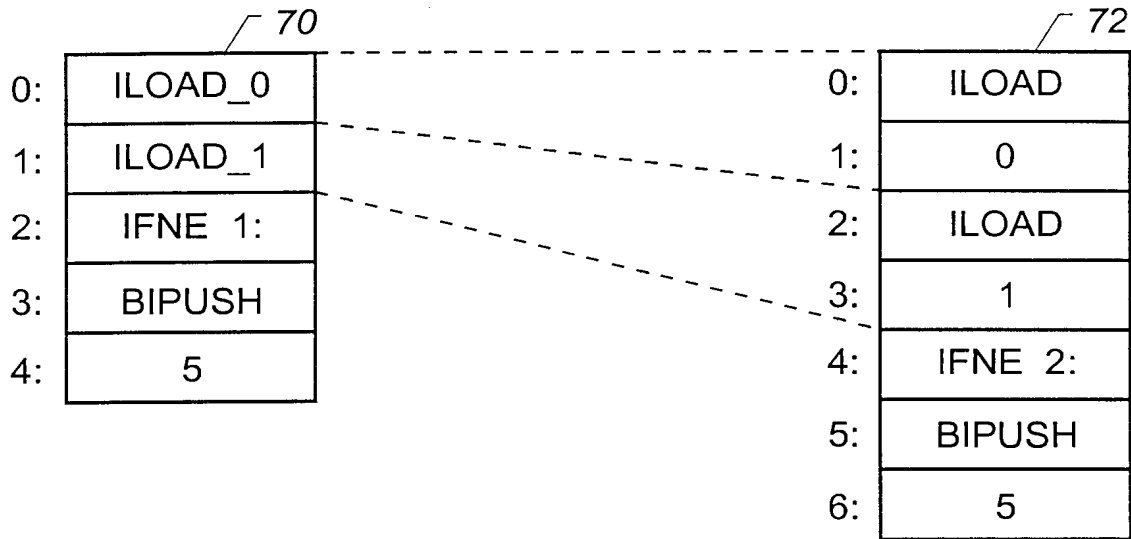
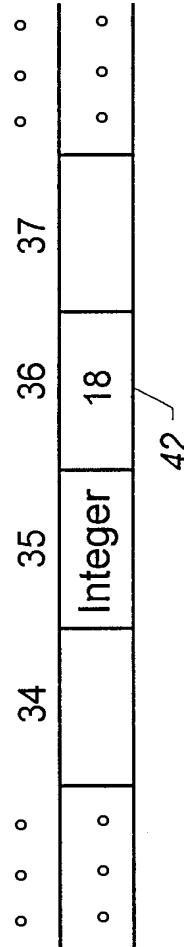
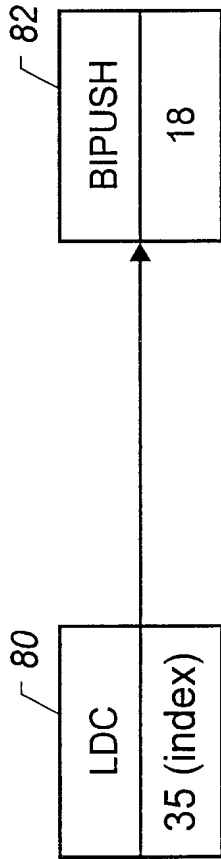


FIGURE 7

8/23



Class file Constant Pool

FIGURE 8

9/23

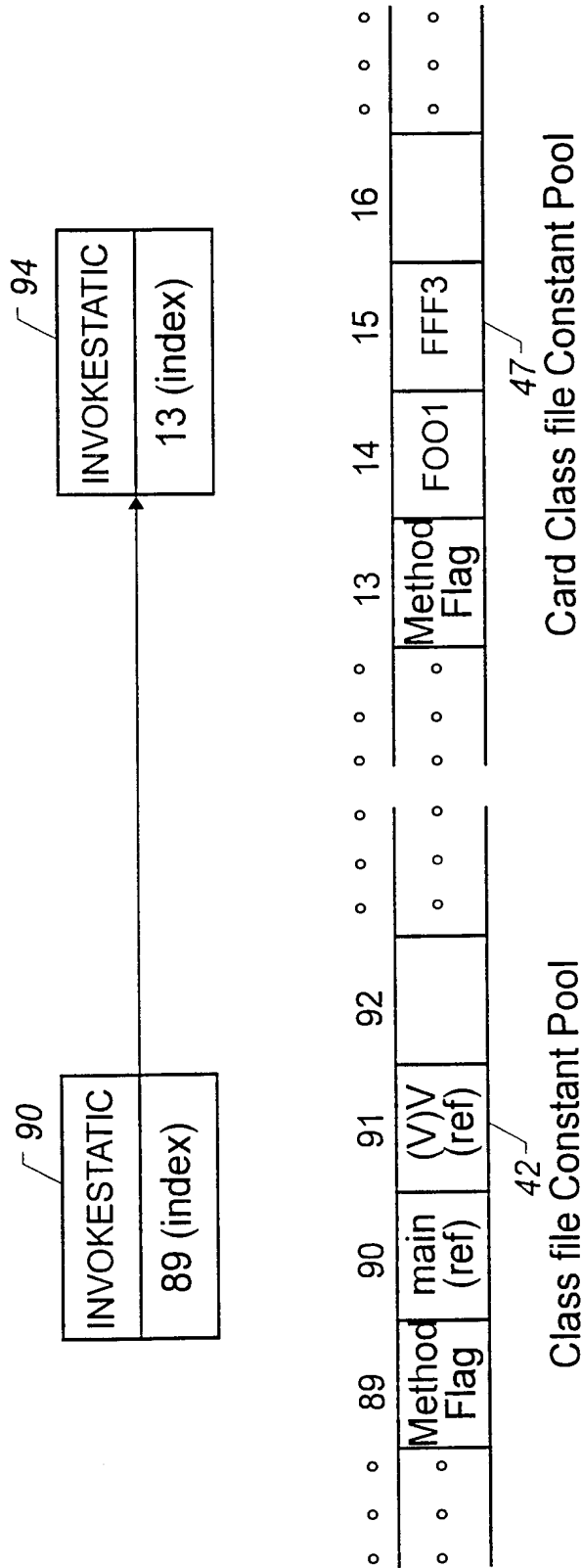


FIGURE 9

10/23

100

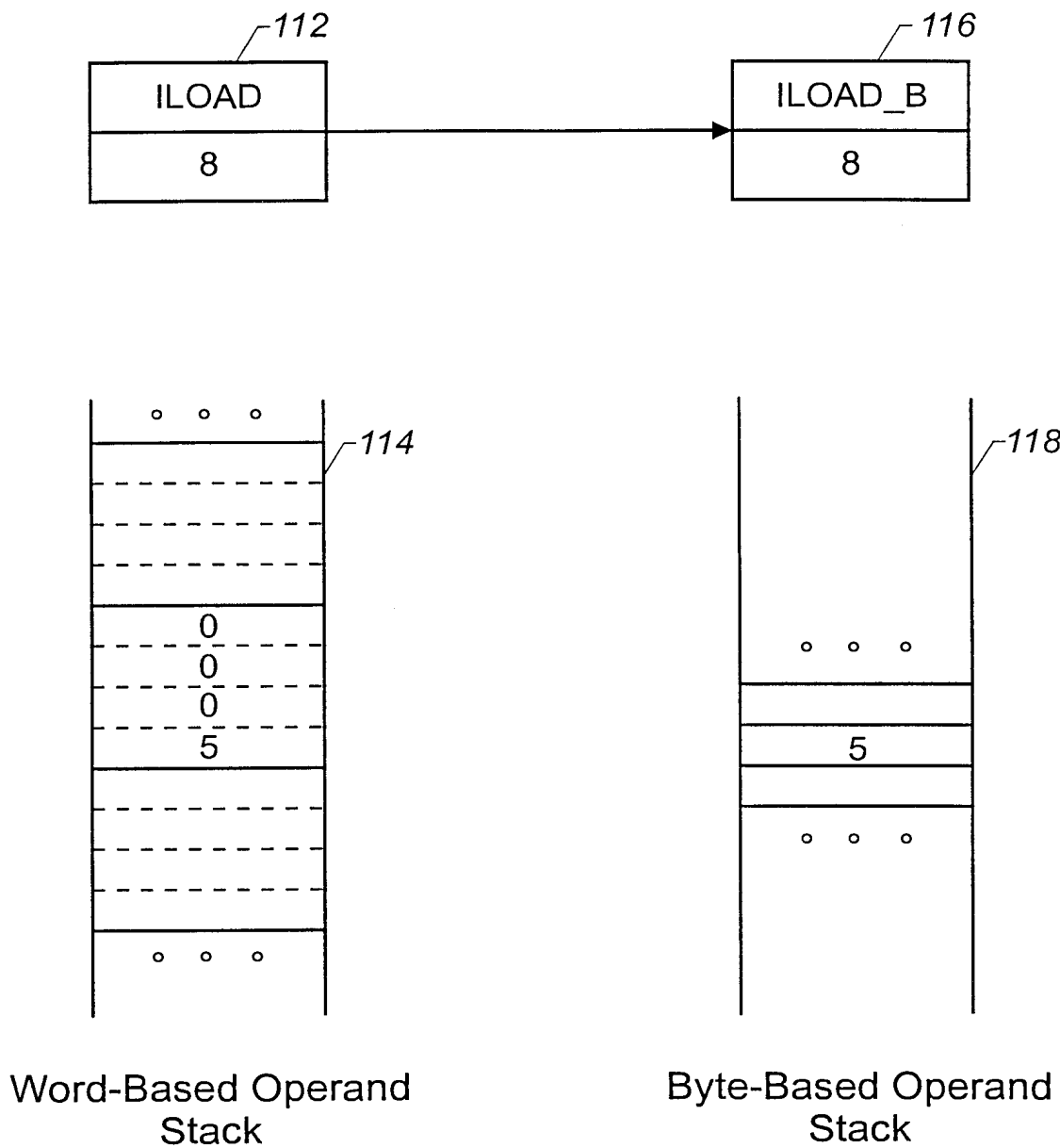
0:	ALOAD 43
1:	0
2:	ILOAD 21
3:	1
4:	IFNE 154 2:
5:	BIPUSH 16
6:	5

102

0:	ALOAD 51
1:	0
2:	ILOAD 50
3:	1
4:	IFNE 27 2:
5:	BIPUSH 49
6:	5

FIGURE 10

11/23



**FIGURE 11**



12/23

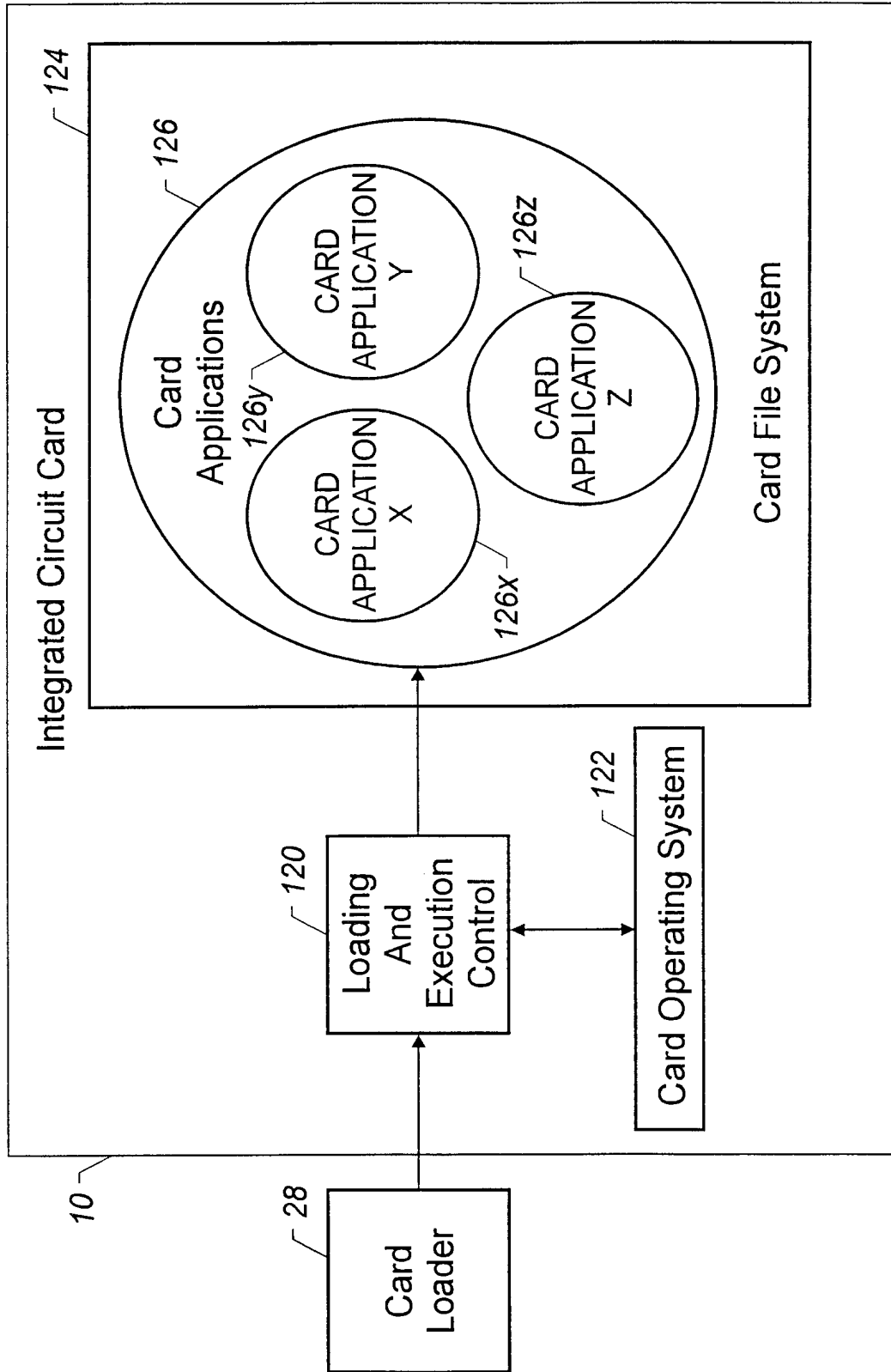


FIGURE 12

13/23

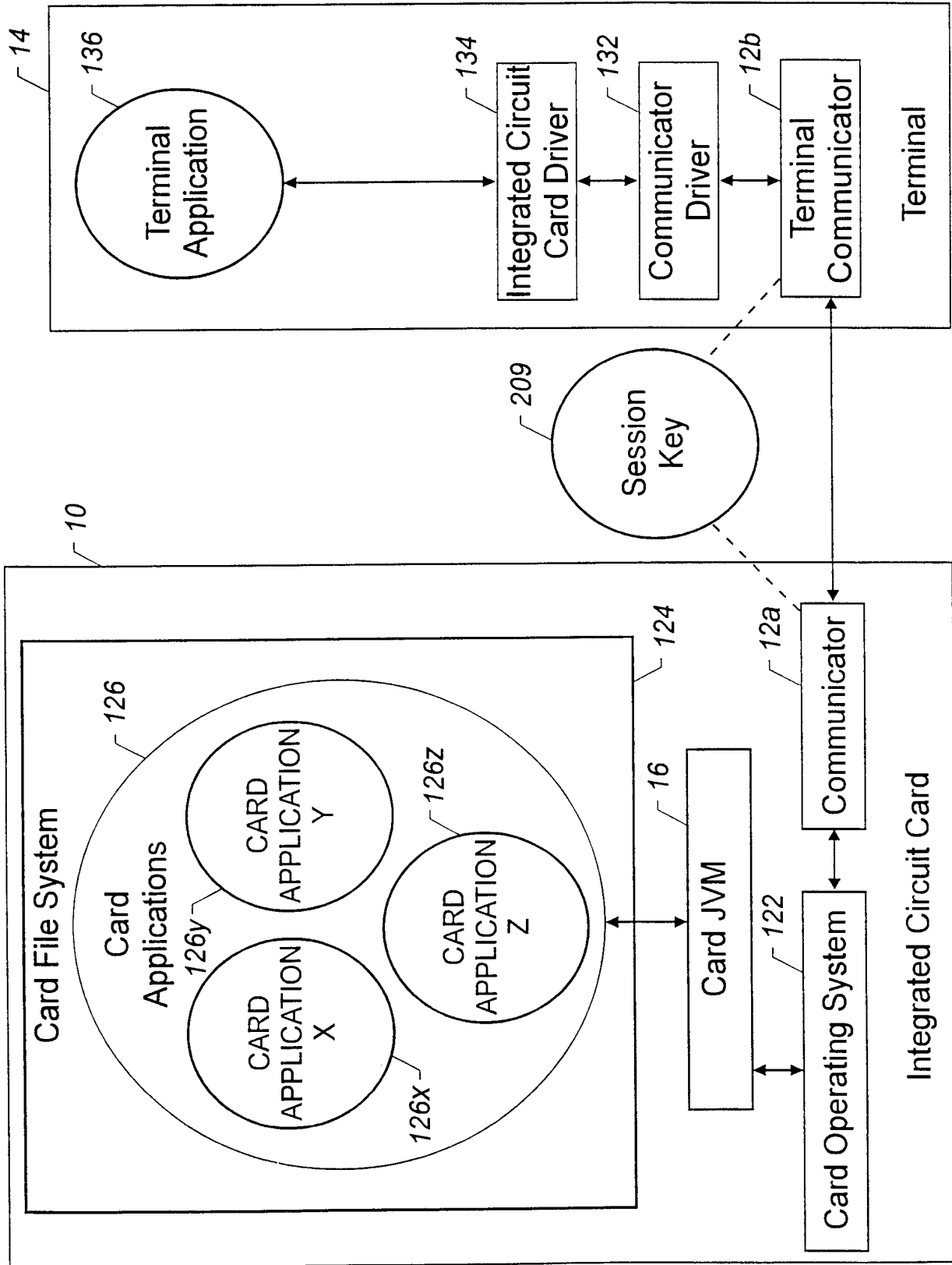


FIGURE 13

14/23

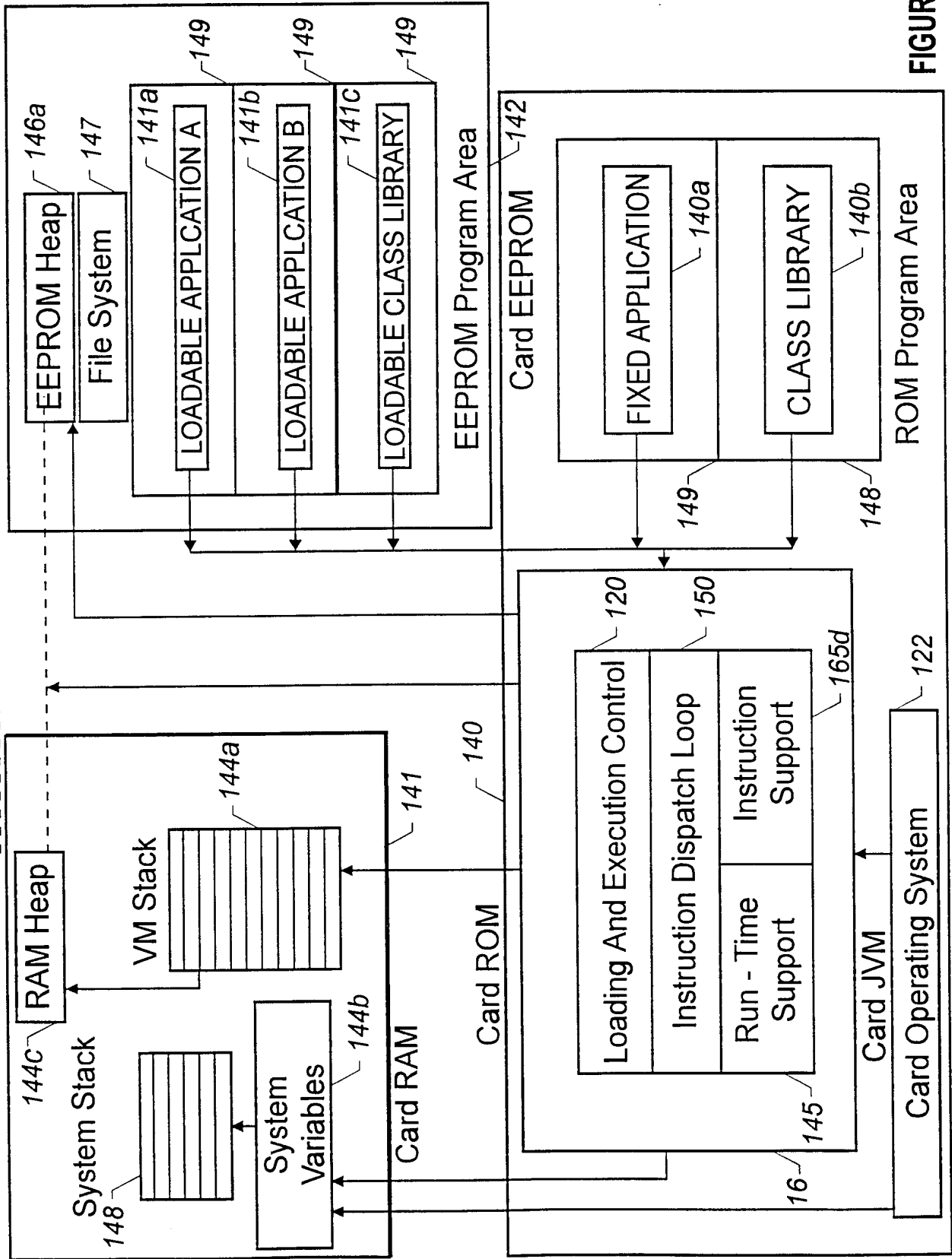


FIGURE 14

15/23

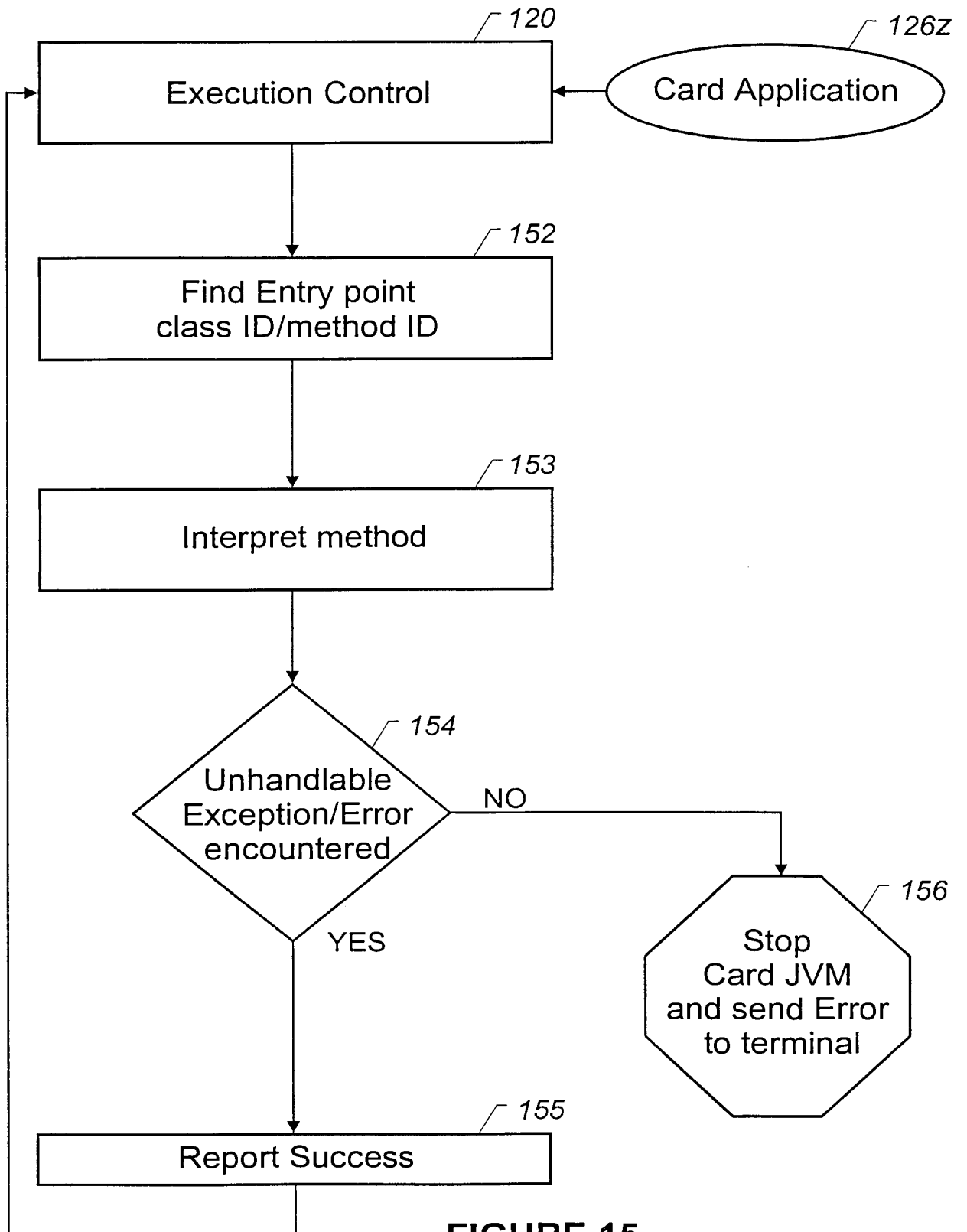


FIGURE 15

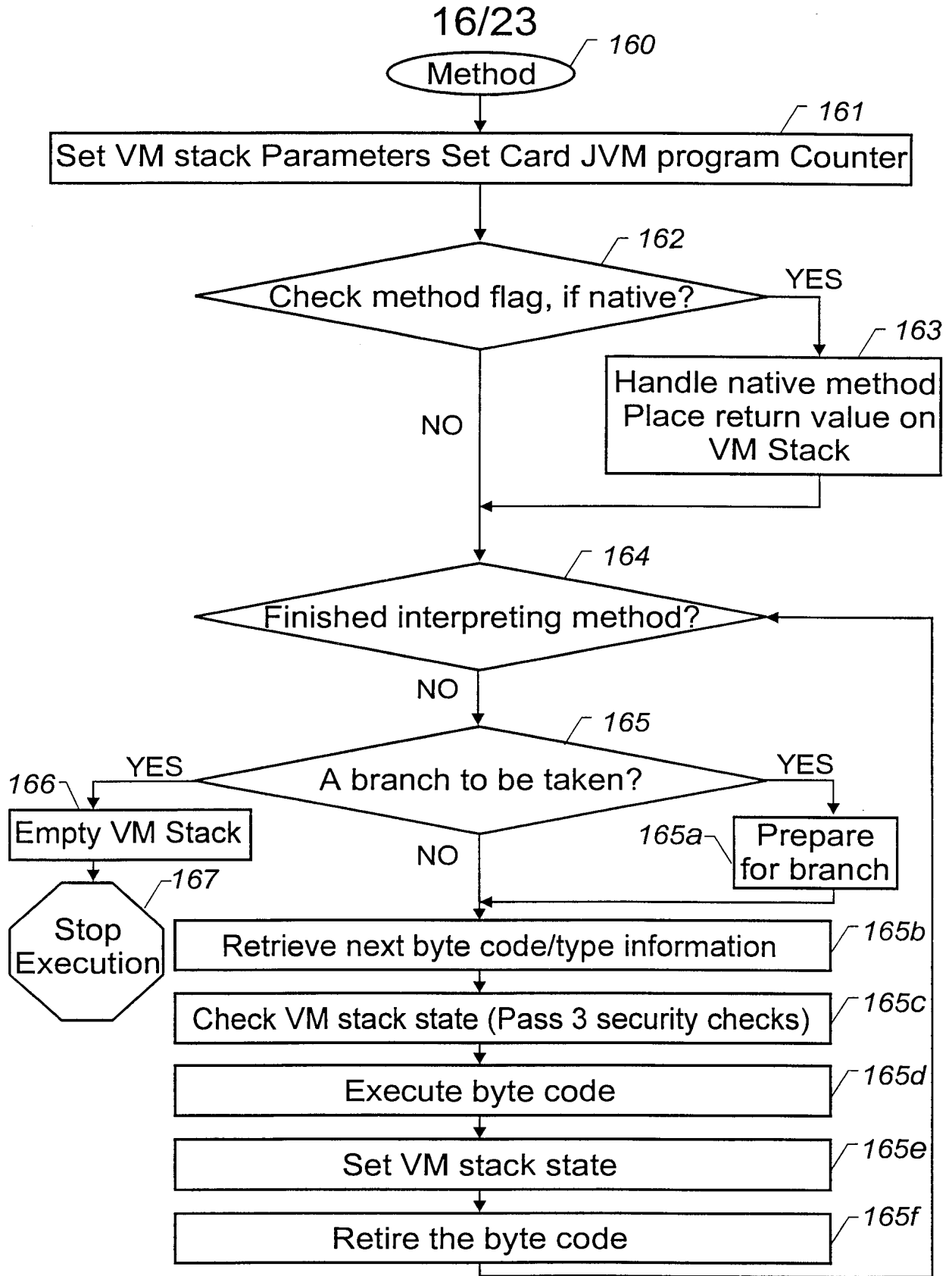


FIGURE 16

17/23

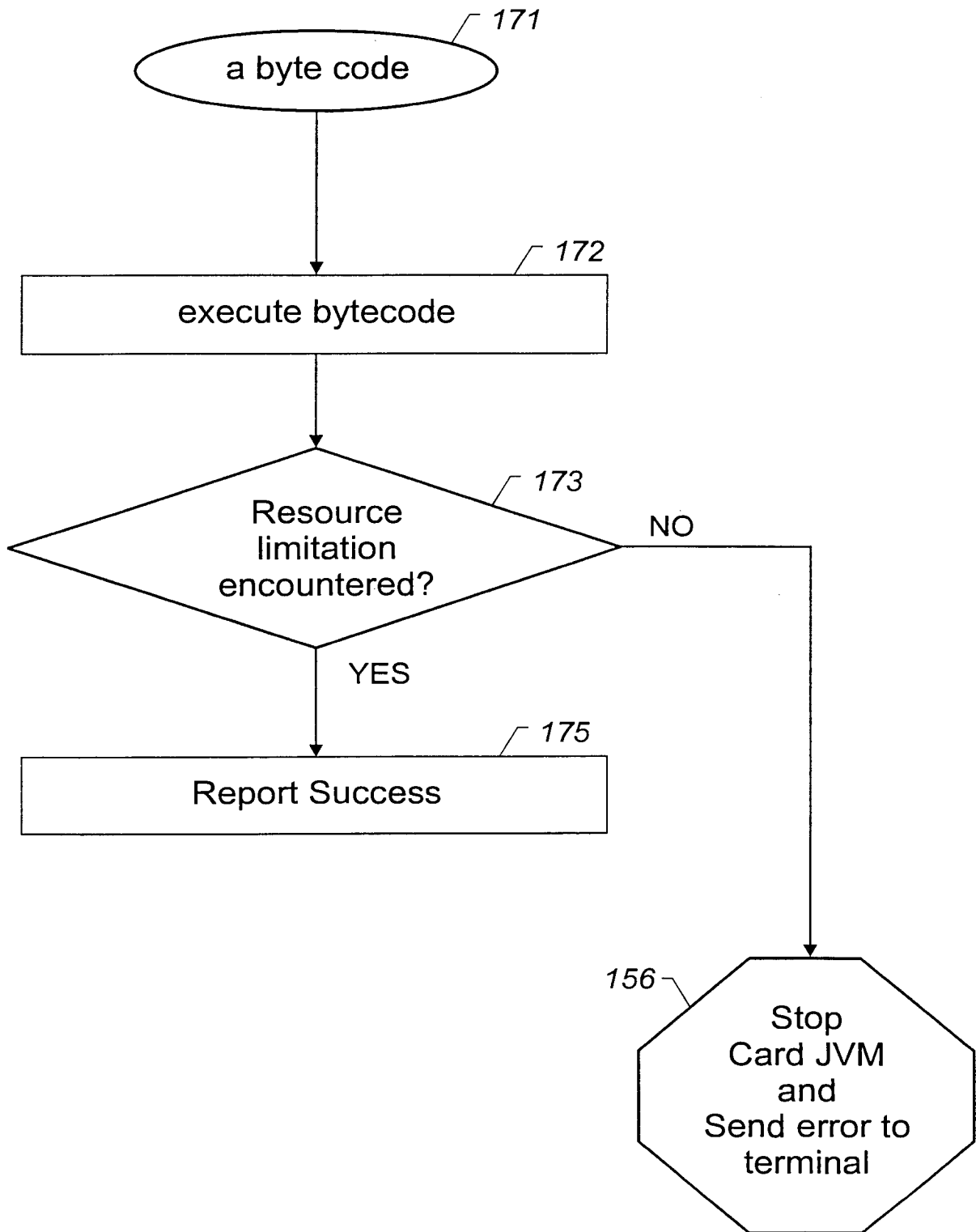


FIGURE 17

18/23

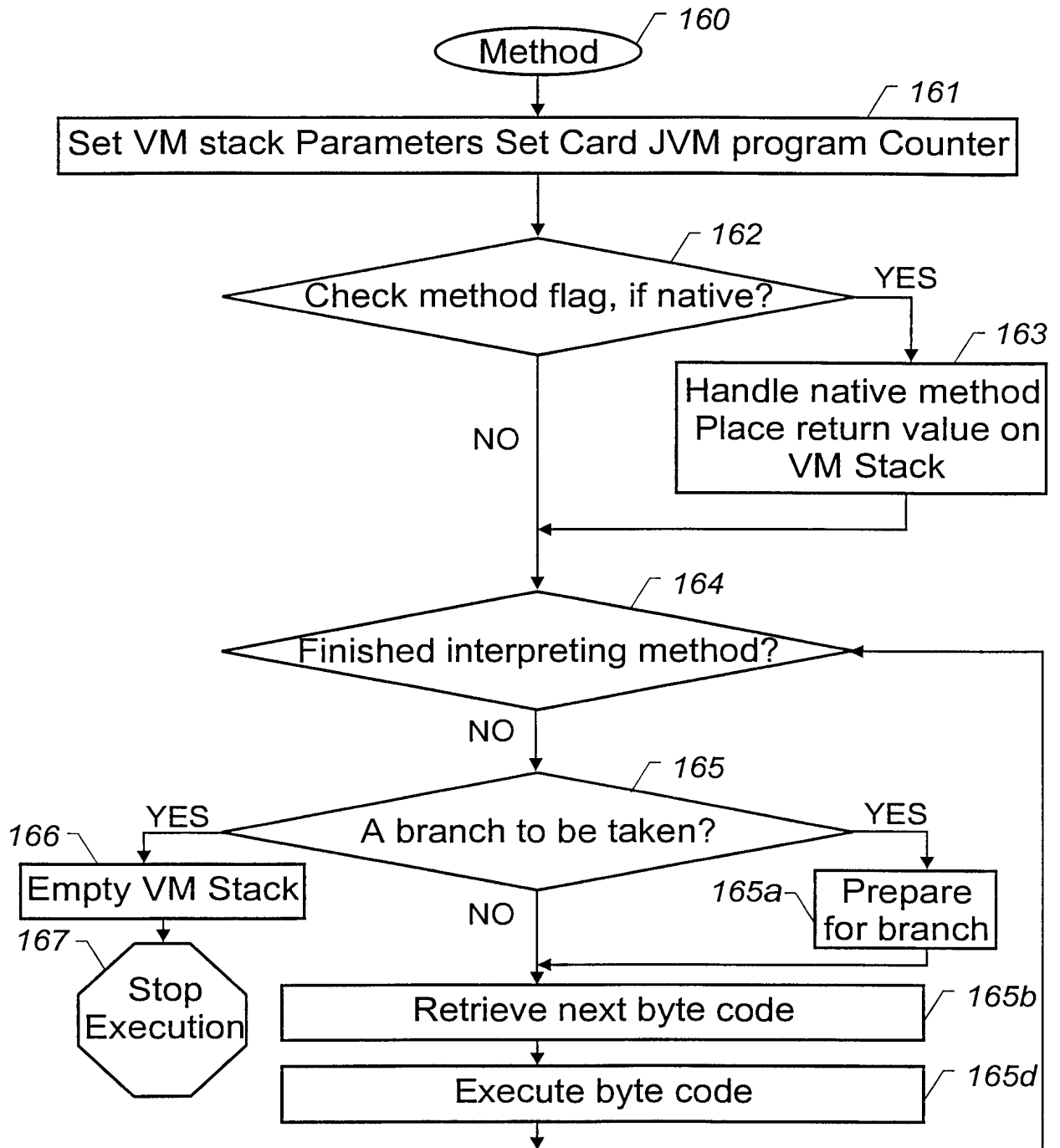


FIGURE 18

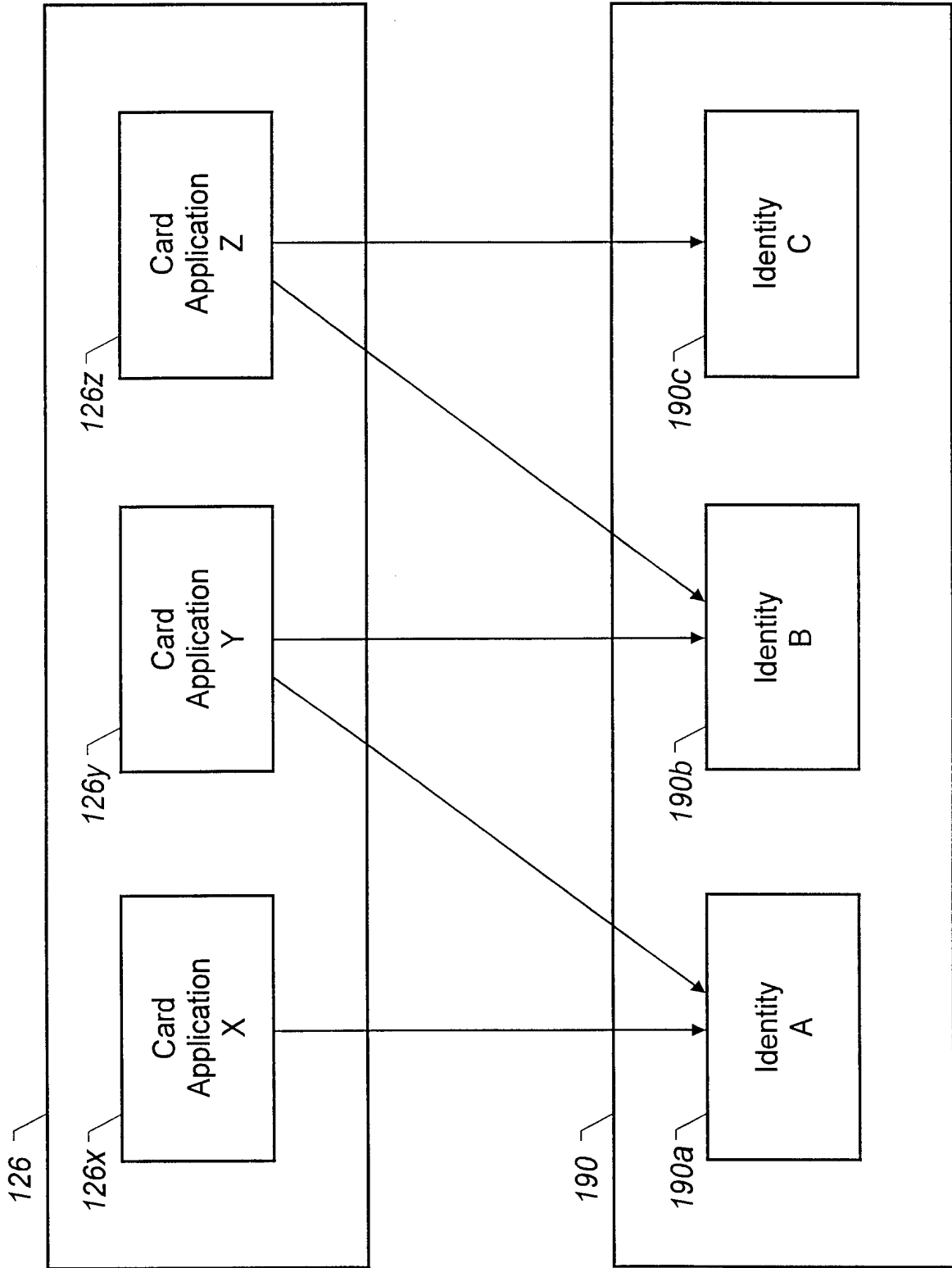


FIGURE 19



20/23

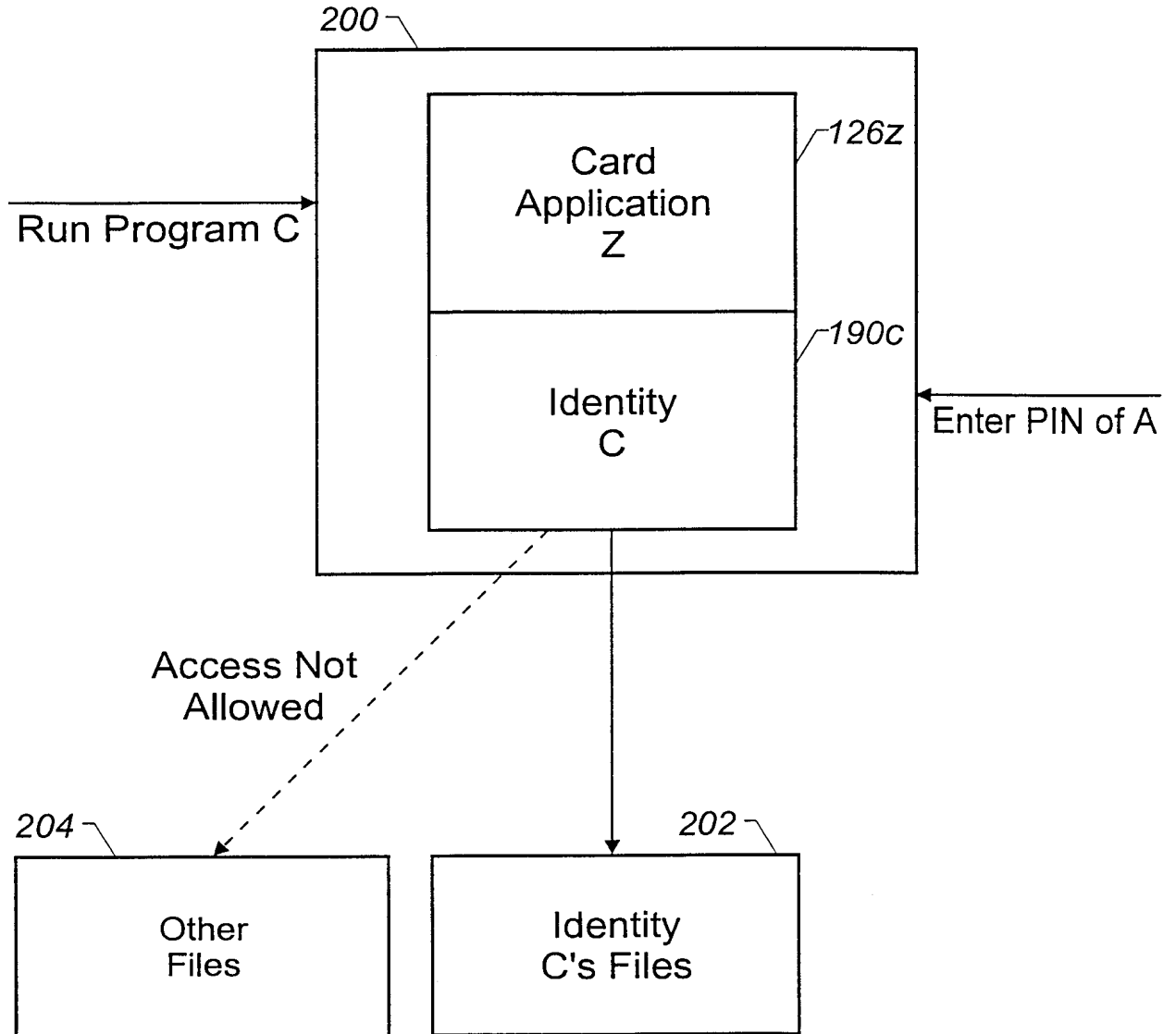


FIGURE 20

21/23

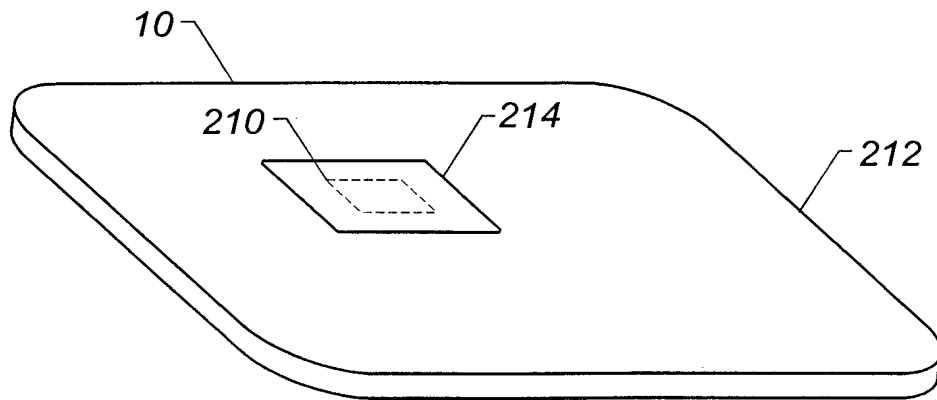


FIGURE 21

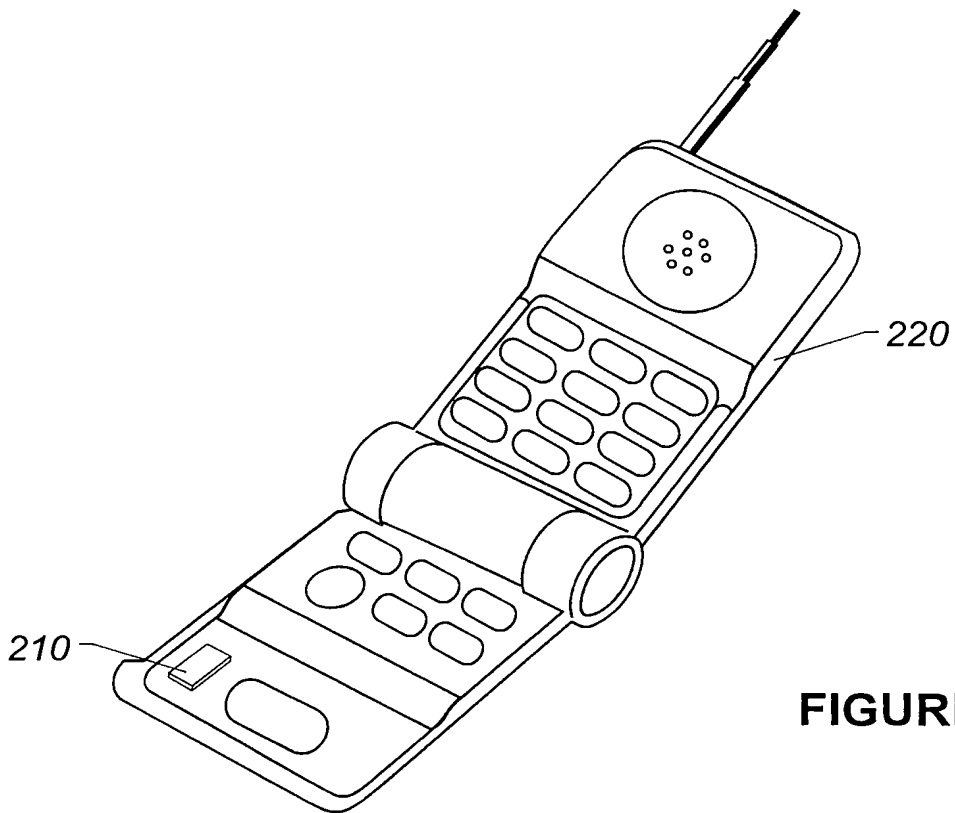


FIGURE 22

22/23

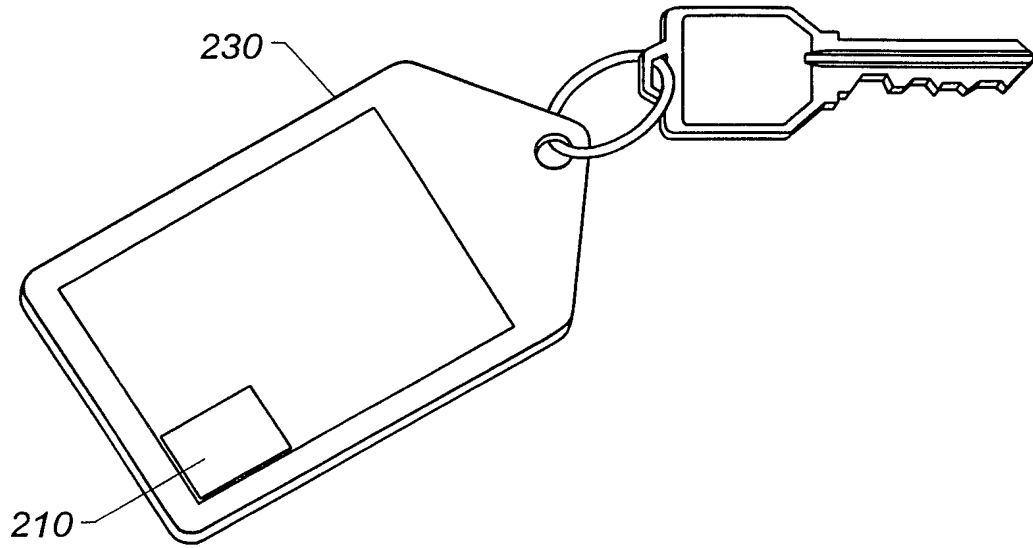


FIGURE 23

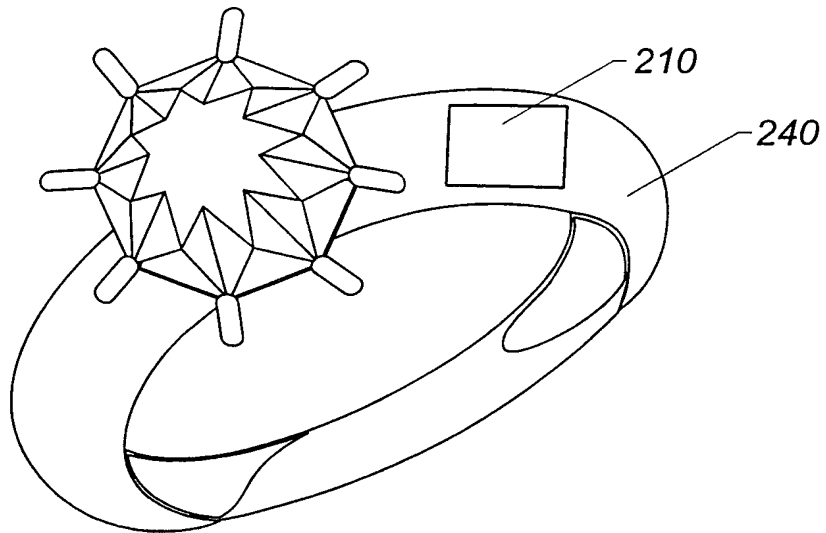


FIGURE 24

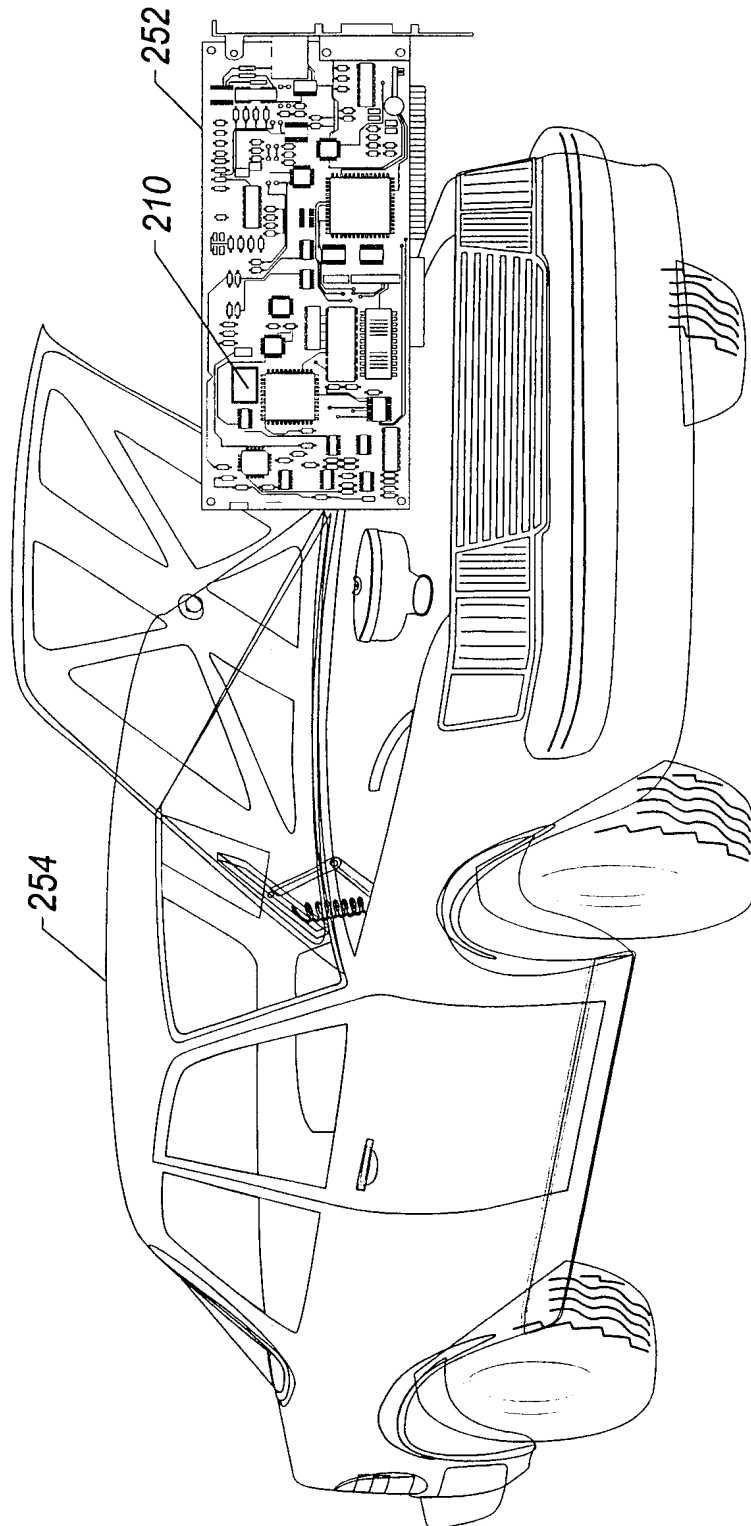


FIGURE 25



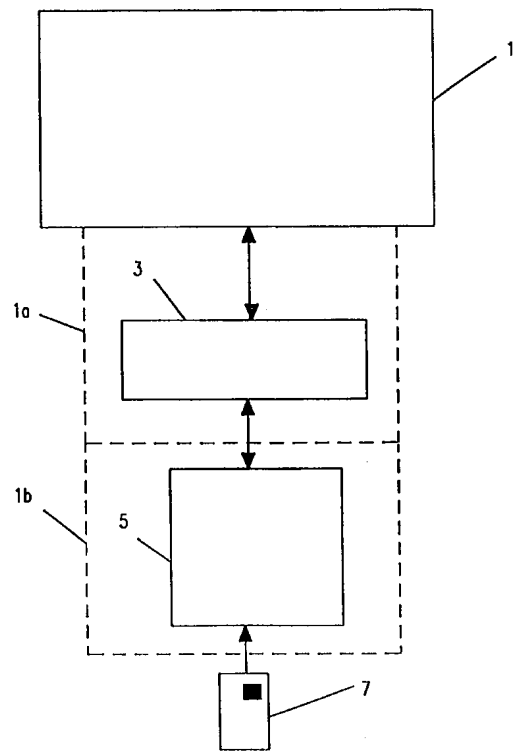
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>G07F 7/10, 17/16</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 98/25238</b> (43) International Publication Date: 11 June 1998 (11.06.98)</p>
<p>(21) International Application Number: PCT/NL97/00660 (22) International Filing Date: 2 December 1997 (02.12.97) (30) Priority Data: 1004658 2 December 1996 (02.12.96) NL (71) Applicant (for all designated States except US): R. CLEWITS BEHEER B.V. [NL/NL]; Bleyenbeek 1, NL-1083 AH Amsterdam (NL). (72) Inventor; and (75) Inventor/Applicant (for US only): CLEWITS, Ritske [NL/NL]; Bleyenbeek 1, NL-1083 AH Amsterdam (NL). (74) Agent: VAN WERMESKERKEN, Stephanie, Christine; Octrooibureau LIOC B.V., P.O. Box 13363, NL-3507 LJ Utrecht (NL).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments. In English translation (filed in Dutch).</i></p>

(54) Title: SYSTEM AND METHOD FOR THE SELECTIVE ACTIVATION OF ONE OR SEVERAL SOFTWARE AND/OR HARDWARE FUNCTIONS OF A PROGRAMMABLE DEVICE

(57) Abstract

A system and method for the selective activation of one or several software and/or hardware functions of a programmable device serves for simplifying the manufacture of these devices. The system and the method according to the invention comprise at least temporarily reading means and an electronically readable information carrier, such that the manufacturer has the certainty that he will receive payment for the activated functions, and the end user will pay only for those functions which have been active.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AL</b>	Albania	<b>ES</b>	Spain	<b>LS</b>	Lesotho	<b>SI</b>	Slovenia
<b>AM</b>	Armenia	<b>FI</b>	Finland	<b>LT</b>	Lithuania	<b>SK</b>	Slovakia
<b>AT</b>	Austria	<b>FR</b>	France	<b>LU</b>	Luxembourg	<b>SN</b>	Senegal
<b>AU</b>	Australia	<b>GA</b>	Gabon	<b>LV</b>	Latvia	<b>SZ</b>	Swaziland
<b>AZ</b>	Azerbaijan	<b>GB</b>	United Kingdom	<b>MC</b>	Monaco	<b>TD</b>	Chad
<b>BA</b>	Bosnia and Herzegovina	<b>GE</b>	Georgia	<b>MD</b>	Republic of Moldova	<b>TG</b>	Togo
<b>BB</b>	Barbados	<b>GH</b>	Ghana	<b>MG</b>	Madagascar	<b>TJ</b>	Tajikistan
<b>BE</b>	Belgium	<b>GN</b>	Guinea	<b>MK</b>	The former Yugoslav Republic of Macedonia	<b>TM</b>	Turkmenistan
<b>BF</b>	Burkina Faso	<b>GR</b>	Greece			<b>TR</b>	Turkey
<b>BG</b>	Bulgaria	<b>HU</b>	Hungary	<b>ML</b>	Mali	<b>TT</b>	Trinidad and Tobago
<b>BJ</b>	Benin	<b>IE</b>	Ireland	<b>MN</b>	Mongolia	<b>UA</b>	Ukraine
<b>BR</b>	Brazil	<b>IL</b>	Israel	<b>MR</b>	Mauritania	<b>UG</b>	Uganda
<b>BY</b>	Belarus	<b>IS</b>	Iceland	<b>MW</b>	Malawi	<b>US</b>	United States of America
<b>CA</b>	Canada	<b>IT</b>	Italy	<b>MX</b>	Mexico	<b>UZ</b>	Uzbekistan
<b>CF</b>	Central African Republic	<b>JP</b>	Japan	<b>NE</b>	Niger	<b>VN</b>	Viet Nam
<b>CG</b>	Congo	<b>KE</b>	Kenya	<b>NL</b>	Netherlands	<b>YU</b>	Yugoslavia
<b>CH</b>	Switzerland	<b>KG</b>	Kyrgyzstan	<b>NO</b>	Norway	<b>ZW</b>	Zimbabwe
<b>CI</b>	Côte d'Ivoire	<b>KP</b>	Democratic People's Republic of Korea	<b>NZ</b>	New Zealand		
<b>CM</b>	Cameroon	<b>KR</b>	Republic of Korea	<b>PL</b>	Poland		
<b>CN</b>	China	<b>KZ</b>	Kazakstan	<b>PT</b>	Portugal		
<b>CU</b>	Cuba	<b>LC</b>	Saint Lucia	<b>RO</b>	Romania		
<b>CZ</b>	Czech Republic	<b>LI</b>	Liechtenstein	<b>RU</b>	Russian Federation		
<b>DE</b>	Germany	<b>LK</b>	Sri Lanka	<b>SD</b>	Sudan		
<b>DK</b>	Denmark	<b>LR</b>	Liberia	<b>SE</b>	Sweden		
<b>EE</b>	Estonia			<b>SG</b>	Singapore		

System and method for the selective activation of one or several software and/or hardware functions of a programmable device

5 The invention relates to a system for the selective activation of one or several software and/or hardware functions of a programmable device, comprising at least temporarily a programmable device and programming means.

The invention also relates to a method of selectively activating one or several software  
10 and/or hardware functions of a programmable device whereby at least one function is selected and activated.

Such a system and such a method are known and are used for simplifying the production  
of programmable devices. Only one type of device is produced instead of individual  
15 devices for each application and/or each wish of an end user. The device is then adapted to the wishes or demands of the end user in that functions are selectively activated in the device. It is thus possible to manufacture a wide range of devices in a uniform production process, each having its own specific price level.

20 A disadvantage of such a system is that it is up to the manufacturer himself to carry out the necessary programming so as to adapt the device to the end user's specific wishes, which may indeed not be known to the manufacturer in some cases. This is because a wholesale firm is often involved, with an intermediary salesman who is more or less far removed from the manufacturer maintaining the contact with the end user.

25 It is accordingly advisable to leave the programming to the relevant intermediary, but this renders it impossible for the manufacturer to see how many devices are programmed, and how many functions therein.

30 The manufacturer thus does not know what amount is due to him as payment for the activated functions.

-2-

The invention has for its object to eliminate the above disadvantages. According to the invention, a system is for this purpose characterized in that the system at least temporarily also comprises reading means which are designed for reading an electronically readable information carrier comprising a programmable memory capable of containing a numerical value.

The electronically readable information carrier, for example a chip card, is provided with a certain credit amount and is delivered by the manufacturer to, for example, an intermediate trader, and paid for by the latter. Whenever a function is activated, a corresponding amount is subtracted from the credit amount on the electronically readable information carrier. The intermediate trader programs the programmable device in accordance with the end user's wishes and buys a fresh electronically readable information carrier from the manufacturer after the full credit amount has been written off this carrier, or has the carrier reprogrammed at the manufacturer's, so that the latter is always paid for the activated functions. An additional advantage for the end user is that he will only pay for functions actually activated and not for any functions not (yet) activated, while still retaining the possibility of having additional functions activated later. This enables the manufacturer to keep an eye on the activated functions without the necessity of programming the programmable devices himself or of activating the functions desired by the end user. The manufacturer as it were provides the end user with a software licensing card for all functions present on the programmable device, a certain value being debited to the card's account whenever one or several functions is or are activated.

EP-A-0 594 493 describes a method and a computer system for obtaining software by means of a microcomputer. The system for this purpose comprises a database in which the software to be used is stored and a detachable storage carrier which contains an access right. This latter carrier can be inserted into a reading device of the microcomputer for enabling a loading of software, for which the carrier contains the relevant access rights, from the database to the microcomputer. The carrier may also contain rights for implementing the loaded software.



EP-A-0 530 601 describes the use of data carrier cards which enable an activation of individual appliance functions of an electronic appliance. The electronic appliance here comprises a circuit arrangement with one or several circuits for putting into action a number of functions of the appliance. The functions to be carried out by the circuit arrangement can be activated by means of the data carrier card.

A major difference between the latter two systems and the system according to the present invention is that said latter two systems use configuration cards which are adapted to the specific wishes of the end user. These cards are capable of activating certain, predetermined functions of the programmable device only. The cards have to be specially manufactured for the end user, which is labour-intensive. In the system according to the invention, on the other hand, an electronically readable information carrier is used which is capable of activating any function of the programmable device while at the same time debiting the card's account for the amount due.

A special embodiment of a system according to the invention is characterized in that the programmable device comprises the programming means and the reading means.

This means that the wholesaler only needs an electronically readable information carrier in order to program the programmable device in accordance with the end user's wishes.

In particular, the programmable device is an automatic payment machine.

Since an automatic payment machine comprises reading means, it is possible to activate or additionally activate one or several functions of the automatic payment machine, provided it is also fitted with programming means, by means of no more than an electronically readable information carrier.

A further special embodiment of system according to the invention is characterized in that the programmable device is coupled at least temporarily to separate programming

-4-

means, which programming means comprise the reading means and, at least temporarily, the electronically readable information carrier.

5 If the programmable device does not comprise the programming means, it is favourable to accommodate these programming means together with the card reader means in one unit into which the wholesaler subsequently inserts the electronically readable information carrier for the purpose of programming.

10 A particular embodiment of a system according to the invention is characterized in that the programmable device is a timer.

Such a timer may be used, for example, with a suntanning couch, a shower at a camping, etc. More or fewer functions of the timer may be activated in dependence on the application. A timer for a shower, for example, is often of a simple construction and  
15 need only determine the maximum shower time and possibly the use per unit time, whereas a timer for a suntanning couch, for example, monitors a warming-up time, a suntanning time, and the total number of hours of operation. Thanks to the system according to the invention, it is now possible for the manufacturer to deliver the same timer to the two customer groups, possibly each at its own specific price, while  
20 nevertheless the customer pays only for the functions he actually obtains.

The invention also relates to a method of selectively activating one or several software and/or hardware functions of a programmable device whereby at least one function is selected and activated. This method is characterized in that the programmable device is  
25 at least temporarily coupled to programming means which are coupled to reading means, and in that the reading means cooperate with an electronically readable information carrier on which a value is stored, while after the activation of a function a corresponding value is debited.

30 This method will usually be carried out by a wholesaler or intermediary who has bought the electronically readable information carrier from the manufacturer. It is also possible

for a (large-scale) end user to carry out the programming himself after buying an electronically readable information carrier, a programmable device, and possibly programming means and reading means from the manufacturer. This constitutes an additional advantage of the system and the method according to the invention. The  
5 manufacturer can offer these facilities to major end users since the payment takes place on the basis of activated functions anyway.

The invention also relates to a programmable device, programming means, and an electronically readable information carrier for use in a system according to the  
10 invention.

The electronically readable information carrier may be, for example, a chip card which comprises a programmable memory capable of containing a numerical value. Besides a decrementable amount, the chip card comprises at least one program for activating a  
15 function of the programmable device.

The invention will now be explained in more detail by way of example with reference to the accompanying drawing, in which:

Fig. 1 diagrammatically shows an embodiment of a system according to the invention,  
20 and

Fig. 2 diagrammatically shows an embodiment of a programmable device according to the invention in greater detail.

Fig. 1 diagrammatically shows an embodiment of a system S according to the invention  
25 for the selective activation of one or several software and/or hardware functions of an electronic device. The system comprises a programmable device 1 which has been provided at the manufacturer's with any number of functions in the form of modules which might be desired by the end users. The modules, however, have not yet been activated, but they are activated on demand by the supplier (wholesaler) against  
30 payment.

-6-

The system further comprises programming means 3 which activate the desired module(s) of the programmable device 1. The programming means may be incorporated into the programmable device in some applications (referenced 1a).

5 The system finally comprises reading means 5 which in this embodiment are constructed as card reader means suitable for reading an electronically readable information carrier, for example a programmable card 7. The card reader means may also be incorporated into the programmable device in some applications (referenced 1b), for example in an automatic payment machine. The programmable card in this  
10 embodiment comprises a programmable memory capable of retaining a numerical value. During programming, i.e. selecting and activating, of the programmable device 1, the programmable card 7 is placed in the card reader means 5 which are coupled to the programming means 3.

15 To ensure that the manufacturer of the programmable device receives payment for the number of functions activated, the programmable card is issued by the manufacturer and provided with a certain credit amount. It is also stored on the card how much is to be debited from the amount for each function to be activated, which may be different for different functions. The wholesaler can now program each programmable device as  
20 desired by the end user and have this user pay for this. After the credit amount on the card has been used up, the user must either have the card recharged at the manufacturer's against payment, or buy a new card.

The programmable device 1 may be constructed, for example, as an automatic payment  
25 machine, for example for use in shops. More or fewer functions may be programmed in dependence on the end user's wishes. For example, the automatic payment machine may thus be made compatible with post giro cards, rechargeable cash cards, credit cards, etc.

The programmable device may alternatively be constructed, for example, as a timer for  
30 use with, for example, a shower, a suntanning couch, etc. The programmable device will usually not comprise the programming means in this application, and the timer will have

-7-

to be programmed in accordance with the end user's wishes. A timer for a shower, for example on a camping, is usually of a simple construction and only determines the shower-taking time and possibly the use of the relevant shower (for example, per day, week, month, etc.). A timer for a suntanning installation in business surroundings, on the other hand, is to monitor and/or register several time periods such as, for example, a warming-up time, an effective tanning time, and the number of hours of operation.

Fig. 2 diagrammatically shows an embodiment of a programmable device 1 in accordance with Fig. 1 in more detail. In this embodiment, the programmable device comprises five modules 11, 12, 13, 14, and 15 in which the respective functions are present. Each of these functions can be activated by the supplier, as desired, after payment by the end user. Fig. 2 shows that the modules 11 and 13 have been activated "A", and the modules 12, 14 and 15 have not.

It will be obvious that the system and the method according to the invention may be adapted in a variety of ways without departing from the scope of the invention. Thus the programming means and the (card) reading means may be integrated with the programmable device, as was noted above.

Furthermore, the electronically readable information carrier, for example a programmable card, may be adapted in various ways and may be constructed as a chip card, for example a rechargeable cash card or otherwise, as long as due payments are made to the manufacturer for the activated functions, i.e. it should not be possible to use a card not issued by the relevant manufacturer for activating a programmable device sold by this manufacturer.

It is also possible, for example, to rent out or lease the programmable devices, in which case the system according to the invention renders it possible not only to activate functions, but also to deactivate functions and to base the renting or leasing bill on the number of functions activated. It is in addition possible, for example, to deactivate a

-8-

function by not debiting the card with a certain amount, or by debiting it with a lesser amount.

## Claims

1. A system for the selective activation of one or several software and/or hardware  
5 functions of a programmable device, comprising at least temporarily a programmable  
device and programming means, characterized in that the system at least temporarily  
also comprises reading means which are designed for receiving an electronically  
readable information carrier comprising a programmable memory capable of containing  
a numerical value.
- 10
2. A system as claimed in Claim 1, characterized in that the programmable device  
comprises the programming means and the reading means.
3. A system as claimed in Claim 2, characterized in that the programmable device  
15 is an automatic payment machine.
4. A system as claimed in Claim 1, characterized in that the programmable device  
is coupled at least temporarily to separate programming means, which programming  
means comprise the reading means and, at least temporarily, the electronically readable  
20 information carrier.
5. A system as claimed in Claim 4, characterized in that the programmable device  
is a timer.
- 25
6. A method of selectively activating one or several software and/or hardware  
functions of a programmable device whereby at least one function is selected and  
activated, characterized in that the programmable device is at least temporarily coupled  
to programming means which are coupled to reading means, and in that the reading  
means cooperate with an electronically readable information carrier on which a value is  
30 stored, while after the activation of a function a corresponding value is debited.

-10-

7. A programming device suitable for use in a system as claimed in Claims 1 to 5.
8. Programming means suitable for use in a system as claimed in Claims 1 to 5.
- 5 9. An electronically readable information carrier suitable for use in a system as claimed in Claims 1 to 5.



1/2

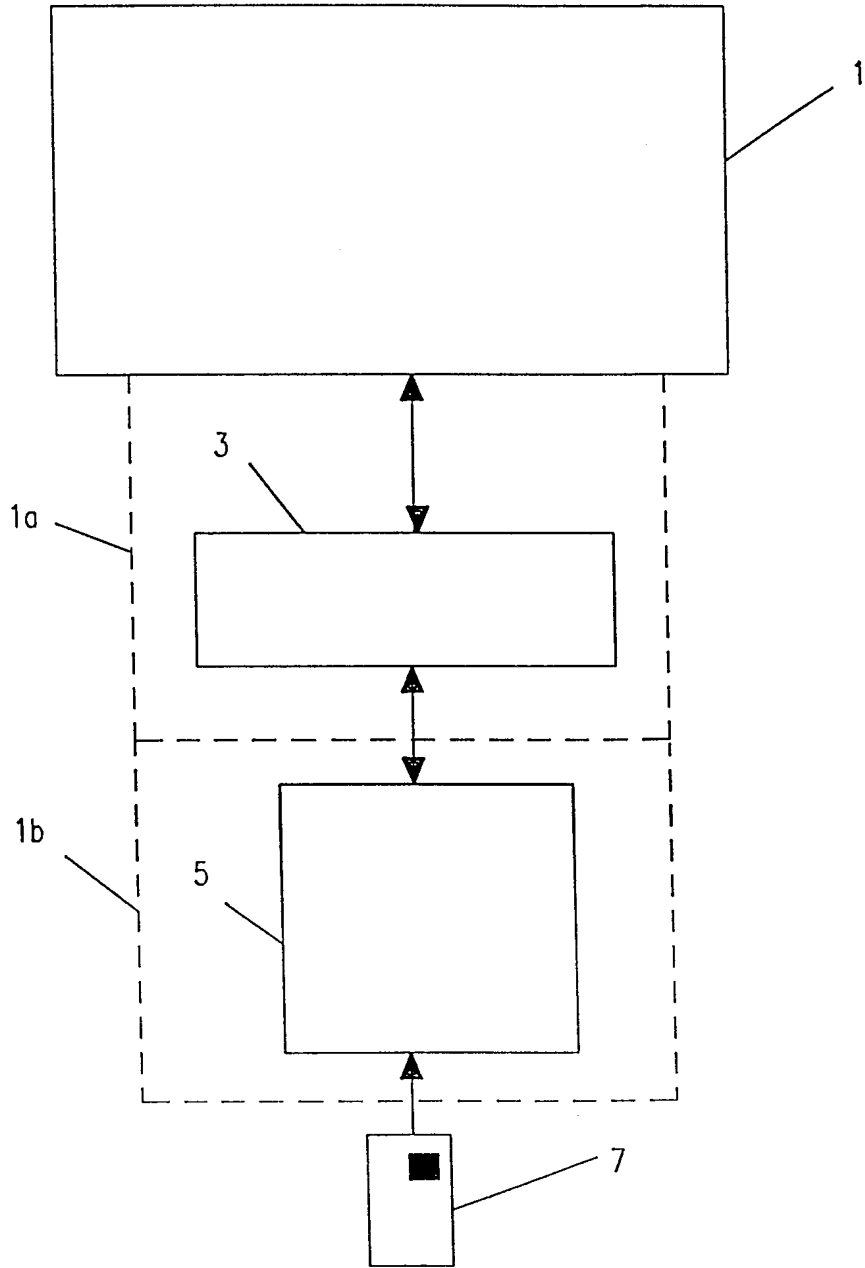


FIG. 1

2/2

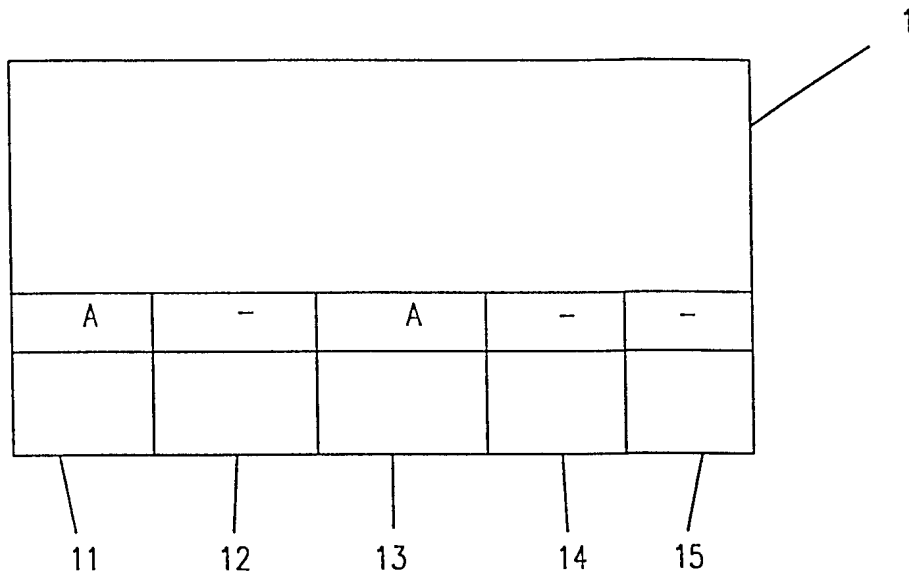


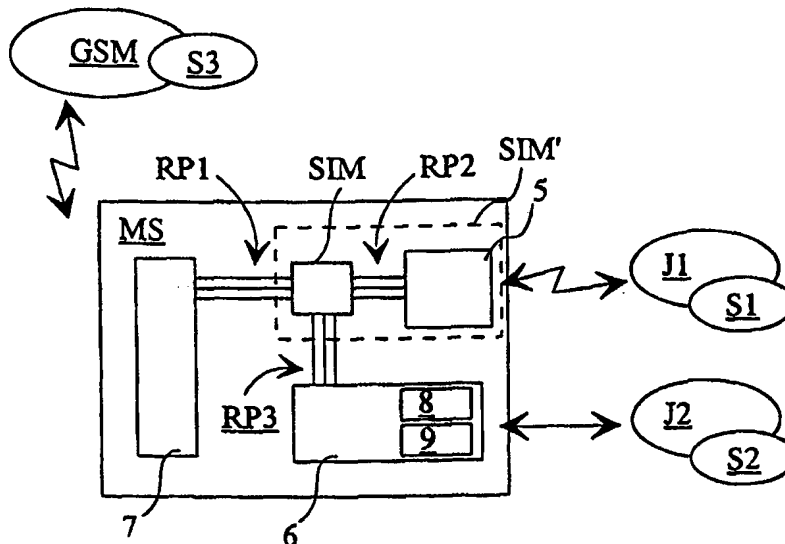
FIG. 2



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>H04Q 7/32, G07F 7/08, G06K 19/073</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 98/33343</b> (43) International Publication Date: 30 July 1998 (30.07.98)</p>
<p>(21) International Application Number: PCT/FI98/00080 (22) International Filing Date: 27 January 1998 (27.01.98) (30) Priority Data: 970339 27 January 1997 (27.01.97) FI (71) Applicant (for all designated States except US): TELECOM FINLAND OY [FI/FI]; Sturenkatu 16, FIN-00510 Helsinki (FI). (72) Inventors; and (75) Inventors/Applicants (for US only): LEHMUS, Marja-Leena [FI/FI]; Iltaruskontie 3 B 10, FIN-02120 Espoo (FI). OKSMAN, Salla [FI/FI]; Ohralantie 7, FIN-00970 Helsinki (FI). ESKOLA, Susanna [FI/FI]; Jalkamylyntie 4, FIN-00920 Helsinki (FI). LINKOLA, Janne [FI/FI]; Kuusikallionkuja 4 F 43, FIN-02210 Espoo (FI). (74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN-00101 Helsinki (FI).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> With international search report. In English translation (filed in Finnish).</p>

(54) Title: SUBSCRIBER IDENTITY MODULE MOBILE STATION AND METHOD FOR PERFORMING A SMART CARD FUNCTION



(57) Abstract

The invention relates to a subscriber identity module that makes it possible to integrate different smart card functions with the SIM card used in a mobile station. The object of the invention is to enable new diversified service combinations to be implemented so as to allow them to be utilised via a data communication device, such as a mobile station. A feature characteristic of these service combinations is that a part of the series of actions is carried out in a system and/or application external to the data communication system and the data communication device in addition to or instead of wireless communication between the mobile station and the data communication system/application.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AL</b>	Albania	<b>ES</b>	Spain	<b>LS</b>	Lesotho	<b>SI</b>	Slovenia
<b>AM</b>	Armenia	<b>FI</b>	Finland	<b>LT</b>	Lithuania	<b>SK</b>	Slovakia
<b>AT</b>	Austria	<b>FR</b>	France	<b>LU</b>	Luxembourg	<b>SN</b>	Senegal
<b>AU</b>	Australia	<b>GA</b>	Gabon	<b>LV</b>	Latvia	<b>SZ</b>	Swaziland
<b>AZ</b>	Azerbaijan	<b>GB</b>	United Kingdom	<b>MC</b>	Monaco	<b>TD</b>	Chad
<b>BA</b>	Bosnia and Herzegovina	<b>GE</b>	Georgia	<b>MD</b>	Republic of Moldova	<b>TG</b>	Togo
<b>BB</b>	Barbados	<b>GH</b>	Ghana	<b>MG</b>	Madagascar	<b>TJ</b>	Tajikistan
<b>BE</b>	Belgium	<b>GN</b>	Guinea	<b>MK</b>	The former Yugoslav Republic of Macedonia	<b>TM</b>	Turkmenistan
<b>BF</b>	Burkina Faso	<b>GR</b>	Greece			<b>TR</b>	Turkey
<b>BG</b>	Bulgaria	<b>HU</b>	Hungary	<b>ML</b>	Mali	<b>TT</b>	Trinidad and Tobago
<b>BJ</b>	Benin	<b>IE</b>	Ireland	<b>MN</b>	Mongolia	<b>UA</b>	Ukraine
<b>BR</b>	Brazil	<b>IL</b>	Israel	<b>MR</b>	Mauritania	<b>UG</b>	Uganda
<b>BY</b>	Belarus	<b>IS</b>	Iceland	<b>MW</b>	Malawi	<b>US</b>	United States of America
<b>CA</b>	Canada	<b>IT</b>	Italy	<b>MX</b>	Mexico	<b>UZ</b>	Uzbekistan
<b>CF</b>	Central African Republic	<b>JP</b>	Japan	<b>NE</b>	Niger	<b>VN</b>	Viet Nam
<b>CG</b>	Congo	<b>KE</b>	Kenya	<b>NL</b>	Netherlands	<b>YU</b>	Yugoslavia
<b>CH</b>	Switzerland	<b>KG</b>	Kyrgyzstan	<b>NO</b>	Norway	<b>ZW</b>	Zimbabwe
<b>CI</b>	Côte d'Ivoire	<b>KP</b>	Democratic People's Republic of Korea	<b>NZ</b>	New Zealand		
<b>CM</b>	Cameroon			<b>PL</b>	Poland		
<b>CN</b>	China	<b>KR</b>	Republic of Korea	<b>PT</b>	Portugal		
<b>CU</b>	Cuba	<b>KZ</b>	Kazakstan	<b>RO</b>	Romania		
<b>CZ</b>	Czech Republic	<b>LC</b>	Saint Lucia	<b>RU</b>	Russian Federation		
<b>DE</b>	Germany	<b>LI</b>	Liechtenstein	<b>SD</b>	Sudan		
<b>DK</b>	Denmark	<b>LK</b>	Sri Lanka	<b>SE</b>	Sweden		
<b>EE</b>	Estonia	<b>LR</b>	Liberia	<b>SG</b>	Singapore		

## SUBSCRIBER IDENTITY MODULE MOBILE STATION AND METHOD FOR PERFORMING A SMART CARD FUNCTION

The present invention relates to a subscriber identity module as defined in the preamble of claim 1.

5 Moreover, the invention relates to a mobile station as defined in the preamble of claim 5. The invention also relates to a procedure for applying a subscriber identity module and a mobile station as defined in the preamble of claim 10.

10 In prior art, a subscriber identity module is known that comprises a memory device, a data processing device connected to it and an interface for connection to a mobile station. Further, in a known method of communication between a subscriber identity module and a mobile station, the mobile station initiates the connection. The subscriber identity module as known at present cannot initiate communication with the mobile station. An example of such a system is the GSM system (*GSM, Global System for Mobile Commu-*  
15 *tions*). Moreover, a subscriber identity module card is known in which a single physical card may contain several independent subscriber identity modules. An example of such a system is a SIM card (*SIM, subscriber identification module*) used in the GSM system that  
20 has two processors on opposite sides of the card. In the GSM mobile telephone network, the SIM card is a component which, in addition to the subscriber's international telephone number, also contains other stored user-specific and network-specific data, such as  
25 the user's coded speed dialling numbers, a password to prevent misuse, and international codes of interconnected systems. A priority level for congestion situations can also be defined for the card. With the double SIM card described above, the user gets two separate subscriber connections, i.e. the user may make  
30 private calls at his/her own cost and on-duty calls at  
35

the cost of his/her employer. A circumstance characteristic of such a solution is that the two processors on the card are unable to communicate between themselves. In other words, the solution described above basically corresponds to a situation where two SIM cards  
5 are disposed on the same carrier.

On the other hand, a smart card is known whose structure mainly corresponds to the above-described subscriber identity module. A smart card is generally  
10 used e.g. as an access card, a key or as a bank card. In prior art, many different types of physical interface between the smart card and the external world are known. The card may be e.g. in galvanic contact with the external world. There may also be a wireless con-  
15 nection between the card and the external world. In this case, both the card and the card reader are provided with coils, between which both information and power needed for the functions of the card are transferred. Therefore, the card can communicate with the ex-  
20 ternal world at radio frequencies without a physical contact with a reader device. Examples of this type of cards are the remote-read cards used e.g. in buses.

It is also known in prior art that the subscriber identity module, or SIM, may communicate  
25 with a mobile station and a physical transmission network over a standardised interface. The data on the SIM card can be changed via the air interface by transferring information to the card using short messages, e.g. SMS and USSD messages (*SMS, Short*  
30 *Message Service; USSD, Unstructured Supplementary Service Data*). It is also possible to use a telecommunication terminal to change the data on the SIM card.

Further, many prior-art systems requiring user identification are based on a card identifying  
35 the user. Such systems include e.g. access control systems. Cards identifying the user are also used in various transactions in which the card indicates that

a payment has been remitted beforehand or registers the transaction as a credit transaction. Examples of such systems are remote-read bus tickets and credit cards issued by banks. In such systems, the updating  
5 of the cards is always done either by physically recharging the card with additional rights using a charger or by replacing an outdated disposable card with a new one. Another alternative is to update the reader, but this is only possible in the case of a li-  
10 mited number of users.

A problem with these systems is that the user must carry several different cards used in different systems. When using different systems, the user always needs a certain card designed for the particular sys-  
15 tem.

A further problem is that the various actions for updating of the cards, such as recharging the cards with money, changing the validity time, checking credit information and similar actions must always be  
20 carried out separately for each card at different points. For example, a money card is recharged at a bank, a credit card is updated on the premises of the commercial enterprise giving the credit, a bus ticket is updated at a kiosk, and so on.

25 The object of the present invention is to produce a new type of subscriber identity module that makes it possible to combine several cards used in different systems.

Another object of the invention is to produce  
30 a subscriber identity module that makes it possible to unify the use of different cards, in other words, a subscriber identity module that allows the information on cards of different systems to be updated in a centralised manner and almost independently of location by  
35 using a mobile station.

A further object of the invention is to produce a mobile station that makes it possible to combi-

ne the functions of different smart cards and that can be used in more versatile ways and also for purposes other than its conventional function.

5 A further object of the invention is produce a procedure that allows more diversified functions to be performed using a mobile station.

In short, the object of the invention is to enable new diversified service combinations to be so implemented that they can be utilised via a data communication device, such as a mobile station. A feature characteristic of these service combinations is that a part of the series of actions is carried out in a system and/or application external to the data communication system and the data communication device.

15 As for the features characteristic of the invention, reference is made to the claims.

The subscriber identity module of the invention comprises a data processing device, which may be a very simple logic circuit or a more complex micro-processor. In addition, the module comprises a memory device connected to the data processing device. The memory device may be any known type of memory, such as ROM, RAM, EPROM or EEPROM. Furthermore, the subscriber identity module of the invention comprises a first data transfer device, which is connected to the data processing device and provided with a first interface for data transfer between a mobile station (MS) and the subscriber identity module. The data transfer device may be e.g. in galvanic contact with the mobile station.

30 According to the invention, the subscriber identity module comprises a second data transfer device, which is connected to the data processing device and provided with a second interface, over which a connection for data transmission to a device and/or application other than a mobile station is set up. This other device and/or application may be any exter-



nal system provided with means for reading and/or writing data over the second interface. The subscriber identity module may also comprise more than two data transfer devices and/or interfaces.

5 In an embodiment of the present invention, the subscriber identity module comprises a reading and writing device connected to the data processing device via the second data transfer device. This reading and writing device may be a remote device as generally used e.g. in smart cards, in which information and the power needed by the module is transferred via windings or an equivalent medium. On the other hand, the reading and writing device may be an infrared operated device, in which the signalling takes place in the infrared wavelength range.

10 The invention further relates to a mobile station comprising a subscriber identity module as described above. The mobile station may preferably comprise a remote device as described above, connected over an interface to the subscriber identity module. In this case, the subscriber identity module itself may only contain a second data transfer device with a second interface, over which the desired connection to the remote device in the mobile station is set up.

15 20 25 30 35 In the procedure of the invention for performing a smart card function using a mobile station as described above, a connection between the subscriber identity module and a first external system is first established. This connection setup initialises the smart card transaction and it comprises exchange of information relating to the subscriber identity module and the external system. After this, the user is requested to give his/her approval for the execution of the smart card transaction. The request can be presented e.g. via the display of the mobile station or via a sound signal or a corresponding action. Finally, the first external system is informed of the user's appro-

val. On the other hand, in an embodiment of the invention, in addition to or instead of the user's approval, it is possible to request the approval of a second external system for the execution of the smart  
5 card transaction.

In a preferred embodiment of the procedure, predetermined information for the smart card transaction is stored in the subscriber identity module and the information is updated based on the smart card  
10 transaction under control of the first system. Such information may relate e.g. to the recharging of a rechargeable money card, in which the amount of money stored on the card is reduced on the basis of transactions.

15 The connection to the second external system is preferably established via a mobile communication network. The connection can be set up using short messages, such as SMS and/or USSD messages.

As compared with prior art, the present invention affords the advantage that the subscriber  
20 identity module of the invention makes it possible to combine several cards used in different systems. Further, the invention makes it possible to unify the use of different cards included in the subscriber identity  
25 module, in other words, it makes it possible to update the information on cards of different systems in a centralised manner and almost independently of location by using a mobile station. In addition, the invention allows various smart card services to be used  
30 with a single card.

In addition, the invention makes it possible to produce a mobile station by means of which the  
functions of different smart cards can be used and which can be used in more versatile ways and also for  
35 other purposes besides its conventional function. As a further advantage, the procedure of the invention pro-

vides a handy way to implement the previously slow and difficult smart card functions.

In the following, the invention will be described by the aid of some examples of its embodi-  
5 ments by referring to the attached drawing, in which

Fig. 1 presents a subscriber identity module according to the invention;

Fig. 2 presents a diagram representing a mobile station according to the invention;

10 Fig. 3 represents the signalling in a preferred embodiment of the present invention; and

Fig. 4a - 4c are flow diagrams representing certain preferred embodiments of the procedure of the invention.

15 The subscriber identity module SIM presented in Fig. 1 comprises a processor circuit 1 which controls all functions of the module. Moreover, the module comprises a memory circuit 2, which is connected to the processor circuit and contains all the software  
20 needed in the module, such as the operating system, data transfer protocols for different interfaces, and other programmes required. In addition, the module comprises a first data transfer device 3, which includes the functions for the establishment of a first in-  
25 terface RP1 and is used to set up a connection to a mobile station MS. Furthermore, the module comprises a second data transfer device 4, which comprises the functions for the establishment of a second interface RP2 and is used to set up a connection to a second  
30 system, e.g. to a remote-read card connected to the subscriber identity module.

The subscriber identity module presented in Fig. 1 also has other preferred embodiments, which are not actually shown in the figure but which are obvious  
35 to the skilled person from Fig. 1. One embodiment is a module that contains several processor circuits accessing a common memory area. In this case, one processor

takes care of one interface to the external world. In such an arrangement, it is necessary to ensure that when one processor is writing information to the common memory area, the others cannot read it simultaneously from the same memory area. A mechanism of this type is known e.g. from database solutions.

Another embodiment is a card with a single processor whose capacity is shared between several processes. In this case, one process takes care of data communication over one interface. Such a solution is known e.g. from the computer world. For example, the UNIX operating system can work with a single processor by utilising the processor's multitasking capability. This is the way the card would function in this embodiment. A further possibility is to use a hybrid solution comprising more than one processor but having a number of interfaces that is not the same as the number of processors.

The GSM mobile station MS represented by the diagram in Fig. 2 comprises a SIM' that has been slightly modified from the subscriber identity module SIM in Fig. 1. In addition to a module according to Fig. 1, SIM' comprises a remote-read card 5. The remote-read card 5 is connected via a wireless link to a first system J1, in which a first application S1 is operated. The subscriber identity module SIM is connected to the remote-read card via a second interface RP2. The mobile station MS further comprises an infrared device 6 comprising both an infrared transmitter 8 and an infrared receiver 9. The infrared device can also be used as a bar code reader, and the information read from an application S2 operated in a second system J2 can be transferred over a third interface RP3 into the subscriber identity module for further processing. The mobile station MS further comprises a matching module 7, which is used to establish a connection to the subscriber identity module SIM over the

first interface. In addition, as shown in Fig. 2, the mobile station communicates over a wireless connection with a GSM system and an application/applications S3 operated in it.

5 Fig. 3 represents the signalling between different parts of the assembly in a preferred embodiment of the present invention. This series of actions is also represented by the flow chart in Fig. 4a.

In Fig. 3, the server 10 is a computer com-  
10 prised in a physical transmission medium, such as a GSM network, and it is capable of communicating in the manner required by the application in the subscriber identity module card. An external system J1, e.g. a remote reader, sends a debiting message, containing  
15 information about a sum to be debited, to an application in the subscriber identity module SIM, block 21. The application in the subscriber identity module device SIM recognises the message as one sent by an external device and forwards it via a physical interfa-  
20 ce, e.g. a GSM network, as a short message, such as an SMS or USSD message, to a suitable server 10 in the GSM network. Before forwarding the message, block 22, the application in the subscriber identity module SIM may require an approval of the function from the user.  
25 If no approval is obtained, the transaction is terminated, block 23. The message received from the reader J1 must contain an identifier informing the application in the subscriber identity module SIM that a response to the message is expected. The server 10 in  
30 turn must contain a programme that is able to interpret the messages arriving from the subscriber identity module SIM and respond to them appropriately. An appropriate response may involve e.g. verification of the creditworthiness of the subscriber identity module  
35 that sent the SMS or USSD message, and the granting or turning down of credit. A response indicating granting or rejection of credit is sent to the subscriber iden-

tity module in the form of an SMS or USSD or other short message, which is identified by the module application as a response to a message sent out shortly before, and forwarded to an external reader J1, block 5 24. The arrival of a response in the reader J1 must be indicated e.g. by a sound signal. If an affirmative answer is received, the reader J1 responds by printing a receipt for the payment. If the answer is negative, the reader J1 responds by announcing that the payment 10 could not be made, block 25.

An SMS sent by the subscriber identity module SIM must contain a code (e.g. IMSI in the GSM system) identifying the subscriber identity module, the amount debited as well as other information relating to the 15 debiting, such as the date and the place and time of purchase. Moreover, the system must contain encryption and authentication mechanisms.

Referring to Fig. 4b, if the subscriber identity module card in the transaction illustrated by the 20 figure is a so-called prepaid card, no debiting will have to be done from the server 10. Instead, money is first loaded into the module SIM e.g. using a SMS message, block 31. The procedure continues by first reading into the subscriber identity module SIM the 25 sum to be debited, block 32, and then debiting the customer by decreasing (block 33) his/her payment tickets created beforehand on the card SIM. Finally, the seller's system J1 is informed of the remittance.

Correspondingly, in a third example, represented by the flow diagram in Fig. 4c and relating to 30 access control, the signalling is based on the use of a GSM network as a physical transmission link by making use of short messages, such as SMS or USSD messages to transmit information. The user requests 35 access by sending either an SMS, USSD or other short message, block 41. To be able to make the request, the subscriber identity module card SIM must contain an

application that knows how to ask both the user and the server for the right things. In GSM cards, this could be implemented using an Application Toolkit consistent with the GSM standards. The server must perform the required actions to allow or deny access and, if necessary, to debit the user for the permission, in which case the user's creditworthiness must be verified or tickets decreased on a prepaid card. As in the previous example, in this case, too, the server receives information indicating that a response to the message is expected. An external reader verifies the user's right of access by asking the subscriber identity card about the right of access. If the card has the right of access, the reader will indicate this by giving a sound signal or by opening the door. In the case of a card with a right of access granted for a certain period, the right can be removed from the card by sending a new SMS, USSD or other short message and deleting the field indicating right of access.

Another arrangement for verifying the right of access of the card is that the information regarding right of access is located in the reader instead of on the card, and a server in the transmission network sends the reader J1 information regarding the right of access of each card at certain intervals. In this case, the reader J1 only asks the card SIM for an identification number, block 42, and compares it with its own data to decide about the user's right of access, block 43. In the case of rights granted for a certain period, the right of access expires when the card number is no longer updated in the reader as an allowed number entitled to access. In the case of the solution described, the server could be provided with a timer whose triggering would result in removing outdated card numbers indicating right of access.

To sum up, let it be stated that in practice the actions described above are realised by briefly

exposing a telephone to a remote reader and verifying the transaction via the user interface of the telephone, whereupon the transaction is recorded in the remote reader. Depending on the nature of the transaction, 5 either a data link is needed between the remote reader and the data system or the files in the remote reader are transferred into the data system e.g. at the end of each day. Thus, a user having a mobile station with a suitable card in it will be able to carry out various smart card functions using only his/her telephone. 10

The invention is not restricted to the examples of its embodiments described above, but many variations are possible within the scope of the inventive idea defined by the claims.



## CLAIMS

1. Subscriber identity module (SIM), comprising a data processing device (1), a memory device (2) connected to the data processing device, and a first data transfer device (3), which is connected to the data processing device and provided with a first interface (RP1) for data transfer between a mobile station (MS) and the subscriber identity module, characterised in that the subscriber identity module (SIM) comprises a second data transfer device (4), which is connected to the data processing device (1) and provided with a second interface (RP2), over which a data transfer connection to a device and/or application other than a mobile station is set up.
2. Subscriber identity module as defined in claim 1, characterised in that the subscriber identity module (SIM) comprises a reading and writing device (5) connected to the data processing device (1) via the second data transfer device (4).
3. Subscriber identity module as defined in claim 1 or 2, characterised in that the reading and writing device (5) is a remote device.
4. Subscriber identity module as defined in any one of claims 1 - 3, characterised in that the reading and writing device (5) is an infrared device.
5. Mobile station comprising a subscriber identity module that comprises a data processing device (1), a memory device (2) connected to the data processing device, and a first data transfer device (3), which is connected to the data processing device and provided with a first interface for data transfer between the mobile station (MS) and the subscriber identity module, characterised in that the subscriber identity module (SIM) comprises a second data transfer device (4), which is connected to the

data processing device (1) and provided with a second interface, a data transfer connection being set up over the second interface to a device and/or application other than a mobile station.

5           6. Mobile station as defined in claim 5, characterised in that the subscriber identity module (SIM) comprises a reading and writing device (5) connected to the data processing device (1) via the second data transfer device (4).

10           7. Mobile station as defined in claim 5 or 6, characterised in that the reading and writing device (5) is a remote device.

            8. Subscriber identity module as defined in any one of claims 5 - 7, characterised in  
15 that the reading device (5) is an infrared device.

            9. Mobile station as defined in any one of claims 5 - 7, characterised in that the mobile station comprises a remote device (6) connected over a third interface (RP3) to the subscriber identity module (SIM).  
20

            10. Procedure for performing a smart card function using a mobile station as defined in claim 5, characterised in that

            a connection between the subscriber identity  
25 module and a first external system is established;

            the user is requested to give his/her approval for the execution of the smart card function; and

            the first external system is informed of the user's approval.

30           11. Procedure as defined in claim 10, characterised in that a second external system is requested to give its approval for the execution of the smart card function.

            12. Procedure as defined in claim 10 or 11,  
35 characterised in that predetermined information for the smart card function is stored in the subscriber identity module and the information is up-

dated based on the smart card function under control of the first system.

13. Procedure as defined in any one of claims 10 - 12, characterised in that the connection  
5 to the second external system is established via a mobile communication network.

14. Procedure as defined in claim 13, characterised in that short messages, preferably SMS and/or USSD messages, and/or other message  
10 transmission methods defined in the GSM standard are used for the transmission of information in the mobile communication network.

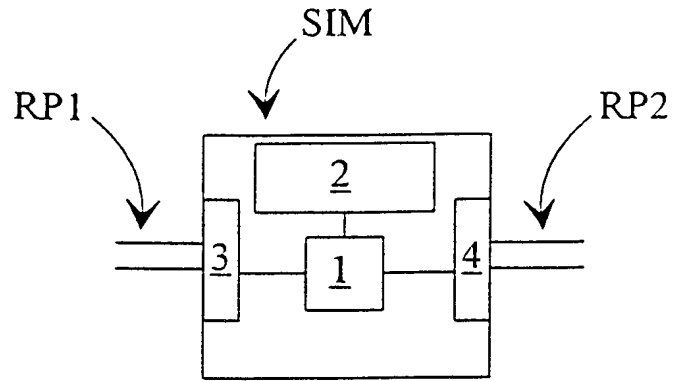


Fig 1

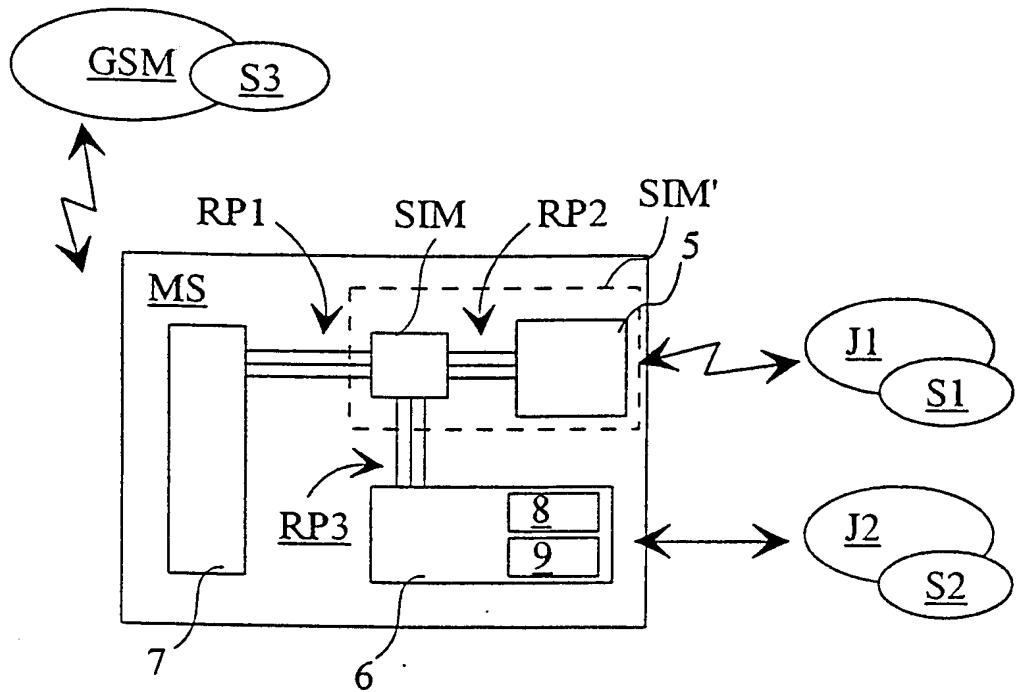


Fig 2

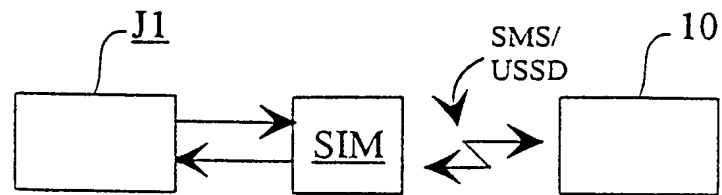


Fig 3

2/2

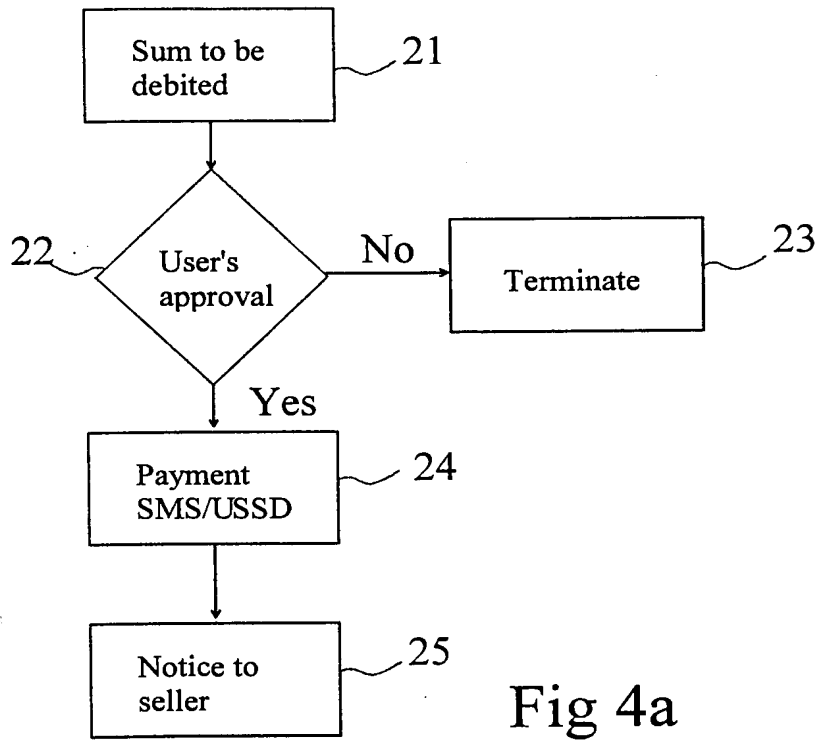


Fig 4a

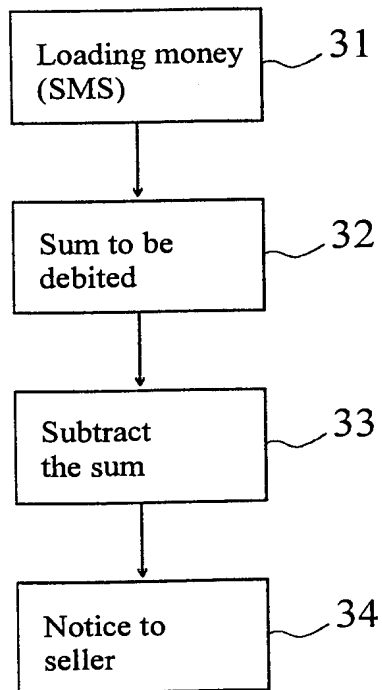


Fig 4b

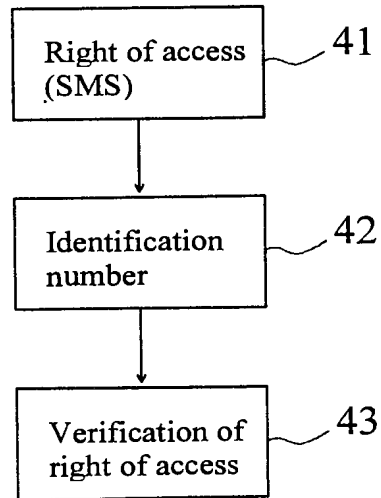


Fig 4c



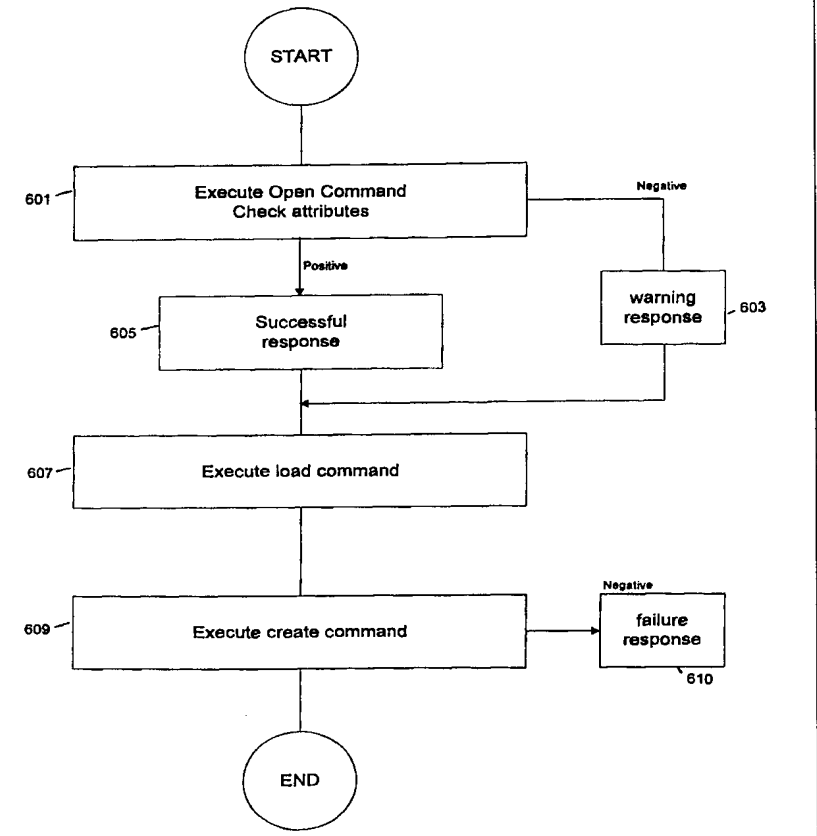
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : <b>G07F 7/10</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 98/37526</b> (43) International Publication Date: 27 August 1998 (27.08.98)</p>
<p>(21) International Application Number: PCT/GB98/00531 (22) International Filing Date: 19 February 1998 (19.02.98) (30) Priority Data: 9703591.9 21 February 1997 (21.02.97) GB 60/046,514 15 May 1997 (15.05.97) US 09/023,057 12 February 1998 (12.02.98) US (71) Applicant: MONDEX INTERNATIONAL LIMITED [GB/GB]; 47-53 Cannon Street, London EC4M 5SQ (GB). (72) Inventors: EVERETT, David, Barrington; 31 Ashdown Avenue, Saltdean, Brighton, East Sussex BN2 8AH (GB). MILLER, Stuart, James; 9 Woodford Green, The Warren, Bracknell, Berkshire RG12 9YQ (GB). PEACHAM, Anthony, David; 4 Lynwood, Groombridge, Tunbridge Wells, Kent TN3 9LX (GB). SIMMONS, Ian, Stephens; The Elms, School Road, Broughton, Cambridgeshire PE17 3AT (GB). RICHARDS, Timothy, Philip; 32 Craig Mount, Radlett, Hertfordshire WD7 7LW (GB). VINER, John, Charles; Hydes, Woodlands Lane, Windlesham, Surrey GU20 6AN (GB). (74) Agents: POTTER, Julian, Mark et al.; D. Young &amp; Co., 21 New Fetter Lane, London EC4A 1DA (GB).</p>	<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>	

(54) Title: MULTI-APPLICATION IC CARD SYSTEM

(57) Abstract

A multi-application IC card system is disclosed having selective application loading and deleting capability. Prior to loading an application onto an IC card a test is conducted to determine if the card is qualified to receive the application using personalization data stored on the card and comparing it with permissions data associated with the application indicating one or more sets of cards upon which the application may be loaded. If the personalization data of the card falls within the allowable set of permissions for that application then the card may be loaded with the application. Preferably, the personalization data includes data representative of the card number, issuer, a product class and the date on which the card is personalized.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AL</b>	Albania	<b>ES</b>	Spain	<b>LS</b>	Lesotho	<b>SI</b>	Slovenia
<b>AM</b>	Armenia	<b>FI</b>	Finland	<b>LT</b>	Lithuania	<b>SK</b>	Slovakia
<b>AT</b>	Austria	<b>FR</b>	France	<b>LU</b>	Luxembourg	<b>SN</b>	Senegal
<b>AU</b>	Australia	<b>GA</b>	Gabon	<b>LV</b>	Latvia	<b>SZ</b>	Swaziland
<b>AZ</b>	Azerbaijan	<b>GB</b>	United Kingdom	<b>MC</b>	Monaco	<b>TD</b>	Chad
<b>BA</b>	Bosnia and Herzegovina	<b>GE</b>	Georgia	<b>MD</b>	Republic of Moldova	<b>TG</b>	Togo
<b>BB</b>	Barbados	<b>GH</b>	Ghana	<b>MG</b>	Madagascar	<b>TJ</b>	Tajikistan
<b>BE</b>	Belgium	<b>GN</b>	Guinea	<b>MK</b>	The former Yugoslav Republic of Macedonia	<b>TM</b>	Turkmenistan
<b>BF</b>	Burkina Faso	<b>GR</b>	Greece			<b>TR</b>	Turkey
<b>BG</b>	Bulgaria	<b>HU</b>	Hungary	<b>ML</b>	Mali	<b>TT</b>	Trinidad and Tobago
<b>BJ</b>	Benin	<b>IE</b>	Ireland	<b>MN</b>	Mongolia	<b>UA</b>	Ukraine
<b>BR</b>	Brazil	<b>IL</b>	Israel	<b>MR</b>	Mauritania	<b>UG</b>	Uganda
<b>BY</b>	Belarus	<b>IS</b>	Iceland	<b>MW</b>	Malawi	<b>US</b>	United States of America
<b>CA</b>	Canada	<b>IT</b>	Italy	<b>MX</b>	Mexico	<b>UZ</b>	Uzbekistan
<b>CF</b>	Central African Republic	<b>JP</b>	Japan	<b>NE</b>	Niger	<b>VN</b>	Viet Nam
<b>CG</b>	Congo	<b>KE</b>	Kenya	<b>NL</b>	Netherlands	<b>YU</b>	Yugoslavia
<b>CH</b>	Switzerland	<b>KG</b>	Kyrgyzstan	<b>NO</b>	Norway	<b>ZW</b>	Zimbabwe
<b>CI</b>	Côte d'Ivoire	<b>KP</b>	Democratic People's Republic of Korea	<b>NZ</b>	New Zealand		
<b>CM</b>	Cameroon	<b>KR</b>	Republic of Korea	<b>PL</b>	Poland		
<b>CN</b>	China	<b>KZ</b>	Kazakhstan	<b>PT</b>	Portugal		
<b>CU</b>	Cuba	<b>LC</b>	Saint Lucia	<b>RO</b>	Romania		
<b>CZ</b>	Czech Republic	<b>LI</b>	Liechtenstein	<b>RU</b>	Russian Federation		
<b>DE</b>	Germany	<b>LK</b>	Sri Lanka	<b>SD</b>	Sudan		
<b>DK</b>	Denmark	<b>LR</b>	Liberia	<b>SE</b>	Sweden		
<b>EE</b>	Estonia			<b>SG</b>	Singapore		

## MULTI-APPLICATION IC CARD SYSTEM

Integrated circuit ("IC") cards are becoming increasingly used for many different purposes in the world today. An IC card (also called a smart card) typically is the size of a conventional credit card which contains a computer chip including a microprocessor, read-only-memory (ROM), electrically erasable programmable read-only-memory (EEPROM), an Input/Output (I/O) mechanism and other circuitry to support the microprocessor in its operations. An IC card may contain a single application or may contain multiple independent applications in its memory. MULTOS™ is a multiple application operating system which runs on IC cards, among other platforms, and allows multiple applications to be executed on the card itself. This allows a card user to run many programs stored in the card (for example, credit/debit, electronic money/purse and/or loyalty applications) irrespective of the type of terminal (i.e., ATM, telephone and/or POS) in which the card is inserted for use.

A conventional single application IC card, such as a telephone card or an electronic cash card, is loaded with a single application at its personalization stage. That application, however, cannot be modified or changed after the card is issued even if the modification is desired by the card user or card issuer. Moreover, if a card user wanted a variety of application functions to be performed by IC cards issued to him or her, such as



both an electronic purse and a credit/debit function, the card user would be required to carry multiple physical cards on his or her person, which would be quite cumbersome and inconvenient. If an application developer or card user desired two different applications to interact or exchange data with each other, such as a purse application interacting with a frequent flyer loyalty application, the card user would be forced to swap multiple cards in and out of the card-receiving terminal, making the transaction difficult, lengthy and inconvenient.

The Applicant has recognised therefore, that it is beneficial to store multiple applications on the same IC card. For example, a card user may have both a purse application and a credit/debit application on the same card so that the user could select which type of payment (by electronic cash or credit card) to use to make a purchase. Multiple applications could be provided to an IC card if sufficient memory exists and an operating system capable of supporting multiple applications is present on the card. Although multiple applications could be pre-selected and placed in the memory of the card during its production stage, it would also be beneficial to have the ability to load and delete applications for card post-production as needed.

The increased flexibility and power of storing multiple applications on a single card create new challenges to be overcome concerning the integrity and security of the information (including application code and associated data) exchanged between the individual card and the application provider as well as within the entire system when loading and deleting applications. The Applicant has further recognised that it would be beneficial to have the capability of the IC card system to exchange data among cards, card issuers, system operators and application

providers securely and to load and delete applications securely at any time from either a terminal or remotely over a telephone line, internet or intranet connection or other data conduit. Because these data transmission lines are not typically secure lines, a number of security and entity-authentication techniques must be implemented to make sure that applications being sent over the transmission lines are only loaded on the intended cards.

As mentioned, it is important -- particularly where there is a continuing wide availability of new applications to the cardholder -- that the system has the capability of adding applications onto the IC card subsequent to issuance. This is highly advantageous since it protects the longevity of the IC cards; otherwise, once an application becomes outdated, the card would be useless. In this regard, to protect against the improper or undesired loading of applications onto IC cards, the Applicant has further recognised that it would be beneficial for the IC card system to have the capability of controlling the loading process and restricting, when necessary or desirable, the use of certain applications to a limited group or number of cards such that the applications are "selectively available" to the IC-cards in the system. This "selective capability" would allow the loading and deleting of applications at, for example, a desired point in time in the card's life cycle. It would also allow the loading of an application only to those cards chosen to receive the selected application.

Accordingly, it is an advantage of a preferred embodiment of the invention that it provides these important features and specifically a secure IC-card system that allows for selective availability of smart card applications which may be loaded onto IC cards.

These and other advantages are achieved by an embodiment of the present invention which provides an IC card system comprising at least one IC card and an application to be loaded onto the card wherein the IC card contains card personalization data and the application is assigned application permissions data designating which IC card or group of IC cards upon which the application may be loaded. The system checks to determine whether the card's personalization data falls within the permissible set indicated by the application's permissions data. If it does, the application may be loaded onto the card.

In a preferred embodiment, the card personalization data is transferred onto the card by the personalization bureau after the card is manufactured. The data preferably includes data representing the card number, the issuer, product class (i.e., such as gold or platinum cards), and the date on which the card was personalized. The card further preferably contains enablement data indicating whether or not the card has been enabled with personalized data.

In a further preferred embodiment, the IC card secure system checks the enablement data prior to loading an application to determine whether or not the card has been enabled. Preferably, if the card has been enabled, the system checks if the card number, the issuer, the product class and/or the date on which the card was personalized are within the acceptable set indicated by the application's permissions data. If so, the application may be loaded onto the IC card.

In yet another preferred embodiment, the application's permissions data may contain data representative of a blanket permission such that all cards would pass for application loading.

Further aspects, features and advantages of embodiments of the invention will become apparent from the following detailed description taken in conjunction with the accompanying figures showing illustrative embodiments of the invention, in which

Fig. 1 is block diagram illustrating the three stages in the life of a multi-application IC card in a secure system;

Fig. 2 is a block diagram illustrating the steps of the card manufacture process;

Fig. 3 is a flow diagram illustrating the steps involved in enabling each of the IC cards in the secure system;

Fig. 4 is a block diagram of an IC card chip which can be used in accordance with an embodiment of the invention;

Fig. 5 is a block diagram illustrating the data stored on the IC card as indicated in block 307 of Fig. 3;

Fig. 5A is a schematic of the data structures residing in an IC card and representing personalization data;

Fig. 6 is a flowchart illustrating the steps of loading an application onto an IC card in the secure system;

Fig. 7 is a flow chart illustrating the checking steps as indicated in block 601 of Fig. 6;

5 Fig. 8 is a flowchart illustrating the steps undertaken in determining if loading of an application may proceed;

Fig. 9 is a block diagram showing the components of the system architecture for the enablement process of an IC card in a secure multi-application IC card system; and

10 Fig. 10 is a system diagram of entities involved with the use of the IC card once it has been personalized.

Throughout the figures, the same reference numerals and characters, unless otherwise stated, are used to denote like features, elements, components or portions of the illustrated embodiments. Moreover, while the subject invention will now be described in detail with reference to the figures, it is done so in connection with the illustrative embodiments. It is intended that changes and modifications can be made to the described embodiments without departing from the true scope and spirit of the subject invention as defined by the appended claims.

15

An embodiment of the present invention provides an IC card system and process which allow the flexibility to load and delete selected applications over the lifetime of a multi-application IC card in response to the needs or desires of the card user, card issuers and/or application developers. A card user who has such a card can selectively load and delete applications as desired if allowed by the card issuer in conjunction with the system operator or Certification Authority ("CA") which controls the loading and deleting process by certifying the transfer of information relating to the process.

By allowing applications to be selectively loaded and deleted from the card, a card issuer can extend additional functionality to an individual IC card without having to issue new cards. Moreover, application developers can replace old applications with new enhanced versions, and applications residing on the same card using a common multiple application operating system may interact and exchange data in a safe and secure manner. For example, a frequent flyer loyalty program may automatically credit one frequent flyer mile to a card user's internal account for every dollar spent with an electronic purse such as the Mondex purse or with a credit/debit application. By allowing the ability to selectively load and delete applications, the card user, subject to the requirements of the card issuer, also has the option of changing loyalty programs as desired.

A card issuer or application developer may intend that a particular application be loaded on only one card for a particular card user in a card system. A regional bank may desire to have a proprietary application reside only on the cards which

the bank issues. Embodiments in accordance with the present invention would allow for this selective loading and specifically allow for the prevention of loading proprietary applications onto unauthorized cards issued by others.

To achieve these desired objectives, embodiments of the present invention give each card a specific identity by storing "card personalization data" on the card. Moreover, each application to be loaded or deleted on one or more cards in the system is assigned "application permissions data" which specify the cards upon which the applications may be loaded.

The type of personalized data can vary depending upon the needs and requirements of the card system. In the preferred embodiment, described in greater detail below, the personalization data include unique card identification designation data, the card issuer, the product class or type (which is defined by the card issuer) and the date of personalization. However, not all of these data elements are required to be used and additional elements could also be included.

The application permissions data associated with an application, also described in greater detail below, can be a single value in an identity field or could include multiple values in the identity field. For example, the application permissions data in the card issuer field could represent both product class A and product class B from a certain Bank X, indicating that the application could be loaded onto cards designated as product classes A and B issued by Bank X (as indicated in the card product ID field of the card's personalization data).

In addition, a “global value” could be stored in the issuer field (or other field) of the application permissions data indicating that all IC cards in the system regardless of who issued the card would match this permissions field. In this case, for example, a data value of zero stored in the application permissions card-issuer field will  
5 match all of the cards’ personalization card-issuer fields.

Figure 1 shows the three steps involved in providing an operational multi-application IC card in a secure system. The first step is the card manufacturing step 101. The second step is the personalization step 103 where card personalization data (also called entity authentication data) is loaded onto the card. The third step is the application  
10 loading step 105 which checks to see if a card is qualified to receive an application, i.e., when the personalization data is checked against the application permissions data associated with the application to be loaded. Each of these three steps is described in detail below.

#### Card Manufacture

15 Figure 2 shows the steps necessary in manufacturing an IC card in a secure system. Step 201 manufactures the physical IC card by creating the integrated circuit on silicon and placing it on the card. The integrated circuit chip will include RAM, ROM and EEPROM memories. When the card is first manufactured, a global public key of the system operator (in this case called the Certification Authority (CA)) is stored on each  
20 card in ROM in step 203. This will allow the card to authenticate that the source of any message to it is from the CA since the public key on the card will be matched to the CA’s secret key.