

17224
U.S. PTO
011906

UTILITY PATENT APPLICATION TRANSMITTAL <i>(Only for new nonprovisional applications under 37 CFR 1.53(b))</i>	Attorney Docket No.	080379-000100US
	First Inventor	Hulst, Hermen-ard
	Title	DATA STORAGE AND ACCESS SYSTEMS
	Express Mail Label No.	EV 383391336 US

112948 U.S. PTO
11/336758

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. **Fee Transmittal Form** (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. **Applicant claims small entity status.**
See 37 CFR 1.27.
3. **Specification** [Total Pages 61]
Both the claims and abstract must start on a new page
(For information on the preferred arrangement, see MPEP 608.01(a))
4. **Drawing(s)** (35 U.S.C. 113) [Total Sheets 17]
5. **Oath or Declaration** [Total Sheets 2]
 a. Newly executed (original or copy)
 b. A copy from a prior application (37 CFR 1.63 (d))
(for a continuation/divisional with Box 18 completed)
 i. **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. **Application Data Sheet.** See 37 CFR 1.76
7. **CD-ROM or CD-R** in duplicate, large table or
 Computer Program (*Appendix*)
 Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
(if applicable, items a. - c. are required)
 a. **Computer Readable Form (CRF)**
 i. Computer Readable Form (CRF)
 ii. Transfer Request (37 CFR 1.821(e))
 b. **Specification Sequence Listing on:**
 i. CD-ROM or CD-R (2 copies); or
 ii. Paper
 c. Statements verifying identity of above copies

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

- ACCOMPANYING APPLICATION PARTS**
9. **Assignment Papers** (cover sheet & document(s))
 Name of Assignee Smart-Flash Limited
 10. **37 CFR 3.73(b) Statement** **Power of Attorney**
(when there is an assignee)
 11. **English Translation Document** (if applicable)
 12. **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
 Copies of foreign patent documents,
 publications, & other information
 13. **Preliminary Amendment**
 14. **Return Receipt Postcard** (MPEP 503)
(Should be specifically itemized)
 15. **Certified Copy of Priority Document(s)**
(if foreign priority is claimed)
 16. **Nonpublication Request** under 35 U.S.C. 122 (b)(2)(B)(i).
 Applicant must attach form PTO/SB/35 or its equivalent.
 17. 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:

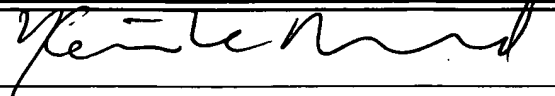
Continuation Divisional Continuation-in-part (CIP) of prior application No: 10/111,716

Prior application information: Examiner S. Paik Art Unit: 2876

19. CORRESPONDENCE ADDRESS

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

Name			
Address			
City	State	Zip Code	
Country	Telephone	Email Address	

Signature		Date	01/19/06
Name (Print/Type)	Kevin T. LeMond	Registration No. (Attorney/Agent)	35,933

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL

For FY 2006

Complete if Known

Application Number	
Filing Date	January 19, 2006
First Named Inventor	Hulst, Hermen-ard
Examiner Name	
Art Unit	
Attorney Docket No.	080379-000100US

 Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	(\$) 2950
-------------------------	-----------

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: Townsend and Townsend and Crew 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) under 37 CFR 1.16 and 1.17 Credit any overpayments

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 Small Entity		SEARCH FEES Small Entity		EXAMINATION FEES Small Entity		Fees Paid (\$)
	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	
Utility	300	150	500	250	200	100	500
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Small Entity	
	Fee (\$)	Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee (\$)	Fee Paid (\$)	Multiple Dependent Claims	Fee (\$)	Fee Paid (\$)
74	-20 or HP = 54	x \$25	= \$1,350			

HP = highest number of total claims paid for, if greater than 20

Indep. Claims	Extra Claims	Fee (\$)	Fee Paid (\$)
14	-3 or HP = 11	x \$100	= \$1,100

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, 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).


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)

Non-English Specification, \$130 fee (no small entity discount)

Other: _____

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	35,933	Telephone	415-576-0200
Name (Print/Type)	Kevin T. LeMond			Date	01/19/06

17224
U.S. PTO
011906

UTILITY PATENT APPLICATION TRANSMITTAL <small>(Only for new nonprovisional applications under 37 CFR 1.53(b))</small>	Attorney Docket No.	080379-000100US
	First Inventor	Hulst, Hermen-ard
	Title	DATA STORAGE AND ACCESS SYSTEMS
	Express Mail Label No.	EV 383391336 US

112948 U.S. PTO
11/336758

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. **Fee Transmittal Form** (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. **Applicant claims small entity status.**
See 37 CFR 1.27.
3. **Specification** [Total Pages 61]
Both the claims and abstract must start on a new page
(For information on the preferred arrangement, see MPEP 608.01(a))
4. **Drawing(s)** (35 U.S.C. 113) [Total Sheets 17]
5. **Oath or Declaration** [Total Sheets 2]
 a. Newly executed (original or copy)
 b. A copy from a prior application (37 CFR 1.63 (d))
(for a continuation/divisional with Box 18 completed)
 i. **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. **Application Data Sheet.** See 37 CFR 1.76
7. **CD-ROM or CD-R** in duplicate, large table or Computer Program (*Appendix*)
 Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
(if applicable, items a. - c. are required)
 a. **Computer Readable Form (CRF)**
 i. Computer Readable Form (CRF)
 ii. Transfer Request (37 CFR 1.821(e))
 b. **Specification Sequence Listing on:**
 i. CD-ROM or CD-R (2 copies); or
 ii. Paper
 c. Statements verifying identity of above copies

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

- ACCOMPANYING APPLICATION PARTS**
9. **Assignment Papers** (cover sheet & document(s))
Name of Assignee Smart-Flash Limited
 10. **37 CFR 3.73(b) Statement** **Power of Attorney**
(when there is an assignee)
 11. **English Translation Document** (if applicable)
 12. **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
 Copies of foreign patent documents, publications, & other information
 13. **Preliminary Amendment**
 14. **Return Receipt Postcard** (MPEP 503)
(Should be specifically itemized)
 15. **Certified Copy of Priority Document(s)**
(if foreign priority is claimed)
 16. **Nonpublication Request** under 35 U.S.C. 122 (b)(2)(B)(i).
Applicant must attach form PTO/SB/35 or its equivalent.
 17. **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:

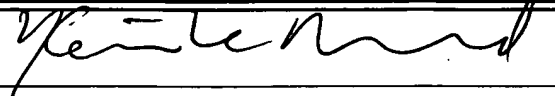
Continuation Divisional Continuation-in-part (CIP) of prior application No: 10/111,716

Prior application information: Examiner S. Paik Art Unit: 2876

19. CORRESPONDENCE ADDRESS

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

Name				
Address				
City	State	Zip Code		
Country	Telephone	Email Address		

Signature		Date	01/19/06
Name (Print/Type)	Kevin T. LeMond	Registration No. (Attorney/Agent)	35,933

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL

For FY 2006

Complete if Known

Application Number	
Filing Date	January 19, 2006
First Named Inventor	Hulst, Hermen-ard
Examiner Name	
Art Unit	
Attorney Docket No.	080379-000100US

 Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	(\$) 2950
-------------------------	-----------

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: Townsend and Townsend and Crew 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) under 37 CFR 1.16 and 1.17 Credit any overpayments

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 Small Entity		SEARCH FEES Small Entity		EXAMINATION FEES Small Entity		Fees Paid (\$)
	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	
Utility	300	150	500	250	200	100	500
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Small Entity	
	Fee (\$)	Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee (\$)	Fee Paid (\$)	Multiple Dependent Claims	Fee (\$)	Fee Paid (\$)
74	-20 or HP = 54	x \$25	= \$1,350			

HP = highest number of total claims paid for, if greater than 20

Indep. Claims	Extra Claims	Fee (\$)	Fee Paid (\$)
14	-3 or HP = 11	x \$100	= \$1,100

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, 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).


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)

Non-English Specification, \$130 fee (no small entity discount)

Other: _____

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	35,933	Telephone	415-576-0200
Name (Print/Type)	Kevin T. LeMond			Date	01/19/06

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.

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 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; 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.

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) 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 last 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.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

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.

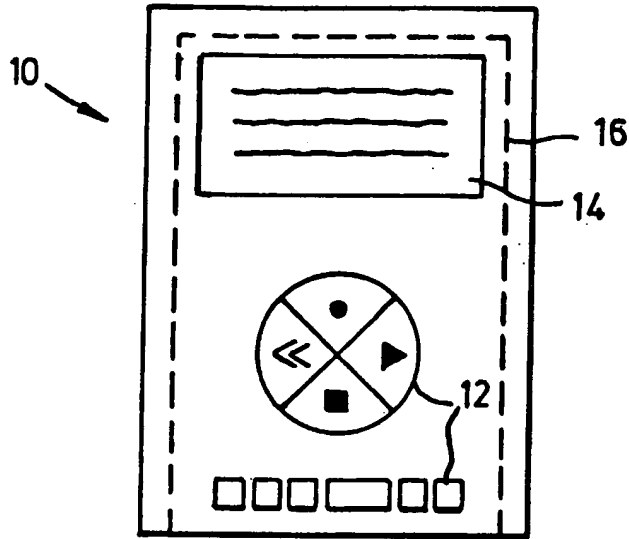
ABSTRACT

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 unauthorized access to data such as compressed music and video data, especially over the Internet.

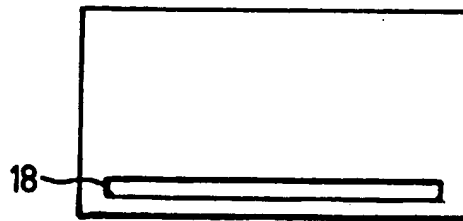
SF 1340006 v1

1/17
Fig. 1

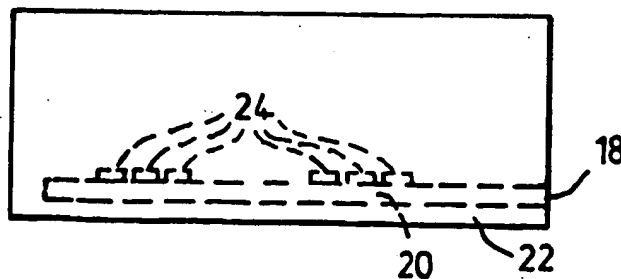
A



B



C



SUBSTITUTE SHEET (RULE 26)

Fig. 2

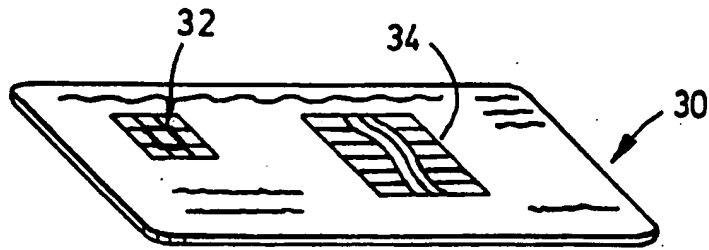
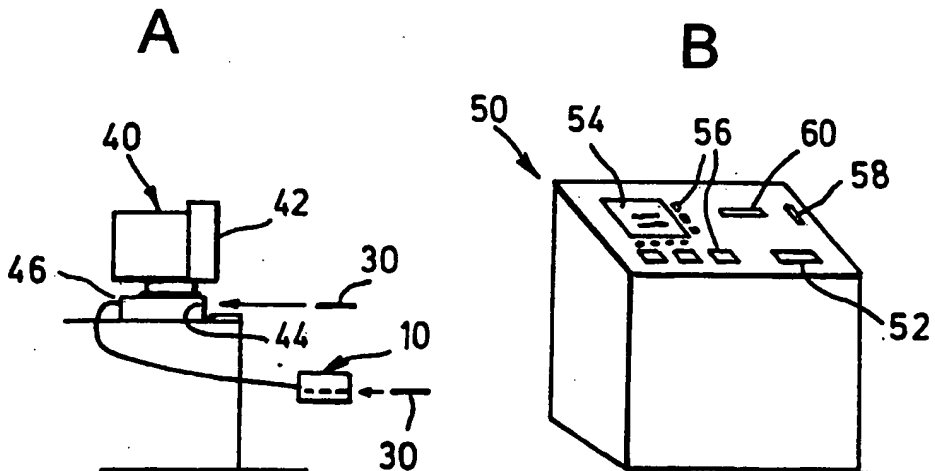


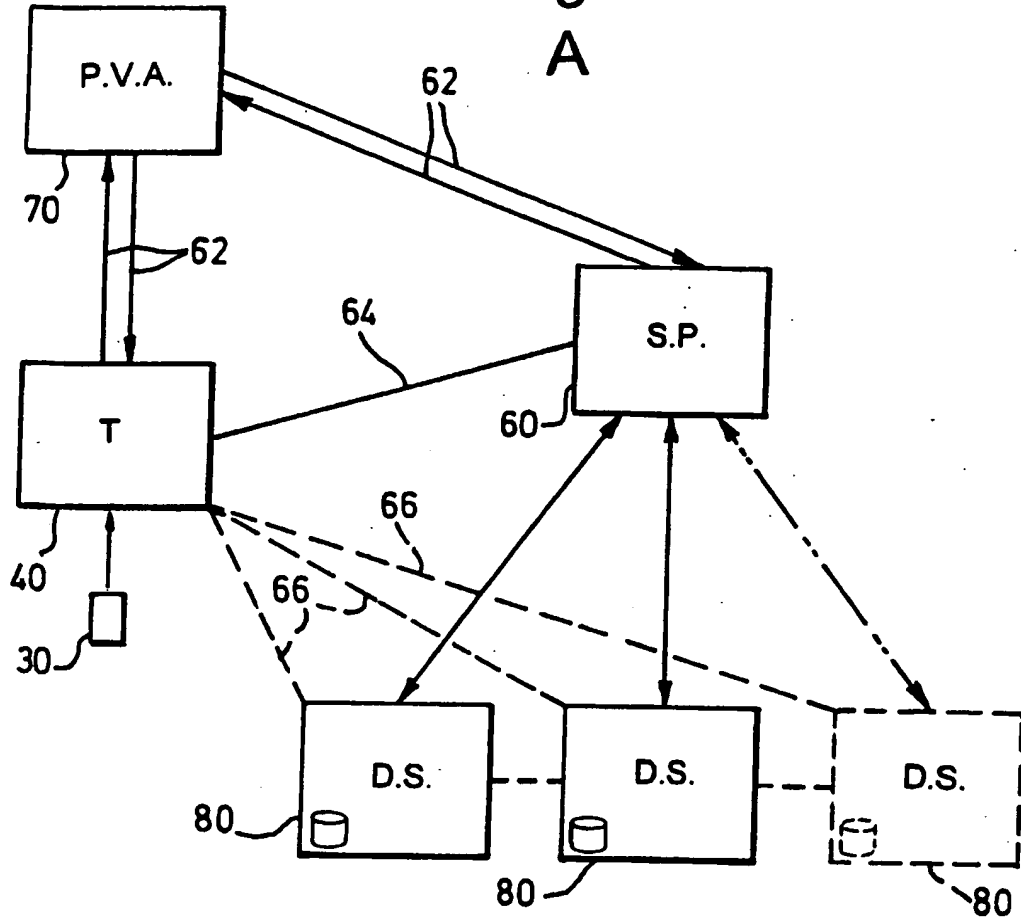
Fig. 3



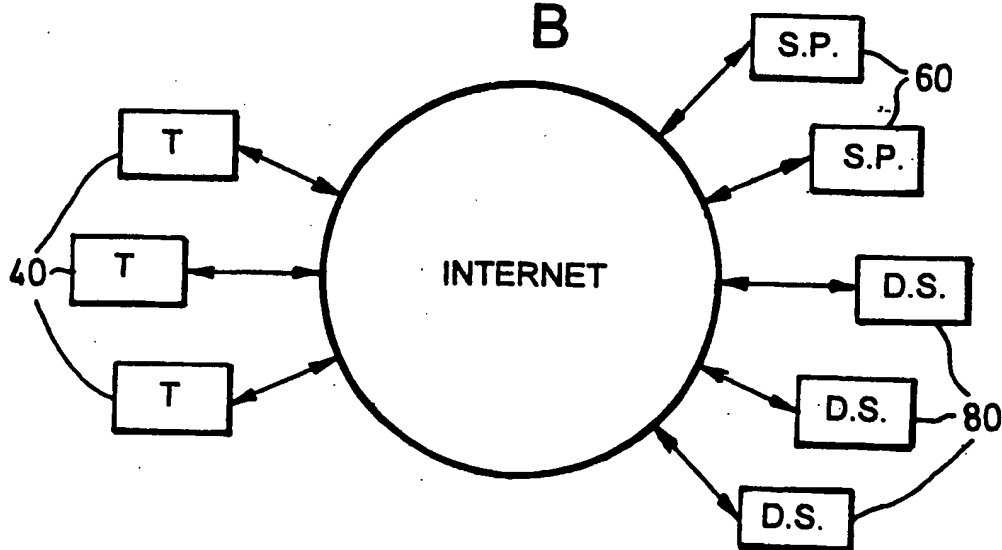
3/17

Fig. 4

A



B



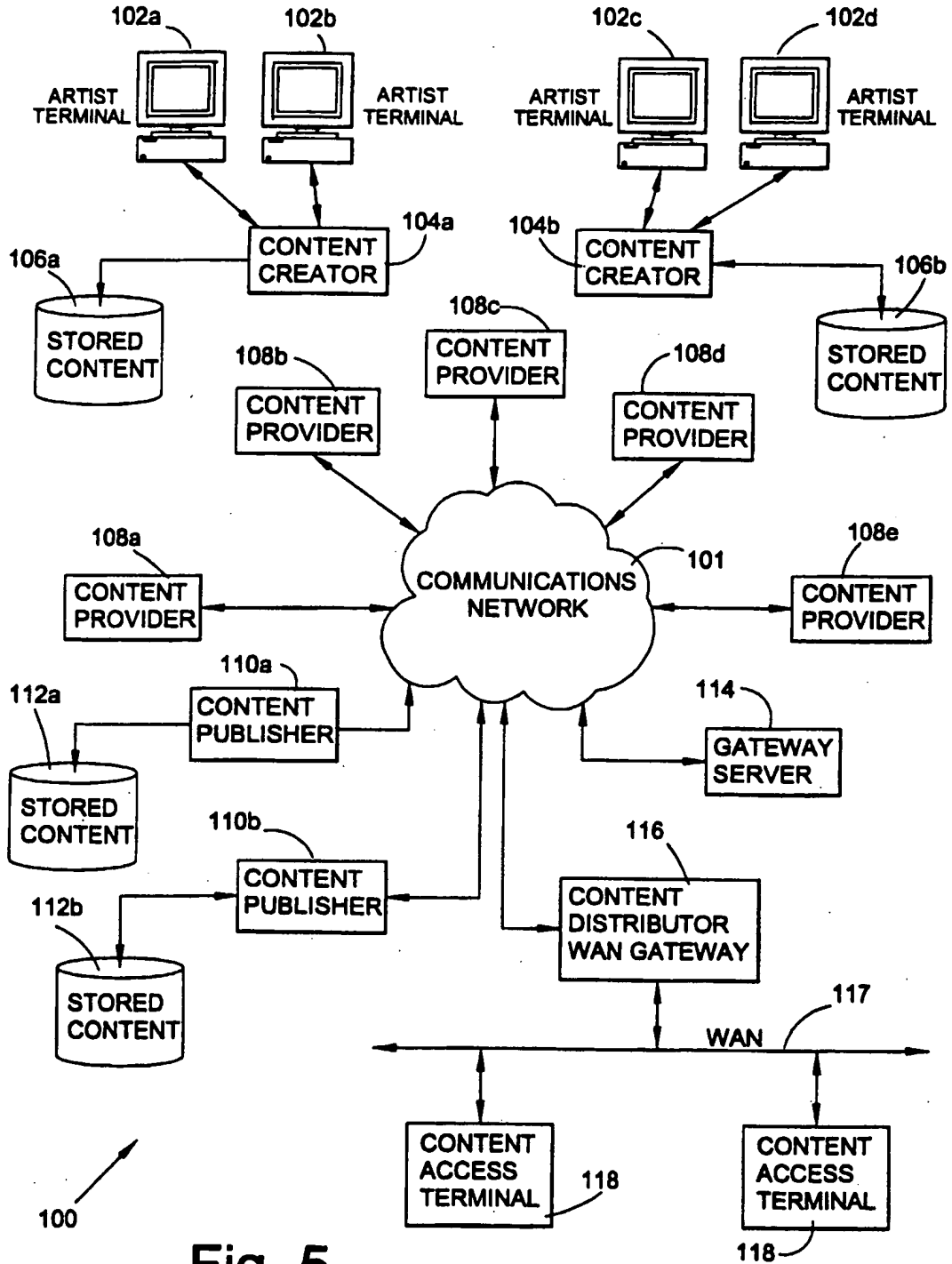


Fig. 5

5/17

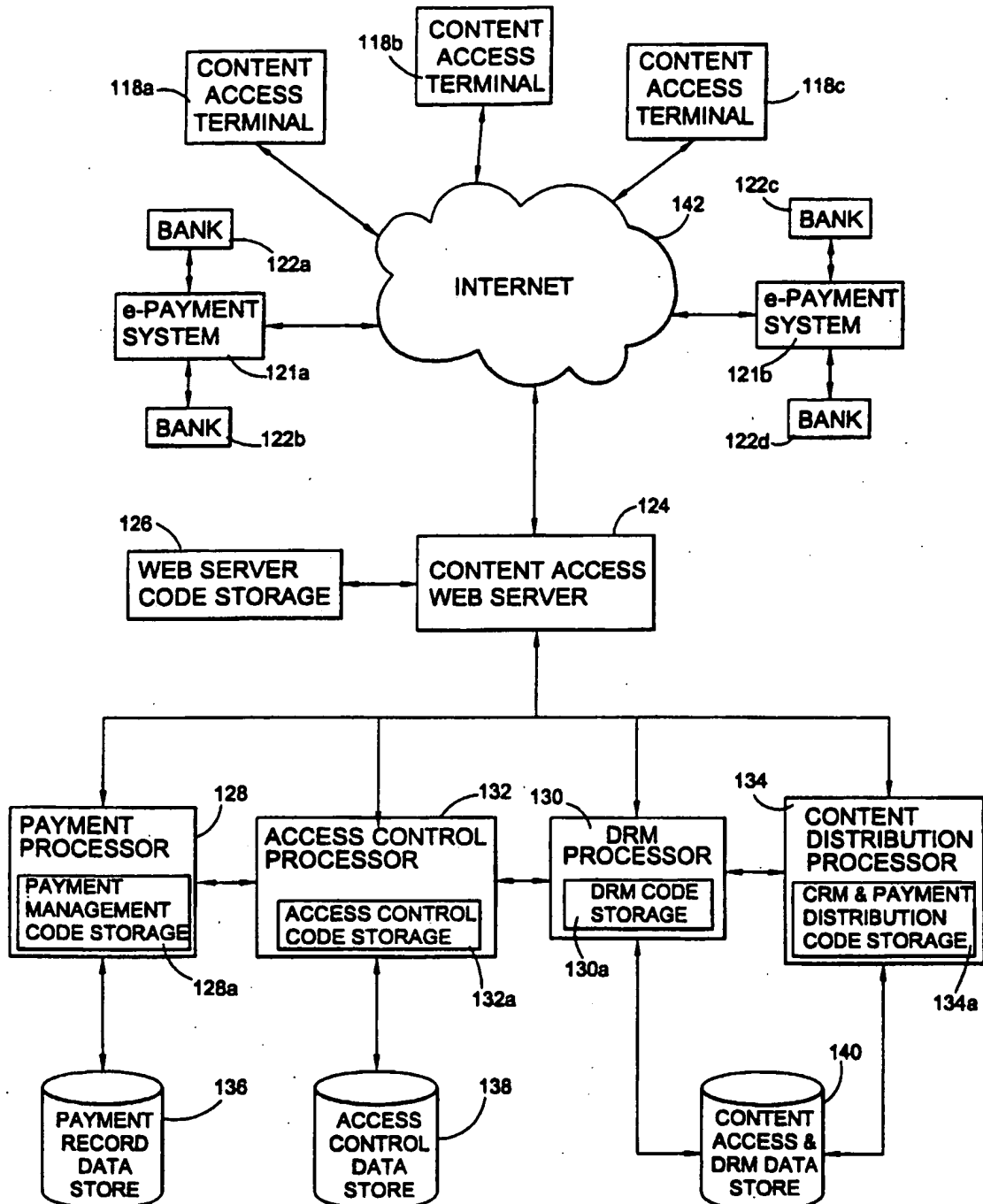


Fig.6

120

6/17

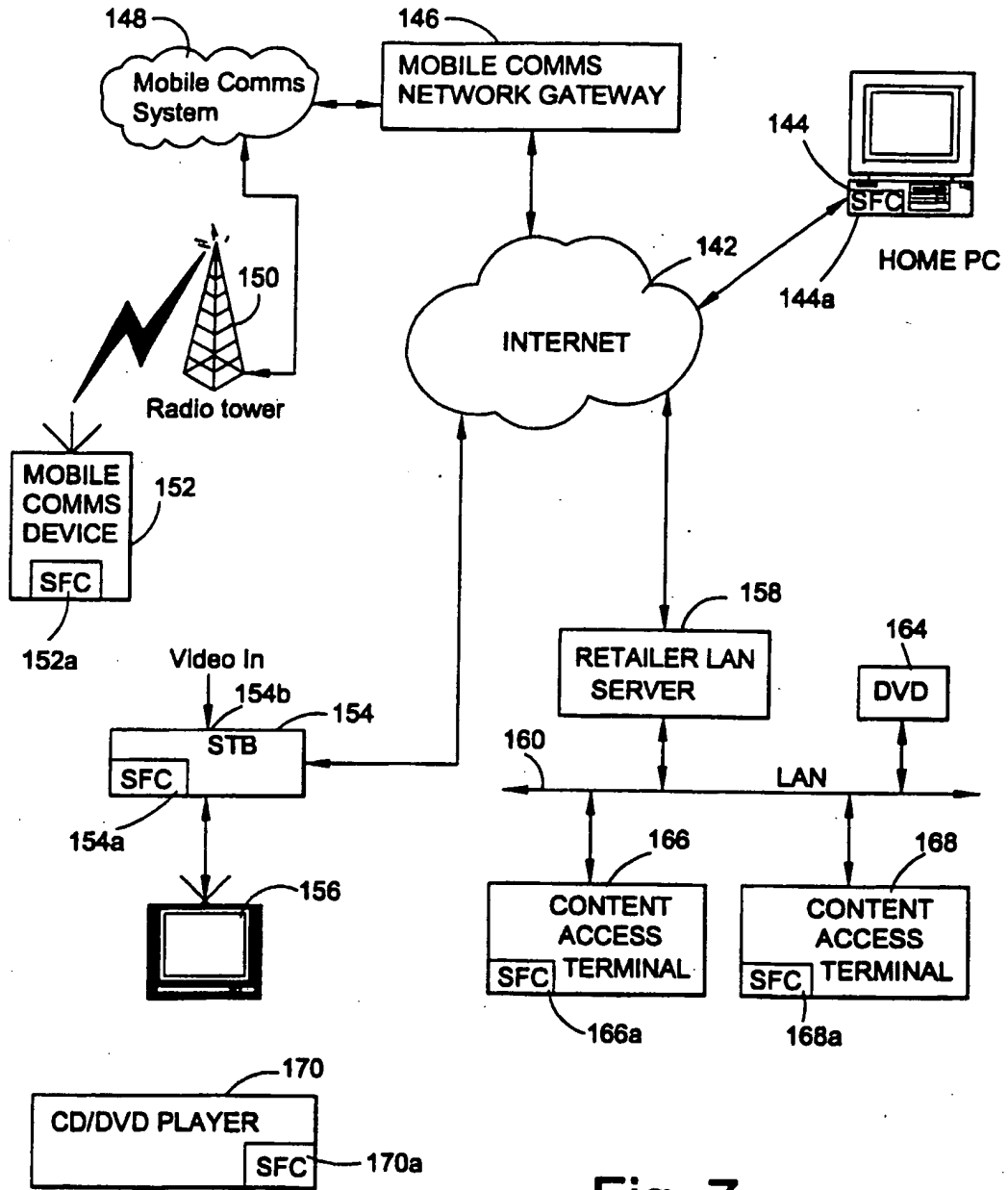


Fig. 7

7/17

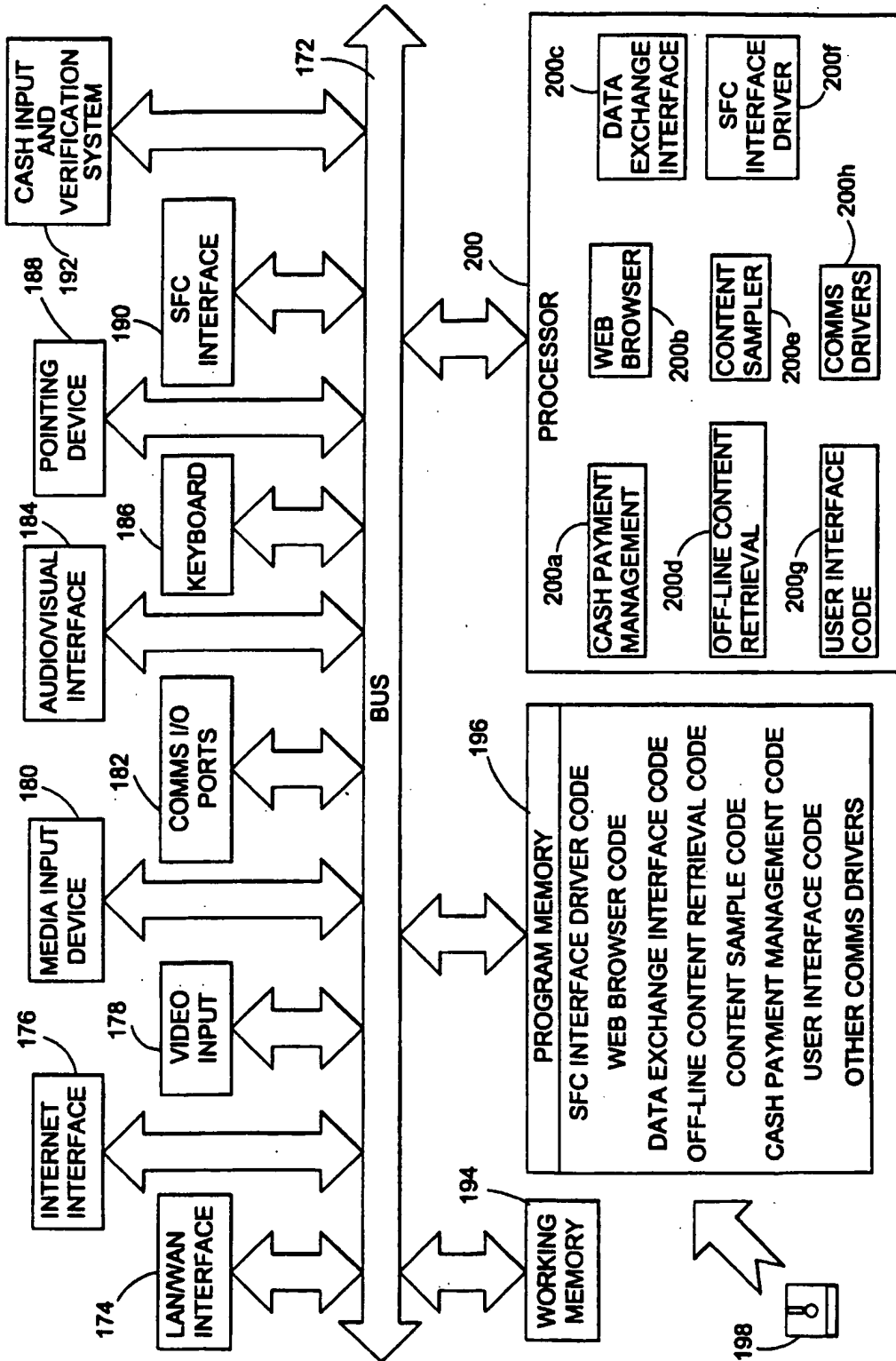


Fig. 8

8/17

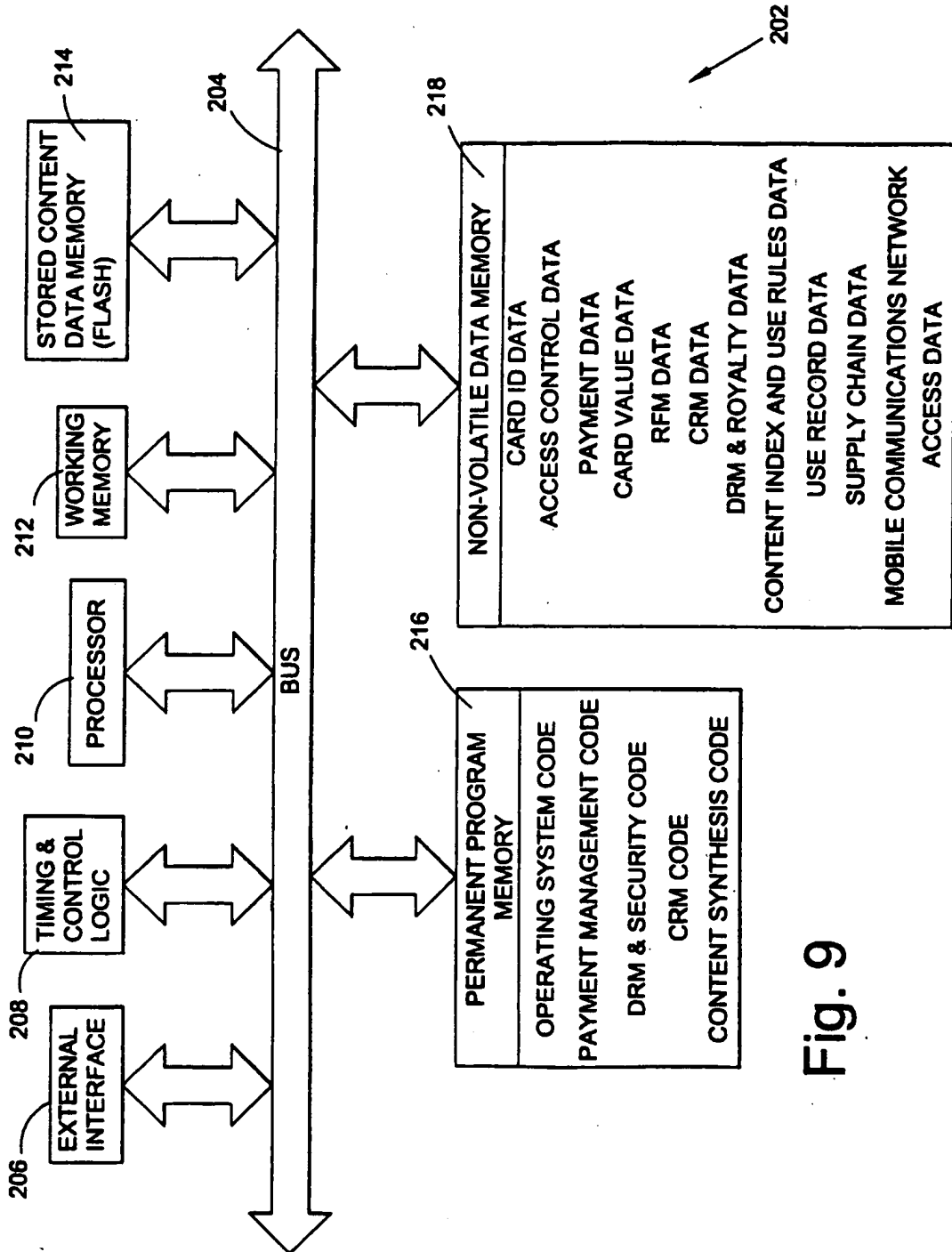


Fig. 9

9/17

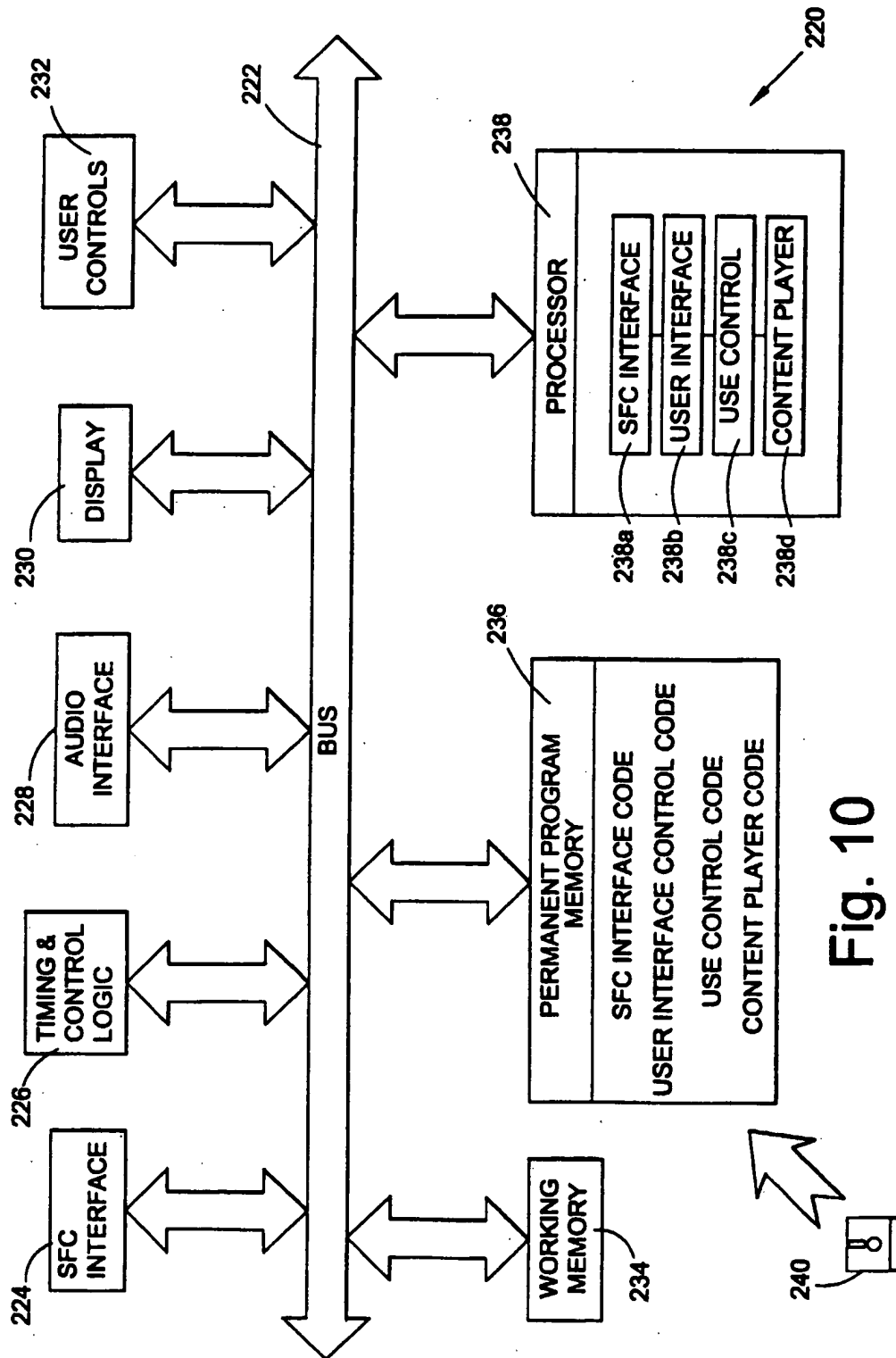


Fig. 10

10/17

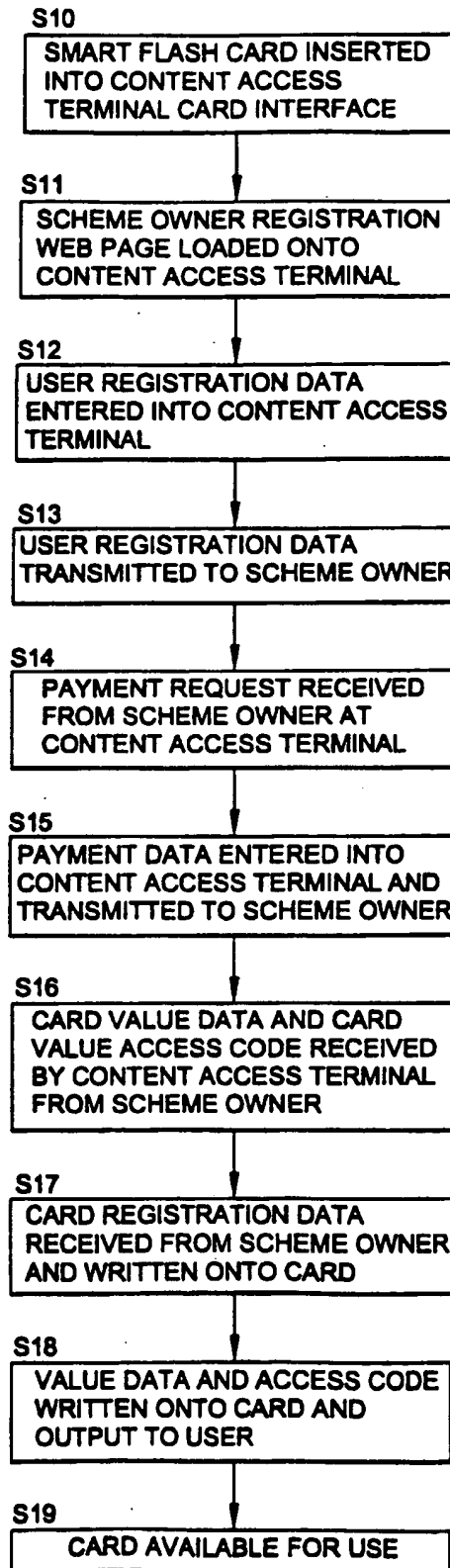


Fig11a

11/17

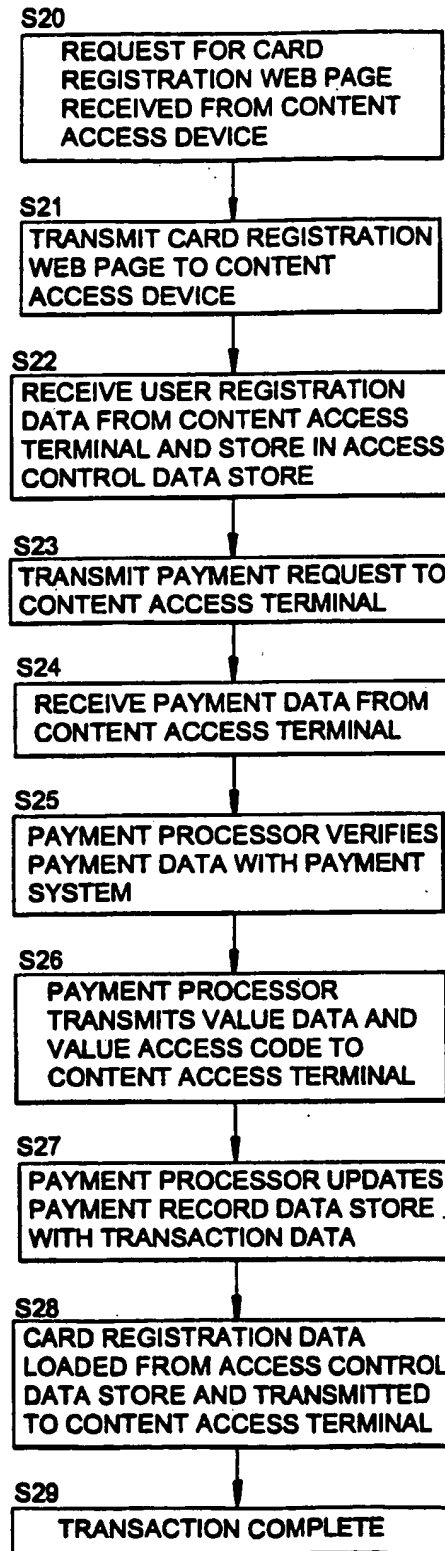


Fig.11b

12/17

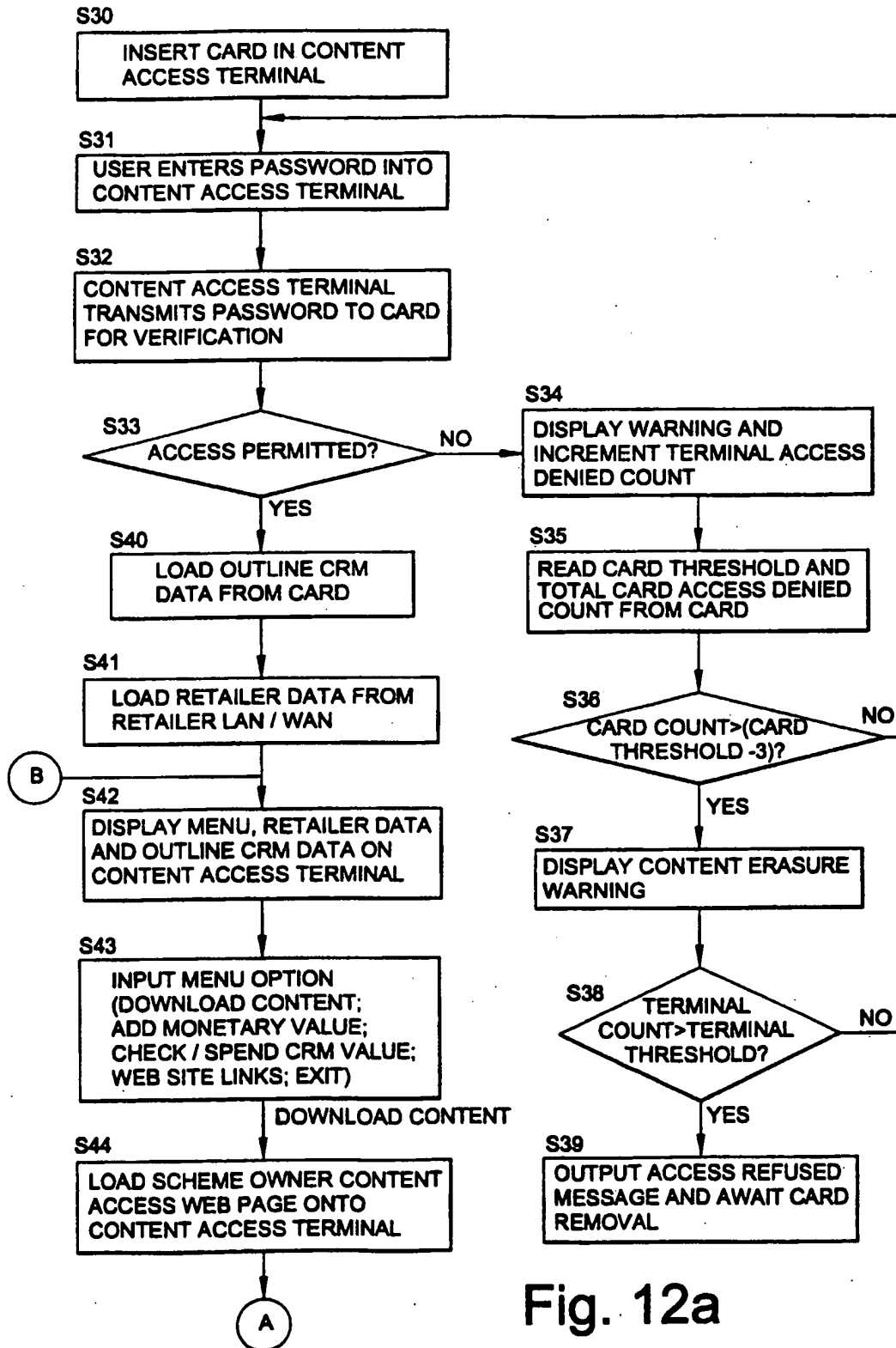


Fig. 12a

13/17

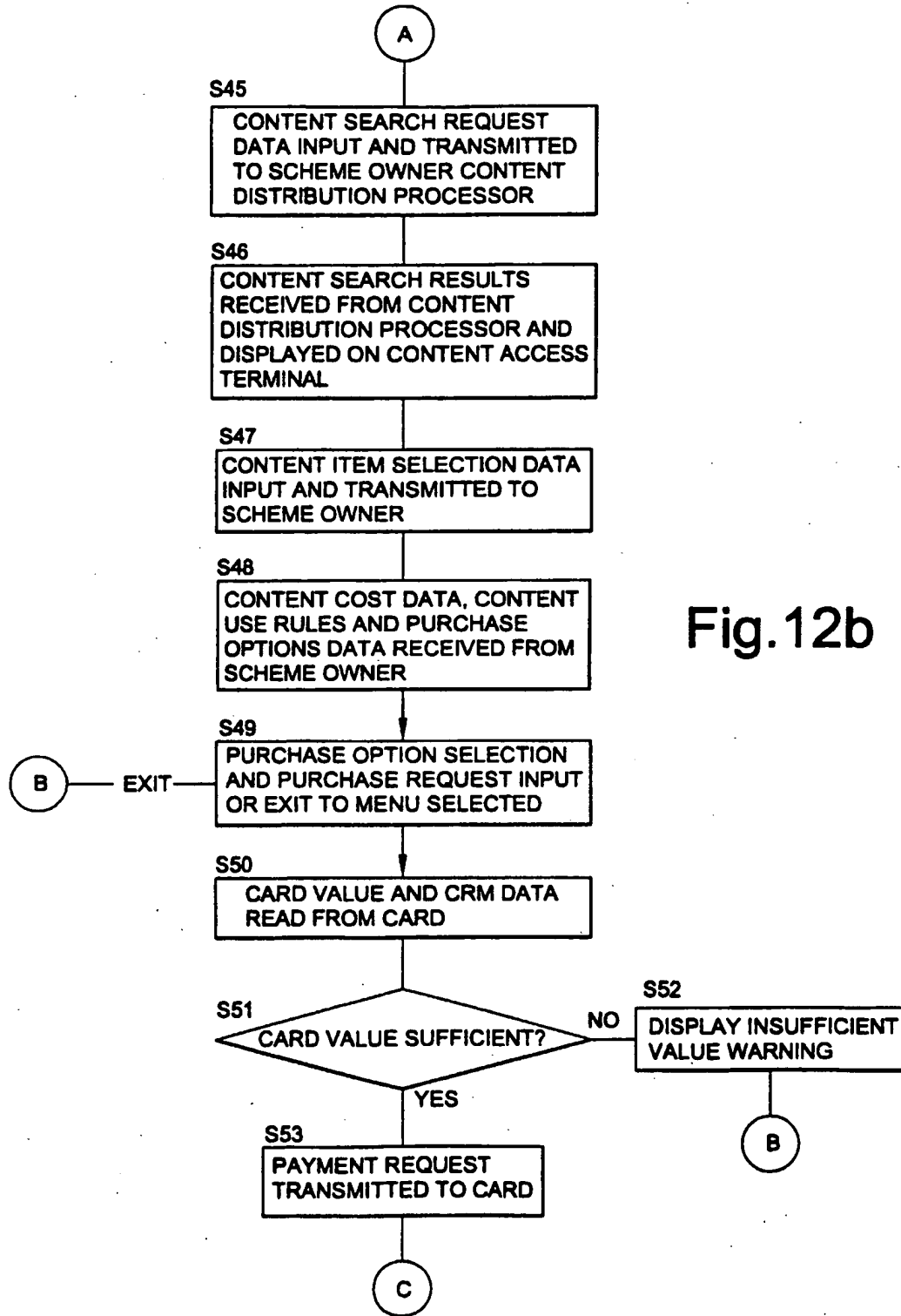


Fig.12b

14/17

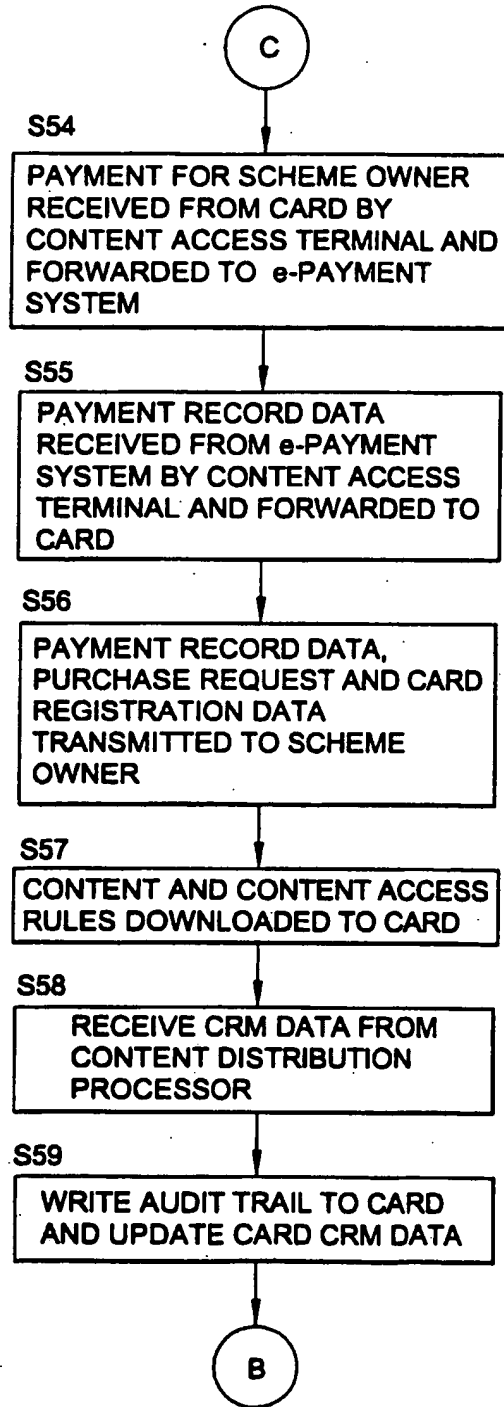


Fig.12c

15/17

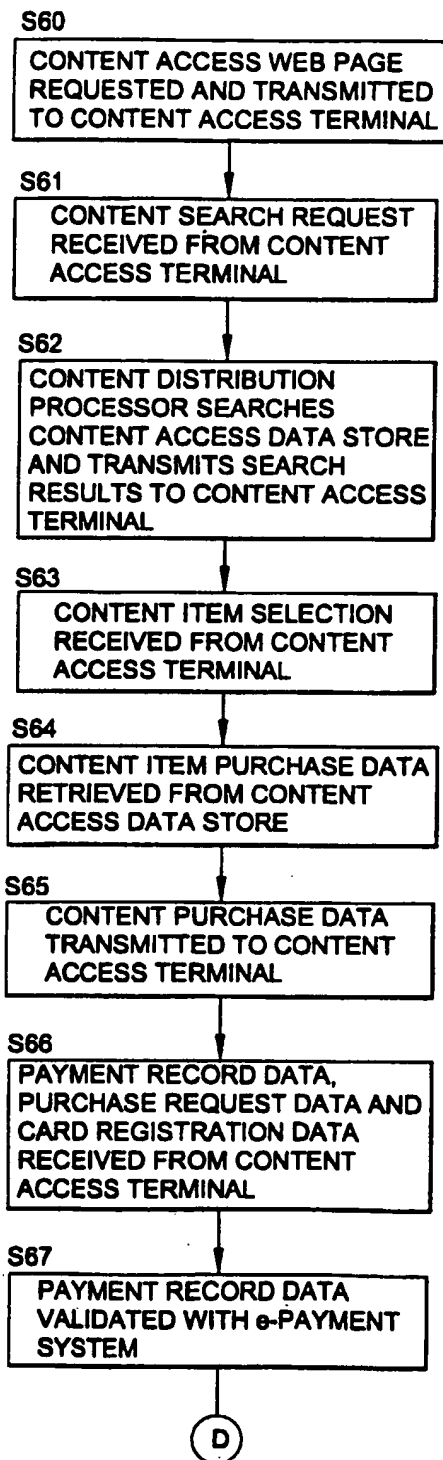


Fig. 12d

16/17

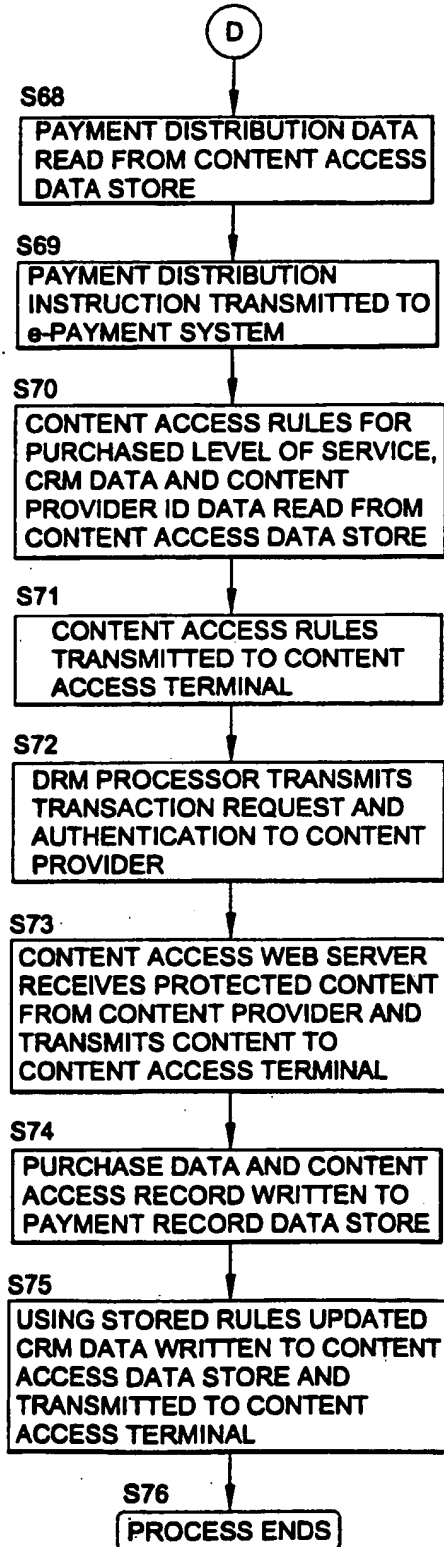


Fig. 12e

17/17

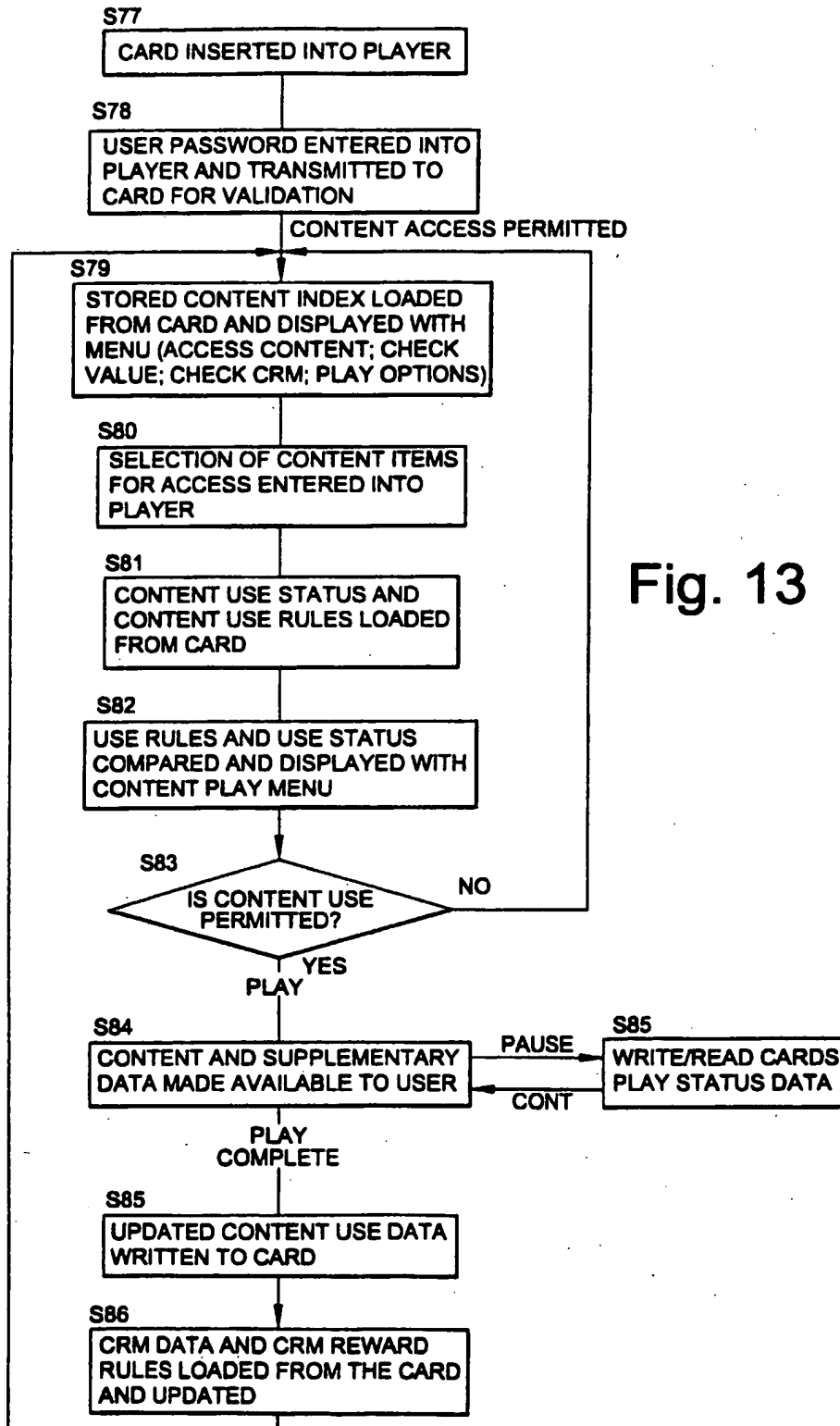


Fig. 13

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKewed/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

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 FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63) <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)	Attorney Docket Number		080379-000000US
	First Named Inventor		HULST, Hermen-ard
	COMPLETE IF KNOWN		
	Application Number	10/111,716	
	Filing Date	October 25, 2000	
	Art Unit		
Examiner Name			

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

(Title of the Invention)

the specification of which

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.

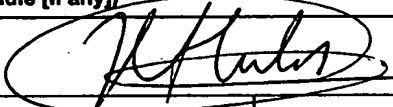
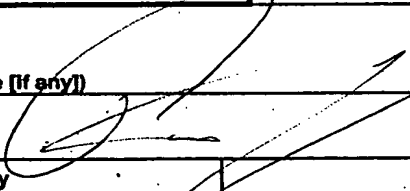
Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
9925227.2	Great Britain	10/25/1999	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>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

DECLARATION — Utility or Design Patent Application

Direct all correspondence to:		<input checked="" type="checkbox"/> Customer Number or Bar Code Label	20350	OR	<input type="checkbox"/> 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:		<input type="checkbox"/> 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 June 12 th 2002	
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:		<input type="checkbox"/> 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 12/5/02	
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
<input type="checkbox"/> Additional inventors are being named on the _____ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.					



080379-005 KTL

APRIL 21, 2003

PTAS
TOWNSEND AND TOWNSEND AND CREW LLP
KEVIN T. LEMOND
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CALIFORNIA 94111-3834

Under Secretary of Commerce For Intellectual Property and
Director of the United States Patent and Trademark Office
Washington, DC 20231
www.uspto.gov



102317843A

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, CG-4, 1213 JEFFERSON DAVIS HWY, SUITE 320, WASHINGTON, D.C. 20231.

RECORDATION DATE: 09/17/2002

REEL/FRAME: 013583/0554
NUMBER OF PAGES: 2

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:

HULST, HERMEN-ARD

DOC DATE: 06/12/2002

ASSIGNEE:

SMART-FLASH LIMITED
UPPER NORDENS, HIGH HURST WOOD
UCKFIELD, EAST SUSSEX, GREAT
BRITAIN
TN22 4AN

SERIAL NUMBER: 10111716
PATENT NUMBER:

FILING DATE: 09/17/2002
ISSUE DATE:

ALLYSON PURNELL, EXAMINER
ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS

BEST AVAILABLE COPY 0098

9/17/02

12-20-2002

U.S. Patent and Trademark Office
U.S. Department of Commerce
Docket No. 080379-000000US

Form PTO-1595
(Rev. 03-01)
OMB No. 0651-0027 (exp. 5/31/2002)



U.S. Department of Commerce
U.S. Patent and Trademark Office

Tab settings >>> 102317843

To the Honorable Commissioner of Patents and Trademarks. Please record the attached original documents or copy thereof

<p>1. Name of conveying party(ies): Hermen-Ard Hulst</p> <p>Additional name(s) of conveying parties attached? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No.</p>	<p>2. Name and address of receiving party(ies)</p> <p>Name: <u>Smart-Flash Limited</u></p> <p>Street Address: <u>Upper Nordens, High Hurst Wood</u></p> <p>City: <u>Uckfield, East Sussex</u> State: <u>Great Britain</u> Zip: <u>TN22 4AN</u></p> <p>Additional names and addresses attached? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>3. Nature of conveyance:</p> <p><input checked="" type="checkbox"/> Assignment <input type="checkbox"/> Merger</p> <p><input type="checkbox"/> Security Agreement <input type="checkbox"/> Change of Name</p> <p><input type="checkbox"/> Other: _____</p> <p>Execution Date: <u>June 12, 2002</u></p>	

4. Application number(s) or patent number(s).

If this document is being filed together with a new application, the execution date of the application is: _____

A. Patent Application No(s): 10/111,716

B. Patent No(s): _____

Additional numbers attached? Yes No

<p>5. Name and address of party to whom correspondence concerning document should be mailed:</p> <p>Name: Kevin T. LeMond TOWNSEND AND TOWNSEND AND CREW LLP Two Embarcadero Center, 8th Floor San Francisco, California 94111-3834 (415) 576-0200</p>	<p>6. Total number of applications and patents involved <u>1</u></p> <p>7. Total fee (37 CFR 3.41): _____ \$40.00</p> <p><input type="checkbox"/> Enclosed</p> <p><input checked="" type="checkbox"/> Authorized to be charged to deposit account</p> <p>8. Deposit account number: <u>20-1430</u></p> <p>(Attach duplicate copy of this page if paying by deposit account)</p>
---	---

09/23/2002 LLANDGRA 00000047 201430 10111716
03 FC:581 40.00 CH

DO NOT USE THIS SPACE

9. Statement and signature.

To the best of my knowledge and belief, the foregoing is true and correct and any attached copy is a true of copy of the original document.

Kevin T. LeMond
Name of Person Signing
Atty. Reg. No. 35,933

Signature

September 17, 2002
Date

Total number of pages including cover sheet, attachments and document 2
Mail documents to be recorded with required cover sheet information to:
Commissioner of Patents and Trademarks, Box Assignments
Washington, D.C. 20231

ASSIGNMENT OF PATENT APPLICATION

WHEREAS, Hermen-ard HULST, Van Tuyll van Serooskerkenweg 75hs, 1076 JG Amsterdam The Netherlands ~~Patrick Sandor RACZ, of 19 Royal Square, St. Helier, Jersey JE1 4WA, Great Britain~~, hereinafter referred to as "Assignors", are the inventors of the invention described and set forth in the below identified application for United States Letters Patent:

Title of the Invention: DATA STORAGE AND ACCESS SYSTEMS

Date(s) of execution: _____

Filing date: October 25, 2000 Serial No.: 10/111,716; and

WHEREAS, SMART-FLASH LIMITED, Upper Nordens, High Hurst Wood, Uckfield, East Sussex TN22 4AN, Great Britain, hereinafter referred to as "Assignee", is desirous of acquiring Assignors' interest in the said invention and application and in any U.S. Letters Patent which may be granted on the same;

NOW, THEREFORE, TO ALL WHOM IT MAY CONCERN: Be it known that, for good and valuable consideration, receipt of which is hereby acknowledged by Assignors, Assignors have sold, assigned and transferred, and by these presents do sell, assign and transfer unto the said Assignee, and Assignee's successors and assigns, all their right, title and interest in and to the said invention and application and all future improvements thereon, and in and to any Letters Patent which may hereafter be granted on the same in the United States, the said interest to be held and enjoyed by said Assignee as fully and exclusively as it would have been held and enjoyed by said Assignor had this Assignment and transfer not been made, to the full end and term of any Letters Patent which may be granted thereon, or of any division, renewal, continuation in whole or in part, substitution, conversion, reissue, prolongation or extension thereof.

Assignors further agree that they will, without charge to said Assignee, but at Assignee's expense, cooperate with Assignee in the prosecution of said application and/or applications, execute, verify, acknowledge and deliver all such further papers, including applications for Letters Patent and for the reissue thereof, and instruments of assignment and transfer thereof, and will perform such other acts as Assignee lawfully may request, to obtain or maintain Letters Patent for said invention and improvement, and to vest title thereto in said Assignee, or Assignee's successors and assigns.

IN TESTIMONY WHEREOF, Assignors have signed their names on the dates indicated.

Date: June 12th 2002



Hermen-ard HULST

Date: _____

~~Patrick Sandor RACZ~~

PATENT APPLICATION SERIAL NO _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

01/25/2006 MWOLDGE1 00000089 201430 11336758

01 FC:2011	150.00 DA
02 FC:2111	250.00 DA
03 FC:2311	100.00 DA
04 FC:2201	1100.00 DA
05 FC:2202	1350.00 DA

PTO-1556

(5/87)

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875 Effective December 8, 2004

Application or Docket Number

11336758

APPLICATION AS FILED - PART I

(Column 1)

(Column 2)

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

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(q), (p), or (r))	N/A	N/A
TOTAL CLAIMS (37 CFR 1.16(i))	74	minus 20 = 54
INDEPENDENT CLAIMS (37 CFR 1.16(h))	14	minus 3 = 11
APPLICATION SIZE FEE (37 CFR 1.16(s))	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).	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		

RATE (\$)	FEE (\$)
N/A	150.00
N/A	\$250
N/A	\$100
X\$ 25 =	1350
X100 =	1100
+180=	
TOTAL	2950

RATE (\$)	FEE (\$)
N/A	300.00
N/A	\$500
N/A	\$200
X\$50 =	
X200 =	
+360=	
TOTAL	

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

APPLICATION AS AMENDED - PART II

(Column 1)

(Column 2)

(Column 3)

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

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))		

RATE (\$)	ADDITIONAL FEE (\$)
X\$ 25 =	
X100 =	
+180=	
TOTAL ADD'L FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X\$50 =	
X200 =	
+360=	
TOTAL ADD'L FEE	

(Column 1)

(Column 2)

(Column 3)

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

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))		

RATE (\$)	ADDITIONAL FEE (\$)
X\$ 25 =	
X100 =	
+180=	
TOTAL ADD'L FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X\$50 =	
X200 =	
+360=	
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.

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. National Phase of:
PCT/GB/004110

HULST HERMEN-ARD

Application No.: Not yet assigned

Filed: Herewith

For: DATA STORAGE AND ACCESS SYSTEMS

PRELIMINARY AMENDMENT

San Francisco, CA 94111
April 25, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

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

PLEASE NOTE: The clauses numbered 1-27 beginning at page 44 are **not to be included as claims**, but as subject matter. The claims at issue begin on page 48 and are number 1-74.

IN THE CLAIMS:

Please substitute the following amended, clean versions of the indicated claims (a marked-up version of the changes to the claims is attached to this Amendment):

3. (amended) A method as claimed in claim 1 further comprising communicating a result of the payment information validating to the data supplier.

4. (amended) A method as claimed in claim 1 further comprising controlling access by the terminal to data from the data supplier using a control data processing system coupled to the Internet.

6. (amended) A method as claimed according to claim 1 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. (amended) A method as claimed in claim 1 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 characterizing a user spending pattern.

8. (amended) A method as claimed in claim 1 wherein said portable data storage device comprises an electronic memory card or smart card.

9. (amended) A method as claimed in claim 1 wherein the downloaded data comprises compressed audio and/or video data.

14. (amended) A portable data carrier as claimed in claim 11, 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.

16. (amended) A portable data carrier as claimed in claim 11, 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. (amended) A portable data carrier as claimed in claim 11 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. (amended) A portable data carrier as claimed in claim 10, 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. (amended) A portable data carrier as claimed in claim 10, 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. (amended) A portable data carrier as claimed in claim 10 wherein said data memory has a capacity of greater than 1 MByte, more preferably > 100 MBytes, and most preferably > 1 GByte.

21. (amended) A portable data carrier as claimed in claim 10 substantially configured as an IC card or smart card.

26. (amended) A computer system as claimed in claim 24, wherein said data access data store further comprises data item access rule data for output to the requester with said data item.

29. (amended) A computer system as claimed in claim 24, 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. (amended) A computer system as claimed in claim 24, further comprising content synthesis code to generate substantially complete item data from partial item data provided from two or more sources.

33. (amended) A method of providing data to a data requester as claimed in claim 32 further comprising:

transmitting data access rule data to requester with the read data.

37. (amended) A data access terminal as claimed in claim 35 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.

39. (amended) A data access terminal as claimed in claim 37 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. (amended) A data access terminal according to claim 35 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.

42. (amended) A data access terminal according to claim 35 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. (amended) A data access terminal according to claim 35 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 characterizing data from the data supplier;
code to retrieve supplementary data in response to said characterizing data; and
code to output the supplementary data.

44. (amended) A data access terminal according to claim 35 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. (amended) A data access terminal according to claim 35 integrated with a mobile communication device, a personal computer, an audio/video player, and/or a cable or satellite television interface device.

49. (amended) A method of providing data as claimed in claim 46, 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. (amended) A method of providing data as claimed in claim 48, 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.

53. (amended) A data access device as claimed in claim 51, 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.

55. (amended) A data access device as claimed in claim 53, further comprising code to retrieve and output supplementary data to the user.

56. (amended) A data access device according to claim 51 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. (amended) A data access device according to claim 51 wherein the device is portable and the data carrier interface is configured for interfacing with a removable data carrier.

58. (amended) A data access device according to claim 57 configured to interface with the data carrier of claim 10.

62. (amended) A method of controlling access according to claim 59, further comprising:

inputting a user access data;

selecting the use rules dependent upon the user access data.

65. (amended) A data access system according to claim 63 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.

73. (amended) A computer program to, when running, carry out the method of claim 1.

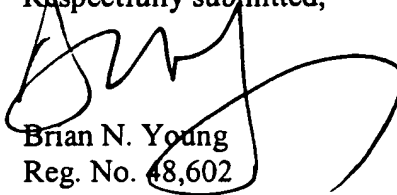
REMARKS:

Claims 1-74 are pending.

Amendment is made to eliminate all multiple dependencies from the claims, thereby avoiding the need to pay the multiple dependent surcharge.

Also attached on a separate page is an Abstract of the Disclosure.

Respectfully submitted,



Brian N. Young
Reg. No. 48,602

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: (415) 576-0200
Fax: (415) 576-0300
KTL/BNY/dxm

SF 1340261 v1

MARKED-UP VERSION OF THE CHANGES TO THE CLAIMS

3. (amended) A method as claimed in [claim 1 or 2] claim 1 further comprising communicating a result of the payment information validating to the data supplier.
4. (amended) A method as claimed in [any one of claims 1 to 3] claim 1 further comprising controlling access by the terminal to data from the data supplier using a control data processing system coupled to the Internet.
6. (amended) A method as claimed according to [any one of claims 1 to 5] claim 1 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. (amended) A method as claimed in [claims 1 to 6] claim 1 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 characterizing a user spending pattern.
8. (amended) A method as claimed in [claims 1 to 7] claim 1 wherein said portable data storage device comprises an electronic memory card or smart card.
9. (amended) A method as claimed in [any one of claims 1 to 8] claim 1 wherein the downloaded data comprises compressed audio and/or video data.
14. (amended) A portable data carrier as claimed in [claim 11, 12 or 13] claim 11, 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.

16. (amended) A portable data carrier as claimed in [any one of claims 11 to 15] claim 11, 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. (amended) A portable data carrier as claimed in [any one of claims 11 to 16] claim 11 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. (amended) A portable data carrier as claimed in [any one of claims 10 to 17] claim 10, 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. (amended) A portable data carrier as claimed in [any one of claims 10 to 18] claim 10, 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. (amended) A portable data carrier as claimed in [any one of claims 10 to 19] claim 10 wherein said data memory has a capacity of greater than 1 MByte, more preferably > 100 MBytes, and most preferably > 1 GByte.

21. (amended) A portable data carrier as claimed in [any one of claims 10 to 20] claim 10 substantially configured as an IC card or smart card.

26. (amended) A computer system as claimed in [claim 24 or 25] claim 24, wherein said data access data store further comprises data item access rule data for output to the requester with said data item.

29. (amended) A computer system as claimed in [any one of claims 24 to 28] claim 24, 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. (amended) A computer system as claimed in [any one of claims 24 to 29] claim 24, further comprising content synthesis code to generate substantially complete item data from partial item data provided from two or more sources.

33. (amended) A method of providing data to a data requester as claimed in [claim 31 or 32] claim 32 further comprising:

transmitting data access rule data to requester with the read data.

37. (amended) A data access terminal as claimed in [claim 35 or 36] claim 35 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.

39. (amended) A data access terminal as claimed in [claim 37 or 38] claim 37 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. (amended) A data access terminal according to [any one of claims 35 to 39] claim 35 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.

42. (amended) A data access terminal according to [any one of claims 35 to 41] claim 35 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. (amended) A data access terminal according to [any one of claims 35 to 42] claim 35 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 characterizing data from the data supplier;
- code to retrieve supplementary data in response to said characterizing data; and
- code to output the supplementary data.

44. (amended) A data access terminal according to [any one of claims 35 to 43] claim 35 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. (amended) A data access terminal according to [any one of claims 35 to 44] claim 35 integrated with a mobile communication device, a personal computer, an audio/video player, and/or a cable or satellite television interface device.

49. (amended) A method of providing data as claimed in [claim 46, 47 or 48] claim 46, 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. (amended) A method of providing data as claimed in [claim 48 or 49] claim 48, 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.

53. (amended) A data access device as claimed in [claim 51 or 52] claim 51, 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.

55. (amended) A data access device as claimed in [claim 53 or 54] claim 53, further comprising code to retrieve and output supplementary data to the user.

56. (amended) A data access device according to [any one of claims 51 to 55] claim 51 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. (amended) A data access device according to [any one of claims 51 to 56] claim 51 wherein the device is portable and the data carrier interface is configured for interfacing with a removable data carrier.

58. (amended) A data access device according to claim 57 configured to interface with the data carrier of [any one of claims 10 to 21] claim 10.

62. (amended) A method of controlling access according to [any one of claims 59 to 61] claim 59, further comprising:
inputting a user access data;
selecting the use rules dependent upon the user access data.

65. (amended) A data access system according to [claim 63 or 64] claim 63 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.

73. (amended) A computer program to, when running, carry out the method of [any preceding method claim] claim 1.

(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).

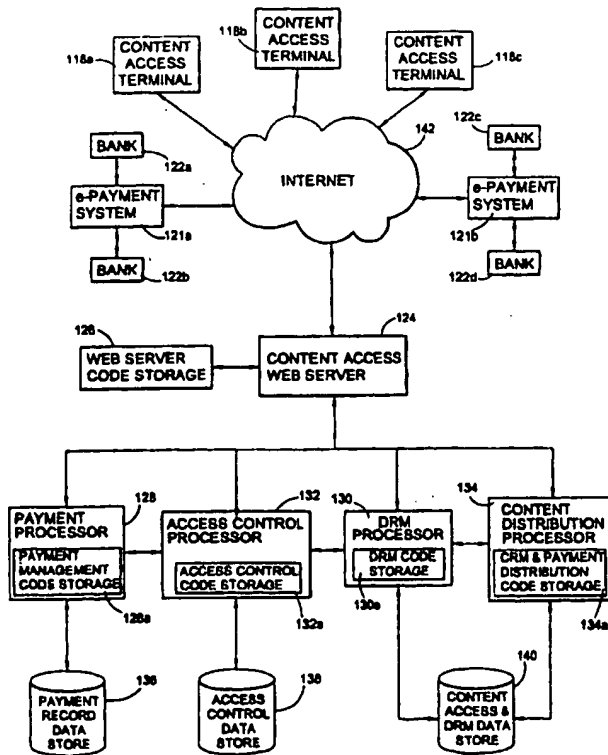
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

(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.*

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

Application Data Sheet

Application Information

Application number::
Filing Date:: 01/19/06
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:: 080379-000100US
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:: 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 Serooskerkerweg 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

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:: St. Heller
State or Province of Residence::
Country of Residence:: Jersey
Street of Mailing Address:: 19 Royal Square
City of Mailing Address:: St. Heller
State or Province of mailing address::

Country of mailing address:: Jersey
Postal or Zip Code of mailing address:: JE1 4WA

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	Continuation of	10/111,716	09/17/02

Foreign Priority Information

Country::	Application number::	Filing Date::
PCT	GB00/04110	10/25/00
United Kingdom	9925227.2	11/25/99

Assignee Information

Assignee Name:: Smart-Flash Limited
Street of mailing address:: Upper Nordens, High Hurst Wood
City of mailing address:: Uckfield
State or Province of mailing address:: East Sussex
Country of mailing address:: Great Britain
Postal or Zip Code of mailing address:: TN22 4AN

"Express Mail" Label No. EV 383391336 US
Date of Deposit January 19, 2006

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to:

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

By: _____

Dana Kane

PATENT

Attorney Docket No.: 080379-000100US

Client Reference No.: F/USP81421X

Con.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Hermen-ard HULST and Patrick
Sandor RACZ

Application No.:

Filed: January 19, 2006

For: DATA STORAGE AND ACCESS
SYSTEMS

Examiner:

Art Unit:

INFORMATION DISCLOSURE
STATEMENT UNDER 37 CFR §1.97 and
§1.98

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

Sir:

The references cited on attached form PTO/SB/08A and PTO/SB/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 Application No. 09/697,534, filed October 25, 2000 (Attorney Docket No. 080528-000000US) and in parent application 10/111,716, filed September 17, 2000 (Attorney Docket No. 080379-000000US). Copies of the Information Disclosure Statement filed with parent application 10/111,716 on April 25, 2002 and the Supplemental Information Disclosure Statement filed therein on January 16, 2004.

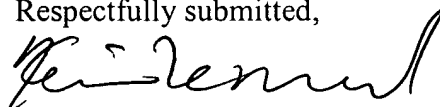
It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

Also enclosed is a copy of the Search/Examination report corresponding to the priority PCT application GB00/04110.

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 a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,



Kevin T. LeMond
Reg. No. 35,933

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
KTL:dk
60682925 v1

I hereby certify that this correspondence being deposited with the United States Postal Service as first class mail in an envelope addressed to:

PATENT
Attorney Docket No.: 080379-000000US
Client Reference No.: F/USP81421X

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

On January 16, 2004

TOWNSEND and TOWNSEND and CREW LLP

By: Mark T. Davis

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

HULST HERMEN-ARD

Application No.: 10/111,716

Filed: September 17, 2002

For: DATA STORAGE AND ACCESS
SYSTEMS

Examiner: Paik, Steve S.

Art Unit: 2876

SUPPLEMENTAL INFORMATION
DISCLOSURE STATEMENT UNDER 37
CFR §1.97 and §1.98

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

Sir:

The references cited on attached form PTO/SB/08A 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 Application No. 09/697,534, filed October 25, 2000 (Attorney Docket No. 080528-000000US). 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.

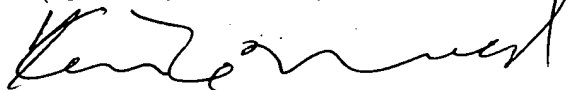
As provided for by 37 CFR 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

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 a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,



Kevin T. LeMond
Reg. No. 35,933

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
KTL:mtd
60113553 v1

Substitute for form 1449A/PTO		Complete If Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Application Number	10/111,716
		Filing Date	September 17, 2002
		First Named Inventor	Hulst, Hermen-Ard
		Art Unit	2876
		Examiner Name	Paik, Steve S.
Sheet 1 of		Attorney Docket Number	080379-000000US

U.S. PATENT DOCUMENTS+						
Examiner Initials*	Cite No. ¹	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 ² (if known)			
	AA	US 5,226,145		07/08/1993	Moronaga et al.	
	AB	US 5,367,150		11/22/1994	Kitta et al.	
	AC	US 5,457,746		10/10/1995	Dolphin	
	AD	US 5,588,146		12/24/1996	Leroux	
	AE	US 5,677,953		10/14/1997	Dolphin	
	AF	US 5,703,951		12/30/1997	Dolphin	
	AG	US 5,754,654		05/19/1998	Hiroya et al.	
	AH	US 5,794,202		08/11/1998	Kim	
	AI	US 5,809,241		09/15/1998	Hanel et al.	
	AJ	US 5,847,372		12/08/1998	Kreft	
	AK	US 5,889,860		03/30/1999	Eller et al.	
	AL	US 5,901,330		11/04/1999	Sun et al.	
	AM	US 5,918,213		06/29/1999	Bernard et al.	
	AN	US 5,923,884		07/13/1999	Peyret et al.	
	AO	US 6,012,634		01/11/2000	Brogan et al.	
	AP	US 6,078,917		06/20/2000	Paulsen et al.	
	AQ	US 6,119,945		09/19/2000	Muller et al.	
	AR	US-6,202,056		03/13/2001	Nuttall	
	AS	US-6,385,731		05/07/2002	Ananda	
	AT	US 6,424,975		07/23/2002	Walter et al.	
	AU	US 6,442,570		08/27/2002	Wu	
	AV	US 6,473,829		10/29/2002	Dahman et al.	
	AW	US 6,510,236		01/21/2003	Crane et al.	
	AX	US-6,553,413		04/22/2003	Leighton et al.	
	AY	US-6,574,643		06/03/2003	Walter et al.	

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No. ¹	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 ⁶
		Country Code ³	Number ⁴	Kind Code ⁵ (if known)				
	AZ	WO	98/19237		05/07/1998		<input type="checkbox"/>	
	BA	WO	98/33343		07/30/1998		<input type="checkbox"/>	
	BB	WO	98/37526		08/27/1998		<input type="checkbox"/>	
	BC	EP	0195098		10/03/1990		<input type="checkbox"/>	
	BD	EP	0713198		05/22/1996		<input type="checkbox"/>	
	BE	EP	0823694		02/11/1998		<input type="checkbox"/>	
	BF	EP	0542298		04/22/1998		<input type="checkbox"/>	
	BG	EP	0843449		05/07/1998		<input type="checkbox"/>	
	BH	EP	0914001		05/06/1999		<input type="checkbox"/>	

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. ¹ Applicant's unique citation designation number (optional). ² Kind Codes of U.S. Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

HULST HERMEN-ARD

Application No.:

Filed: Herewith

For: DATA STORAGE AND ACCESS
SYSTEMS

Examiner: Unassigned

Art Unit: Unassigned

INFORMATION DISCLOSURE
STATEMENT UNDER 37 CFR §1.97 and
§1.98

San Francisco, CA 94111
April 25, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

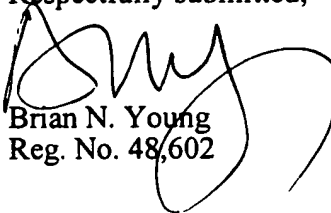
Sir:

The references cited on attached form PTO/SB/08A and PTO/SB/08B are being called to the attention of the Examiner. Copies of the references are 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 no fee is required for submission of this statement, since it is being submitted prior to the first Office Action. However, if a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,



Brian N. Young
Reg. No. 48,602

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
KTL/BNY/dxm

SF 1340359 v1

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No. ¹	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 ²
		Country Code ³	Number ⁴	Kind Code ⁵ (if known)				
	AA	EP	0713198	A2	05/22/1998			
	AB	EP	0823694	A1	02/11/1998			
	AC	EP	0843449	A2	05/20/1998			
	AD	EP	0914001	A1	05/06/1999			
	AE	WIPO	WO 98/19237	A1	05/07/1998			
	AF							
	AG							
	AH							

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.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 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.
 SF 1340359 v1

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11,336,758
---	---

APPLICATION AS FILED – PART I		
	(Column 1)	(Column 2)
FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(a), (b), or (c))		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		
TOTAL CLAIMS (37 CFR 1.16(i))	74	minus 20 = 54
INDEPENDENT CLAIMS (37 CFR 1.16(h))	16	minus 3 = * 13
APPLICATION SIZE FEE (37 CFR 1.16(s))	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	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		

SMALL ENTITY	
RATE (\$)	FEE (\$)
	150
	250
	100
X\$ 25	1350
X\$100	1300
180	3150
TOTAL	

OTHER THAN SMALL ENTITY	
RATE (\$)	FEE (\$)
	300
	500
	200
X\$50	
X\$200	
360	
TOTAL	

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

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 =	
180	
TOTAL	
ADD'T FEE	

OTHER THAN SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
360	
TOTAL	
ADD'T FEE	

AMENDMENT 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 =	
N/A	
TOTAL	
ADD'T FEE	

OTHER THAN SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
N/A	
TOTAL	
ADD'T 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.

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.

BEST AVAILABLE COPY

PATENT APPLICATION SERIAL NO 11.336.758

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

01/25/2006 MWOLDGE1 00000089 201430 11336758

01 FC:2011	150.00 DA
02 FC:2111	250.00 DA
03 FC:2311	100.00 DA
04 FC:2201	1100.00 DA
05 FC:2202	1350.00 DA

03/02/2006 CV0111 00000001 201430 11336758

01 FC:2201	200.00 DA
------------	-----------

PTO-1556

(5/87)



UNITED STATES PATENT AND TRADEMARK OFFICE

den

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.
11/336,758	01/19/2006	Hermen-ard Hulst	080379-000100US	3911

20350 7590 08/29/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

PAIK, STEVE S

ART UNIT PAPER NUMBER

2876

DATE MAILED: 08/29/2006

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

Office Action Summary

Application No. 11/336,758	Applicant(s) HULST ET AL.	
Examiner Steven S. Paik	Art Unit 2876	

-- 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 1 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 19 January 2006.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) 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

- 4) Claim(s) 1-74 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) _____ is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) 1-74 are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ 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).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1/19/06.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
 - I. Claims 1-9, drawn to a method of providing portable data, classified in class 235, subclass 487.
 - II. Claims 10-21, 51-58, 67, and 68 drawn to a portable data carrier, classified in class 23, subclass 379.
 - III. Claims 22, 23, 35-50, and 59-62 drawn to a method and an apparatus of controlling access to data, classified in class 235, subclass 382.
 - IV. Claims 24-34, 63-66, and 69-74 drawn to a system controlled by data bearing records, classified in class 235, subclass 375.

2. The inventions are distinct, each from the other because of the following reasons:

Inventions Group I - Group IV are related as product and process of use. The inventions can be shown to be distinct if either or both of the following can be shown: (1) the process for using the product as claimed can be practiced with another materially different product or (2) the product as claimed can be used in a materially different process of using that product (MPEP § 806.05(h)). In the instant case the process for using the product claimed can be practiced with materially different product.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Groups II, III, or IV restriction for examination purposes as indicated is proper.

3. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a petition under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steven S. Paik whose telephone number is 571-272-2404. The examiner can normally be reached on Monday - Friday 5:30a-2:00p (Maxi-Flex*).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 571-272-2398. 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

Application/Control Number: 11/336,758

Page 4

Art Unit: 2876

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.


Steven S. Paik
Primary Examiner
Art Unit 2876

ssp

1/19/06

Substitute for form 1449A/PTO		Complete If Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>		Application Number	48441,710 <i>11/336,758</i>
		Filing Date	September 17, 2002
		First Named Inventor	Hulst, Hermen-Ard
		Art Unit	2876
		Examiner Name	Paik, Steve S.
		Attorney Docket Number	080379-000000US <i>080379-000100US</i>
Sheet	1	of	2

U.S. PATENT DOCUMENTS+						
Examiner Initials*	Cite No. ¹	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 ² (if known)			
SSP	AA	US 5,226,145		07/08/1993	Moronaga et al.	
	AB	US 5,367,150		11/22/1994	Kitta et al.	
	AC	US 5,457,746		10/10/1995	Dolphin	
	AD	US 5,588,146		12/24/1996	Leroux	
	AE	US 5,677,953		10/14/1997	Dolphin	
	AF	US 5,703,951		12/30/1997	Dolphin	
	AG	US 5,754,854		05/18/1998	Hiroya et al.	
	AH	US 5,794,202		08/11/1998	Kim	
	AI	US 5,809,241		09/15/1998	Hanel et al.	
	AJ	US 5,847,372		12/08/1998	Kreft	
	AK	US 5,889,860		03/30/1999	Eller et al.	
	AL	US 5,901,330		11/04/1999	Sun et al.	
	AM	US 5,918,213		08/29/1999	Bernard et al.	
	AN	US 5,923,884		07/13/1999	Peyret et al.	
	AO	US 6,012,634		01/11/2000	Brogan et al.	
	AP	US 6,078,917		08/20/2000	Pautsen et al.	
	AQ	US 6,119,945		09/19/2000	Muller et al.	
	AR	US-6,202,056		03/13/2001	Nuttall	
	AS	US-6,385,731		05/07/2002	Ananda	
	AT	US 6,424,975		07/23/2002	Walter et al.	
	AU	US 6,442,570		08/27/2002	Wu	
	AV	US 6,473,829		10/29/2002	Dahman et al.	
	AW	US 6,510,236		01/21/2003	Crane et al.	
	AX	US-6,553,413		04/22/2003	Leighton et al.	
SSP	AY	US-6,574,843		06/03/2003	Walter et al.	

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No. ¹	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 ⁶
		Country Code ³	Number ⁴	Kind Code ⁵ (if known)				
SSP	AZ	WO	98/19237		05/07/1998		<input type="checkbox"/>	
	BA	WO	98/33343		07/30/1998		<input type="checkbox"/>	
	BB	WO	98/37526		08/27/1998		<input type="checkbox"/>	
	BC	EP	0195098		10/03/1990		<input type="checkbox"/>	
	BD	EP	0713198		05/22/1996		<input type="checkbox"/>	
	BE	EP	0823694		02/11/1998		<input type="checkbox"/>	
	BF	EP	0542298		04/22/1998		<input type="checkbox"/>	
	BG	EP	0843449		05/07/1998		<input type="checkbox"/>	
SSP	BH	EP	0914001		05/06/1999		<input type="checkbox"/>	

Examiner Signature	/Steven Paik/	Date Considered	08/22/2006
--------------------	---------------	-----------------	------------

*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. ¹ Applicant's unique citation designation number (optional). ² Kind Codes of U.S. Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.
60113553 v1

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No. ¹	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 ²
		Country Code ³	Number ⁴	Kind Code ⁵ (if known)				
SSP ↓	AA	EP	0713198	A2	05/22/1998			
	AB	EP	0823694	A1	02/11/1998			
	AC	EP	0843449	A2	05/20/1998			
	AD	EP	0914001	A1	05/08/1999			
SSP	AE	WIPO	WO 98/19237	A1	05/07/1998			
	AF							
	AG							
	AH							

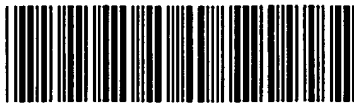
Examiner Signature	/Steven Paik/	Date Considered	08/22/2006
--------------------	---------------	-----------------	------------

*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.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 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.
 SF 1340359 v1

Index of Claims



Application/Control No.

11/336,758

Examiner

Steven S. Paik

Applicant(s)/Patent under Reexamination

HULST ET AL.

Art Unit

2876

√	Rejected
=	Allowed

-	(Through numeral) Cancelled
+	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date	
Final	Original		
	8/22/06		
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			

Claim		Date	
Final	Original		
	8/22/06		
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			
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			

Claim		Date	
Final	Original		
101			
102			
103			
104			
105			
106			
107			
108			
109			
110			
111			
112			
113			
114			
115			
116			
117			
118			
119			
120			
121			
122			
123			
124			
125			
126			
127			
128			
129			
130			
131			
132			
133			
134			
135			
136			
137			
138			
139			
140			
141			
142			
143			
144			
145			
146			
147			
148			
149			
150			



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. 3911

SERIAL NUMBER 11/336,758	FILING OR 371 (c) DATE 01/19/2006 RULE	CLASS 235	GROUP ART UNIT 2876	ATTORNEY DOCKET NO. 080379-000100US
------------------------------------	--	---------------------	-------------------------------	---

APPLICANTS

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

**** CONTINUING DATA *******

This application is a CON of 10/111,716 09/17/2002 which is a 371 of PCT/GB00/04110 10/25/2000

SSP
verified

**** FOREIGN APPLICATIONS *******

UNITED KINGDOM 9925227.2 11/25/1999

SSP
verified

IF REQUIRED, FOREIGN FILING LICENSE

**** SMALL ENTITY ****

GRANTED ** 03/01/2006

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 Verified and Acknowledged Examiner's Signature <i>[Signature]</i> Initials <i>SSP</i>	STATE OR COUNTRY NETHERLANDS	SHEETS DRAWING 17	TOTAL CLAIMS 74	INDEPENDENT CLAIMS 16
---	--	-----------------------------	---------------------------	---------------------------------

ADDRESS

20350

TITLE

Data storage and access systems

FILING FEE RECEIVED 3150	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

RECEIVED
CENTRAL FAX CENTER

SEP 29 2006

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office, Fax No. 1-571-273-8300 on September 29, 2006.

PATENT
Attorney Docket No.: 080379-000100US
Client Ref. No.: F/USP81421X Con.

TOWNSEND and TOWNSEND and CREW LLP

By: Musta M. Munnac

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

HULST HERMEN-ARD

Application No.: 11/336,758

Filed: January 19, 2006

For: DATA STORAGE AND ACCESS SYSTEMS

Customer No.: 20350

Confirmation No. 3911

Examiner: Steve S. Paik

Technology Center/Art Unit: 2876

RESPONSE TO RESTRICTION REQUIREMENT

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

Sir:

In response to the Office Action mailed August 29, 2006, 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 6 of this paper.

RECEIVED
CENTRAL FAX CENTER

SEP 29 2006

Atty Docket No. 080379-000100U

PTO FAX NO.: 1-571-273-8300

ATTENTION: Examiner Steve S. Paik

Group Art Unit 2876

**OFFICIAL COMMUNICATION
FOR THE PERSONAL ATTENTION OF
EXAMINER STEVE S. PAIK**

CERTIFICATION OF FACSIMILE TRANSMISSION

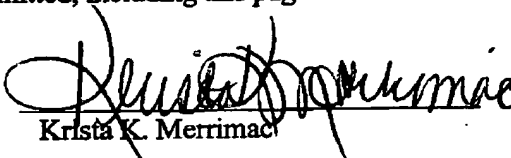
I hereby certify that the following documents in re Application of Herman-ard HULST, Application No. 11/366,758, filed January 19, 2006 for DATA STORAGE AND ACCESS SYSTEMS are being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Documents Attached

- 1. SB/21 Transmittal Form (1 page)
- 2. Response to Restriction Requirement (8 pages)
- 3. Substitute Specification (37 pages)
- 4. Comparison Copy of Substitute Specification (42 pages)

Number of pages being transmitted, including this page: 88

Dated: September 29, 2006



Krista K. Merrimac

**PLEASE CONFIRM RECEIPT OF THIS PAPER BY
RETURN FACSIMILE AT (415) 576-0300**

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, CA 94111-3834
Telephone: 415-576-0200
Fax: 415-576-0300
3994

60881163 v1

RECEIVED
CENTRAL FAX CENTER

002/089

SEP 29 2006 PTO/SB/21 (07-38)

TRANSMITTAL FORM <small>(to be used for all correspondence after initial filing)</small>	Application Number	11/336,758	
	Filing Date	January 19, 2006	
	First Named Inventor	Hulst, Herman-ard	
	Art Unit	2876	
	Examiner Name	PAJK, Steve S.	
Total Number of Pages in This Submission	88	Attorney Docket Number	080379-000100US

ENCLOSURES (Check all that apply)		
<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to T
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input checked="" type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Terminal Disclaimer	<input checked="" type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Request for Refund	Substitute Specification, Facsimile Coversheet
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> CD, Number of CD(s) _____	
	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Certified Copy of Priority Document(s)	Remarks	The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.
<input type="checkbox"/> Reply to Missing Parts/ Incomplete Application		
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm Name	Townsend and Townsend and Crew LLP		
Signature			
Printed name	Jason D. Lohr		
Date	September 29, 2006	Reg. No.	48,163

CERTIFICATE OF TRANSMISSION/MAILING	
I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office, Fax No. 1-571-273-8300 on September 29, 2006.	
Signature	
Typed or printed name	Krista K. Merrimac
Date	September 29, 2006

60881158 v1

RECEIVED
CENTRAL FAX CENTER

PATENT

Appl. No. 11/366,758
Amđt. dated September 29, 2006
Reply to Office Action of August 29, 2006

SEP 29 2006

BEST AVAILABLE COPY

Amendments to the Claims:

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

Listing of Claims:

Claims 1-21. (Canceled)

22. (Original) 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. (Original) 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.

Claims 24-34. (Canceled)

35. (Original) 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;

Appl. No. 11/366,758
Amdt. dated September 29, 2006
Reply to Office Action of August 29, 2006

PATENT

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. (Original) 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. (Previously Presented) A data access terminal as claimed in claim 35 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. (Original) 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. (Previously Presented) A data access terminal as claimed in claim 37 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. (Previously Presented) A data access terminal according to claim 35 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. (Original) 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.

Appl. No. 11/366,758
Amdt. dated September 29, 2006
Reply to Office Action of August 29, 2006

PATENT

42. (Previously Presented) A data access terminal according to claim 35 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. (Previously Presented) A data access terminal according to claim 35 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 characterizing data from the data supplier;
code to retrieve supplementary data in response to said characterizing data; and
code to output the supplementary data.

44. (Previously Presented) A data access terminal according to claim 35 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. (Previously Presented) A data access terminal according to claim 35 integrated with a mobile communication device, a personal computer, an audio/video player, and/or a cable or satellite television interface device.

46. (Original) 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. (Original) 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.

Appl. No. 11/366,758
Amdt. dated September 29, 2006
Reply to Office Action of August 29, 2006

PATENT

48. (Original) A method of providing data as claimed in claim 47, wherein the payment validation system comprises a payment processor at the data supplier.

49. (Previously Presented) A method of providing data as claimed in claim 46 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. (Previously Presented) A method of providing data as claimed in claim 48. 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.

Claims 51-58. (Canceled)

59. (Original) 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. (Original) A method of controlling access according to claim 59, further comprising:

- writing updated use status data to the carrier after an access attempt.

Appi. No. 11/366,758
Amdt. dated September 29, 2006
Reply to Office Action of August 29, 2006

PATENT

61. (Original) 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. (Previously Presented) A method of controlling access according to claim 59, further comprising:

inputting a user access data;

selecting the use rules dependent upon the user access data.

Claims 63-74. (Canceled)

Appl. No. 11/366,758
Amdt. dated September 29, 2006
Reply to Office Action of August 29, 2006

RECEIVED
CENTRAL FAX CENTER

PATENT

SEP 29 2006

REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed August 29, 2006. Claims 1-74 were pending in the present application. This Amendment cancels claims 1-21, 24-34, 51-58, and 63-74, without adding or amending any claims, leaving pending in the application claims 22-23, 35-50, and 59-62. Consideration of the elected claims is respectfully requested.

I. Restriction of the Claims.

The claims are subjected to restriction under 35 U.S.C. §121 as being drawn to groups classified as:

Group I: Claims 1-9, as being drawn to a method of providing portable data;

Group II: Claims 10-21, 51-58, 67, and 68, as being drawn to a portable data carrier;

Group III: Claims 22-23, 35-50, and 59-62, as being drawn to a method and apparatus of controlling access to data; and

Group IV: Claims 24-34, 63-66, and 68-74, as being drawn to a system controlled by data bearing records.

Although Applicants do not necessarily agree with these groupings and/or the need for restriction, Applicants hereby elect to prosecute the claims of Group III without traverse. Applicants reserve the right to present the non-elected claims in subsequent continuing applications. Applicants hereby cancel the claims of Groups I, II, and IV, and request consideration and examination of the claims of Group III (claims 22-23, 35-50, and 59-62).

II. Substitute Specification

Submitted with this response is a substitute specification under 37 C.F.R. §1.125. This substitute specification is submitted in order to correct various informalities and typographical errors in the specification. This substitute specification does not include any new matter. The substitute specification is attached in two versions as required, a version with marking showing all the changes relative to the immediate prior version of the specification of record, and an

RECEIVED
CENTRAL FAX CENTER
PATENT
SEP 29 2006

Appl. No. 11/366,758
Amdt. dated September 29, 2006
Reply to Office Action of August 29, 2006

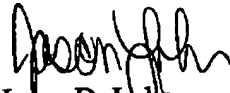
accompanying clean version without markings. Applicants respectfully request acceptance of the substitute specification.

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.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,


Jason D. Lohr
Reg. No. 48,163

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 650-326-2422
JDL/km
60876654 v1

Attorney Docket No.: 080379-000100US
Client Reference No.: F/USP81421X

SUBSTITUTE SPECIFICATION

DATA STORAGE AND ACCESS SYSTEMS

BACKGROUND OF THE INVENTION

5 [0001] 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.

10

[0002] 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 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.

15

[0003] 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.

20

25

30

SUMMARY OF THE INVENTION

[0004] 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; 5 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.

[0005] Another aspect of the invention provides a corresponding mobile data retrieval device 10 for retrieving and outputting data such as stored music and/or noise from the data storage device.

[0006] 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 15 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.

[0007] A further advantage of the system is that it allows users under the age of 18 to make 20 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 25 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. 30 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 35 as a credit card, it can be used by young people without the risk of their incurring large debt...

[0008] 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.

[0009] 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 a memory storing information to identify the person who is paying for the downloaded data.

[0010] 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.

[0011] 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 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
 5 level on a game or to enable further tracks of an album.

[0012] 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
 10 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.

[0013] In one embodiment the data storage means comprises an electronic memory card or
 15 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
 20 track and/or an accompanying video.

[0014] 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.
 25 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
 30 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.

[0015] Data held on the data storage means may advantageously include data relating to the
 35 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.

5

[0016] 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.

10

[0017] 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 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 storage means has a capacity of 128 megabytes or greater.

15

20

[0018] 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.

25

[0019] 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 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

30

35

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.

5

[0020] 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 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.

10

[0021] 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 (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.

15

[0022] 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.

20

25

[0023] 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.

30

[0024] 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

35

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 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
 5 exchange of payment/use data with an external system to validate the use.

[0025] 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 control over the stored data for the data content provider or data copyright owner. Preferably,
 10 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.

15 [0026] 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
 20 storage/retrieval. Preferably, however, access to any stored value/payment data is nevertheless retained.

[0027] Supplementary data may also be stored on the carrier in association with stored content data. This supplementary data may comprise customer reward management data
 25 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.

30 [0028] 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
 35 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 5 frequencies and low frequencies (for audio). This arrangement also facilitates customer reward and loyalty management.

[0029] In one embodiment the data carrier further comprises memory for storing data for 10 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 15 onto the carrier.

[0030] 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 20 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 25 provides a small and convenient portable format and facilitates removable interfacing with a variety of devices.

[0031] 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 30 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.

[0032] According to another aspect of the invention, there is provided a computer system for 35 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
5 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
10 interface.

[0033] 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
15 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, 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
20 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.

[0034] Preferably, the computer system includes payment distribution information so that
25 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 computer system to the computer systems of other relevant parties
30 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.

5 [0035] 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, 10 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.

15 [0036] 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 20 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.

25 [0037] 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.

30 [0038] 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 35 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
5 and to write the retrieved data into the data carrier.

[0039] 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
10 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.

15 [0040] 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,
20 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
25 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.

30 [0041] 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
35 carrier. 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
5 such as a local area network (LAN), wide area network (WAN) or extranet.

[0042] 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
10 writing the retrieved data into the data carrier.

[0043] 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
15 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.

[0044] 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
25 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.

[0045] 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
35 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.

5 [0046] 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.

10 [0047] 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.

20 [0048] 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.

25 [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 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.

30 [0050] 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
35 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,
 5 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.

10

[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 printer location data identifying an electronic address for a
 15 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
 20 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.

25

[0052] 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
 30 from a data store; and outputting payment data to a payment system for distributing the payment for the requested data.

30

[0053] 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;
 35 receiving payment data from the requester relating to payment for the requested data;

35

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

5 [0054] These and other aspects of the invention will now be further described, by way of example only, with reference to the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS.

10 [0055] Figure 1 shows a data access device a) from the top; b) from the front; and c) from the side;

[0056] Figure 2 shows, conceptually, a portable data carrier;

[0057] Figures 3a and b show exemplary data access terminals;

15 [0058] 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;

[0059] Figure 5 shows a content provision system;

20 [0060] Figure 6 shows a data supply computer system;

[0061] Figure 7 shows a variety of data access terminals;

25 [0062] Figure 8 shows a schematic diagram of components of a data access terminal;

[0063] Figure 9 shows a schematic diagram of components of a data carrier;

[0064] Figure 10 shows a schematic diagram of components of a data access device;

30 [0065] Figures 11a and 11b are flow diagrams of a data carrier registration process;

[0066] 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;
35 and

[0067] Figure 13 shows a flow diagram of data retrieval using a data access device.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0068] 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).

[0069] 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.

[0070] 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.

[0071] 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.

[0072] 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 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.

5

[0073] 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.

10

[0074] 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.

15

[0075] 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.

20

[0076] 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.

25

[0077] 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,

30

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
 5 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
 10 network.

[0078] 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
 15 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.

[0079] The content provision system includes a plurality of content providers 108a-e, each
 20 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
 25 content data.

[0080] 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
 30 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
 35 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.

5 [0081] 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 10 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.

15 [0082] 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 20 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 25 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.

30 [0083] 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.

[0084] 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 35 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.

[0085] 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.

[0086] 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.

[0087] 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.

[0088] 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 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, 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.

[0089] 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, while the value of £10 might permit an unlimited number of plays of the track and copying of the track for personal use.

[0090] 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 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.

[0091] 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).

5 [0092] 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.

10 [0093] 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
15 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
20 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.

25 [0094] 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
30 removed from the terminal, but in some embodiments the data carrier may be integral with the terminal.

[0095] 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
35 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.

5 [0096] 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.

15 [0097] 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 20 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.

25 [0098] 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 30 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 35 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.

5 [0099] 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
10 between a smart Flash card interface to the terminal and data supply system 120.

[0100] 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
15 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.

20 [0101] 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
25 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.

[0102] Referring in more detail to Figure 9, a data and communications bus 204 links
30 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-
35 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.

- 5 [0103] 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
- 10 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.
- 15 [0104] 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.
- 20 [0105] 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
- 25 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
- 30 intermediaries, for example on a commission or reward points basis.
- [0106] 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
- 35 into which the data memory is partitioned are larger.

[0107] 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.

[0108] 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.

[0109] 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 233c 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) which is hereby incorporated by reference.

[0110] 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 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.

[0111] 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).

[0112] 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 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 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.

[0113] 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 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.

[0114] Figure 11b shows the corresponding registration steps performed by the system 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 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 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.

[0115] 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.

[0116] 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.

[0117] 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.

[0118] 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.

5 [0119] 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
10 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.

[0120] 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
15 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.

[0121] In the presently described embodiment, payment record data received in step S55 is
20 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.

[0122] In step S56, together with the payment record data, purchase request and card
25 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
30 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.

[0123] 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
5 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
10 of data which are not correctly received.

[0124] Also at step S57, one or more content access rules is 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
15 allowed access to the content data item.

[0125] 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
20 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-
25 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.

[0126] The add monetary value menu option provided by the menu operates in a similar
30 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
35 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.

[0127] 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.

[0128] 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.

[0129] 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.

5

10

[0130] 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, 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.

15

20

25

[0131] 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

30

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.

5 [0132] 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.

25 [0133] 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.

35 [0134] 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.

10 [0135] 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
15 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
20 menu; if content use is permitted the system proceeds to step S84.

[0136] 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
25 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
30 (trade mark) motor bikes for rock music/video).

[0137] 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
35 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.

[0138] 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.

[0139] 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.

[0140] 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.

[0141] 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.

[0142] The skilled person will understand that many variants to the system are possible and
5 the invention is not limited to the described embodiments but encompasses modifications
which lie within the spirit and scope of the present invention.

60881106 v1

COMPARISON COPY

WO-01/31599

PCT/GB00/04110

Attorney Docket 80379-000100US
Client Ref. F/USP81421X

SUBSTITUTE SPECIFICATION

DATA STORAGE AND ACCESS SYSTEMS

Background of the Invention

[0001] 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.

~~One~~**[0002]** 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 ~~unauthorised~~ unauthorized or legitimate means and then make this data available essentially world-wide over the internet without ~~authorisation~~ authorization. Data can be a very valuable commodity, but once it has been published on the ~~Internet~~ internet it is difficult to police access to and use of it by Internet users who may not even ~~realise~~ 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.

[0003] 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 ~~realise~~ realize the potential of this, and many ~~unauthorised~~ 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.

~~The invention described below addresses this and related problems.~~

Summary of the Invention

[0004] 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.

[0005] 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.

[0006] 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.

[0007] 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.

[0008] 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.

[0009] The downloaded data ~~maybe~~ 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 a memory storing information to identify the person who is paying for the downloaded data.

[0010] 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.

[0011] The data storage means and/or the retrieval device can be provided with access control means to prevent ~~unauthorised~~-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 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.

[0012] 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.

[0013] 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.

[0014] 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.

[0015] 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.

[0016] 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.

[0017] 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 can include software, and particularly games, share price information, current news information, transport timetable information, weather information and catalogue-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 storage means has a capacity of 128 megabytes or greater.

[0018] 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.

[0019] 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 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.

[0020] 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 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.

[0021] 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 (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.

[0022] 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.

[0023] 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.

[0024] 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~~ 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 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.

[0025] 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~~ while 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.

[0026] 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.

[0027] 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.

[0028] 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~~, 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 ~~scheme~~ 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.

[0029] 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.

[0030] 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.

[0031] 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.

[0032] 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.

[0033] The computer system is operated by a data supplier or data supply ~~scheme~~ "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 (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.

[0034] 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,~~ while 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 ~~Ee-~~payment system. Alternatively, the computer system can issue appropriate instructions to a third party ~~Ee-~~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.

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] The terminal reads payment data from the data carrier and transmits this to a payment validation system for validating the data and ~~authorising~~ 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.

[0041] 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~~ characterizing data such as card user preference data from the data supplier computer system, and this ~~characterising~~ 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 (LAN), wide area network (WAN) or extranet.

[0042] 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.

[0043] 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.

[0044] 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.

[0045] 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.

[0046] 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.

[0047] 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.

[0048] 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.

[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 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.

[0050] 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.

[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 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-the~~ 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-the~~ payment data.

[0052] 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.

[0053] 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.

[0054] 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:-~~

Brief Description of the Drawings

[0055] Figure 1 shows a data access device a) from the top; b) from the front; and c) from the side;

[0056] Figure 2 shows, conceptually, a portable data carrier;

[0057] Figures 3a and b show exemplary data access terminals;

Figure[0058] 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;

[0059] Figure 5 shows a content provision system;

[0060] Figure 6 shows a data supply computer system;

[0061] Figure 7 shows a variety of data access terminals;

[0062] Figure 8 shows a schematic diagram of components of a data access terminal;

[0063] Figure 9 shows a schematic diagram of components of a data carrier;

[0064] Figure 10 shows a schematic diagram of components of a data access device;

[0065] Figures 11a and 11b ~~show a~~ are flow diagrams of a data carrier registration process;

[0066] 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

[0067] Figure 13 shows a flow diagram of data retrieval using a data access device.

Description of the Preferred Embodiments

[0068] 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~~ 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).

[0069] 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.

[0070] 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.

[0071] 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.

[0072] 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~~ 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.

[0073] 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.

[0074] 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.

[0075] 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.

[0076] 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.

[0077] 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.

[0078] 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.

[0079] 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.

[0080] 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~~ **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.

[0081] 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~~

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.

[0082] 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~~ 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.

[0083] In alternative embodiments, a data carrier such as the smart ~~flash~~ Flash card described below may be used to create value bearing digital signatures as is well-known to those familiar with e-money.

[0084] 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~~ "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 ~~thence~~ 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 ~~echeque-check~~ spend and website link functions described below.

[0085] 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.

[0086] 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.

[0087] 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.

[0088] 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 a user when registering with the ~~scheme~~ system owner. This data comprises a user password for accessing stored

content and/or payment data; user ~~characterising~~ characterizing data, for example ~~characterising~~ characterizing 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.

[0089] 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~~ while the value of £10 might permit an unlimited number of plays of the track and copying of the track for personal use.

[0090] 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~~ 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.

[0091] 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).

[0092] 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.

[0093] 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-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 ~~scheme-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 ~~thence-then~~ to a portable data carrier.

[0094] 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.

[0095] 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.