UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/779,299	07/06/2010	7748636	FINN-C18	1938

63397 7590 06/16/2010

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 497 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

David Finn, Tourmakeady, IRELAND;

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINNN, David**
	Art Unit	
	Examiner Name	
Sheet 2 OF 2	Practitioner Docket No.	**FINN-C18**

U.S. PATENT APPLICATION PUBLICATIONS

Exam. Initials	Cite No.	Publication Number.	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
	A1	US 2001 0043702	11-22-2001	Elteto et al.	
	A2	US 2001 0054148	12-20-2001	Hoornaert	
	A3	US 2002 0011516	01-31-2002	Lee	
	A4	US 2003 0000267	01-02-2003	Jacob et al.	
	A5	US 2003 0028797	02-06-2003	Long et al.	
	A6	US 2003 0087601	05-08-2003	Agam et al.	
	A7	US 2003 0102380	06-05-2003	Spencer	
	A8	US 2003 0236821	12-25-2003	Jiau	
	A9	US 2005 0274803	12-15-2005	Lee	(HK 04104126.5)
	A10	US 2005 0109841	05-26-2005	~~FINN~~ Ryan et al.	a related application (c4)

DG 12/3/10

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

Note: this is not an EFS form
Filename: C18_substitute_IDS_Foreign_rev

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	11/779,299
	Filing Date	7/18/2007
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	FINN, David
	Art Unit	
	Examiner Name	Tuyen Kim Vo
Sheet 1 OF 1	Practitioner Docket No.	FINN-C18

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	DE19631050	02-05-1998	Bergler et al.	Drawings
	2	HK 1063994	12/2004		
	3	HK 1063995	10/2004		
	4	JP2004246720	09-02-2004	Sazawa et al.	Drawings
	5	WO99 052051	10-14-1999	International Business Machines	
	6	WO99 038062	07-29-1999	Kobil Computer GMBH	Abs.(Engl), Dwg.
	7	WO00 036252	06-22-2000	Jacob	Abs.(Engl), Dwg.
	8	WO00 042491	07-20-2000	Rainbow Technologies, Inc.	
	9	WO00 065180	11-02-2000	Muller et al.	Abs.(Engl), Dwg.
	10	WO00 075755	12-14-2000	Eutron Infosecurities	
	11	WO01 014179	03-01-2001	Wittwer et al.	Abs.(Engl), Dwg.
	12	WO01 038673	03-31-2001	Wittwer et al.	Abs.(Engl), Dwg.
	13	WO01 039102	11-02-2001	Muller et al.	
	14	WO01 048339	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.
	15	WO01 048342	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.
	16	WO01 061692	08-23-2001	Trek Technology	
	17	WO01 088693	11-22-2001	Seysen	Abs.(Engl), Dwg.
	18	WO01 096990	12-20-2001	Rainbow Technologies, Inc.	
	19	WO03 014887	02-20-2003	Activcard Ireland	
	20	WO03 034189	04-23-2003	Activcard Ireland	
	21	WO04 002058	12-31-2003	Gemplus	Abs.(Engl), Dwg.
	22	WO04 081706	09-23-2004	Digisafe Ltd.	
	23	WO04 081769	09-24-2004	Axalto SA	
	24	WO05 022288	2005-03-10	Alladin Knowledge Systems	

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

63397 7590 05/26/2010

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121

EXAMINER	
VO, TUYEN KIM	
ART UNIT	PAPER NUMBER
2887	

DATE MAILED: 05/26/2010

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/779,299	07/18/2007	David Finn	FINN-C18	1938

TITLE OF INVENTION: PORTABLE IDENTITY CARD READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	08/26/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

63397 7590 05/26/2010

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/779,299	07/18/2007	David Finn	FINN-C18	1938

TITLE OF INVENTION: PORTABLE IDENTITY CARD READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	08/26/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
VO, TUYEN KIM	2887	235-492000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/779,299	07/18/2007	David Finn	FINN-C18	1938

63397 7590 05/26/2010

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121

EXAMINER	
VO, TUYEN KIM	
ART UNIT	PAPER NUMBER
2887	

DATE MAILED: 05/26/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 497 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 497 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Notice of Allowability	Application No.	Applicant(s)	
	11/779,299	FINN, DAVID	
	Examiner	Art Unit	
	Tuyen Kim Vo	2887	

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *04/28/2010*.

2. ☒ The allowed claim(s) is/are *1-15*.

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

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/T. K. V./
Examiner, Art Unit 2887

DETAILED ACTION

Acknowledgment

1. This Office action is responsive to the amendment filed on 04/28/2010.

Allowable Subject Matter

2. Claims 1-15 are allowed.

3. The following is an examiner's statement of reasons for allowance:

The prior art of record, taken alone or in combination, fail to teach or fairly suggests the arrangement of system and method of a portable RFID reader/card for physical access or logical access comprising a generally rectangular reader body; circuitry disposed within the reader body; portion a contactless ID card disposed in close proximity to the reader body; especially the limitations of an antenna positioned around the perimeter of the reader body which can act as a compensating antenna or to communicate with the contactless ID card (element 110, fig. 1); at least one antenna coil disposed in the reader body for communicating with corresponding at least one contactless fob (elements 120 and 130, fig. 1) inserted into the reader body in a contactless mode and the corresponding method steps as recited in claims 5 and 6 and further limitations of the dependent claims 2-4 and 7-15, respectively.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tuyen Kim Vo whose telephone number is (571)270-1657. The examiner can normally be reached on Monday - Friday, 7:30a.m. - 5:00p.m., EST.

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

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

/T. K. V./
Examiner, Art Unit 2887

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

Notice of References Cited	Application/Control No. 11/779,299	Applicant(s)/Patent Under Reexamination FINN, DAVID	
	Examiner Tuyen Kim Vo	Art Unit 2887	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0040242	02-2005	Beenau et al.	235/492
*	B	US-2005/0011961	01-2005	Uesaka, Kouichi	235/492
*	C	US-2004/0118930	06-2004	Berardi et al.	235/492
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

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

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. 1938

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/779,299	07/18/2007	235	2887	Finn-C18

APPLICANTS

David Finn, Tourmakeady, IRELAND;

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

This application is a CIP of 11/420,747 05/27/2006 PAT 7,597,250
and claims benefit of 60/832,799 07/24/2006
and is a CIP of 11/355,264 02/15/2006
and is a CIP of 10/990,296 11/16/2004 PAT 7,213,766

Yes/tkv

**** FOREIGN APPLICATIONS *************************** None/tkv

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
07/28/2007

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/TUYEN KIM VO/ Examiner's Signature	☐ Initials	IRELAND	2	15 tkv	3

ADDRESS

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121
UNITED STATES

TITLE

Portable Identity Card Reader System For Physical and Logical Access

FILING FEE RECEIVED		
425	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	6	(rfid (radio adj frequency adj identification)) same reader same (contactless (non adj contact)) same (slot recess) same fob	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:11
S2	14	(rfid (radio adj frequency adj identification)) same reader same (slot recess) same fob	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:13
S3	41	("20010043702" | "20010054148" | "20020011516" | "20030000267" | "20030028797" | "20030087601" | "20030102380" | "20030236821" | "3941489" | "4367965" | "5761648" | "6067235" | "6085320" | "6148354" | "6168077" | "6189098" | "6240184" | "6283658" | "6370603" | "6385677" | "6505773" | "6543690" | "6567273" | "6658516" | "6676420" | "6694399" | "6724680" | "6748541" | "6752321" | "6763399" | "6772956" | "6798169" | "6801956" | "6848045" | "6876420" | "6879597" | "6983888").PN. OR ("7213766").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:16
S4	30	S3 and card	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:20
S5	2	S4 and (contactless (non adj contact))	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:23
S6	30	("6116927" | "6190184" | "6375479" | "6439900").PN. OR ("6676420"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:25
S7	2	S6 and (contactless (non adj contact))	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:30
S8	2	S6 and rfid	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:30
S9	17	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same (slot recess) same fob	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:31
S10	1003	card$1 same (contactless (non adj contact) rfid) same (slot recess)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48

S11	362	card$1 same (contactless (non adj contact) rfid) same (slot recess) same reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48
S12	4808	235/451,492.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48
S13	41	S11 and S12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48
S14	83	("4443027" | "4614861" | "4641374" | "4684791" | "4700055" | "4749982" | "4851654" | "4877945" | "5180902" | "5272319" | "5276311" | "5367572" | "5434395" | "5521362" | "5530232" | "5534683" | "5544246" | "5741184").PN. OR ("6012636").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:01
S15	27	S14 and (contactless (non adj contact))	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:02
S16	69	("20010000405" | "20010045458" | "20010053239" | "20020017558" | "20020025062" | "20020060243" | "20020073315" | "20020095389" | "20020123972" | "20020128980" | "20020130187" | "20020138438" | "20020148892" | "20020150282" | "20020153424" | "20020158747" | "20020164057" | "20020166891" | "20020178124" | "20020180584" | "20030028481" | "20030031321" | "20030046249" | "20030083954" | "20030093385" | "20030116621" | "20030116630" | "20030218065" | "20040029409" | "20040199469" | "3868057" | "4529870" | "4879645" | "5239166" | "5484997" | "5530232" | "5559885" | "5578808" | "5623552" | "5657389" | "5680205" | "5770849" | "5787186" | "5796832" | "5907149" | "5987155" | "6012039" | "6012636" | "6182892" | "6193152" | "6213391" | "6219439" | "6270011" | "6293462" | "6325285" | "6334575" | "6335688" | "6422462" | "6424249" | "6454173" | "6457640" | "6464146" | "6505772" | "6631201" | "6698654").PN. OR ("6983882").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:34
S17	7	S16 and contactless	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:37
S18	1	"20040188519".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:42

S19	7	S16 and ((non adj contact) contactless)	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:17
S20	234	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3)	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:25
S21	6418	((non adj contact) contactless) same card	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:25
S22	21	S20 same S21	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:25
S23	11	S22 and rfid	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:31
S24	2	"20060219776".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 17:40
S25	1	"20060219776".pn. and (SD same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 17:41
S26	2	"20060219776".pn. and rfid	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:23
S27	84	(rfid (radio adj frequency adj identification)) same ((dual multiple multi plurality plural) adj interface$1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:27
S28	9405	235/492,451,380.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:27
S29	8	S27 and S28	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:27
S30	1	"20040188519".pn. and contactless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:55

S31	1	"20040188519".pn. and activat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:16
S32	1	"20060219776".pn. and (electronic same immobilizer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:23
S33	3	(pda (personal adj digital adj assistan $2)) same electronic same immobilizer	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:32
S34	24	(pda (personal adj digital adj assistan $2) rfid) same electronic same immobilizer	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:35
S35	2	"20060219776".pn. and nfc	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:59
S36	1	"20060219776".pn. and synchronize	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 09:15
S37	40	(transaction with (authenticat$3 or authoriz$5 or verif$5) with (number)) same (((one near time) or (single near use)) near2 (password or key code))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:46
S38	4	(transaction near (authenticat$3 or authoriz$5 or verif$5) near (number)) same (((one near time) or (single near use)) near2 (password or key code))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:47
S39	6	(synchroniz$5 or simultaneous$2) with (internet near atomic near clock)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:51

S40	0	(single near (sign adj (on in))) with (fingerprint or biometric)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:59
S41	1	(single near (sign adj (on in))) with (multiple plural$3) with (network or (web near (site or page)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:00
S42	0	(electronic$3 with immobilizer) near ((rfid (radio adj frequency identification)) adj (reader)) near car	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:07
S43	0	(electronic$3 with immobilizer) near ((rfid (radio adj frequency identification)) adj (reader))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:07
S44	0	(electronic$3 near immobilizer) near ((rfid (radio adj frequency identification)) adj (reader))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:08
S45	1	(electronic$3 near immobilizer) same (rfid (radio adj frequency adj identification)) same authenticat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:08
S46	8	(electronic$3 near immobilizer) same (rfid (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:09
S47	200	(electronic$3 near immobilizer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:09
S48	53	S47 and (rfid (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:10

S49	3	S48 and authenticat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:10
S50	12	(reader adaptor) near ((plural$3 different multiple (multi adj ple)) adj (recess$2 slot$2)) near card$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:36
S51	0	S50 and (rfid or (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:39
S52	10	("20040188519" | "20040201457" | "20040230831" | "6078908" | "6639957").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 19:12
S53	424	card$1 same (contactless (non adj contact) rfid) same (slot recess) same reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 19:19
S54	52	(contactless (non adj contact) rfid) same (slot recess) same reader same biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 19:20
S55	70	("20010000405" | "20010045458" | "20010053239" | "20020017558" | "20020025062" | "20020060243" | "20020073315" | "20020095389" | "20020123972" | "20020128980" | "20020130187" | "20020138438" | "20020148892" | "20020150282" | "20020153424" | "20020158747" | "20020164057" | "20020166891" | "20020178124" | "20020180584" | "20030028481" | "20030031321" | "20030046249" | "20030083954" | "20030093385" | "20030116621" | "20030116630" | "20030218065" | "20040029409" | "20040199469" | "3868057" | "4529870" | "4879645" | "5239166" | "5484997" | "5530232" | "5559885" | "5578808" | "5623552" | "5657389" | "5680205" | "5770849" | "5787186" | "5796832" | "5907149" | "5987155" | "6012039" | "6012636" | "6182892" | "6193152" | "6213391" | "6219439" | "6270011" | "6293462" | "6325285" | "6334575" | "6335688" | "6422462" | "6424249" | "6454173" |	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:24

		"6457640" | "6464146" | "6505772" | "6631201" | "6698654").PN. OR ("6983882").URPN.				
S56	35	biometric and S55	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:25
S57	6	S56 and contactless	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:31
S58	62	("4614861" | "4972476" | "5180906" | "5235680").PN. OR ("5770849"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:33
S59	16	biometric and S58	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:34
S60	1188	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:49
S61	438962	switch$3 with power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:49
S62	158	S60 and S61	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:49
S63	4674	235/451,492.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:50
S64	7617	340/572.$.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:51
S65	11980	S63 S64	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:51
S66	101	S60 and S65	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:51
S67	241	(contactless (non adj contact) rfid (radio adj frequency adj identification)) with reader with biometric with card	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:03
S68	31596	switch$3 with power with activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:04
S69	2	S67 and S68	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:04
S70	2	(contactless (non adj contact) rfid (radio adj frequency adj identification)) with reader with biometric with switch$3 with power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:08
S71	15	(contactless (non adj contact) rfid (radio adj frequency adj identification)) with reader with biometric with switch$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:08
S72	4482	finn.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 20:11
S73	19556	rfid with reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 20:11

S74	28	S72 and S73	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 20:11
S75	107	("4443027" | "4614861" | "4641374" | "4684791" | "4700055" | "4749982" | "4851654" | "4877945" | "5180902" | "5272319" | "5276311" | "5367572" | "5434395" | "5521362" | "5530232" | "5534683" | "5544246" | "5741184").PN. OR ("6012636").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:35
S76	1212	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:36
S77	12	S75 and S76	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:36
S78	205	biometric same sensor same (activat $3 (turn adj on)) same power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:40
S79	70	S76 and S78	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:40
S80	127	selker.in.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:44
S81	2084	biometric same activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:44
S82	0	S80 and S81	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:44
S83	511	reader same biometric same activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S84	2857849	power battery	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S85	174	S83 same S84	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S86	30798	rfid	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S87	55	S85 same S86	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S88	1	"6012636".pn. and activat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 11:50
S89	1195	biometric with activat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 11:52

S90	10	biometric with activat$3 with contactless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 11:52
S91	43	biometric with activat$3 with power	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 13:22
S92	110263	power with activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:28
S93	1212	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:29
S94	156	S92 and S93	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:29
S95	5	S92 same S93	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:29
S96	169	reader same biometric same activat$3 same power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:30
S97	118479	("20030141365" | "20030169152" | "20040073726" | "20060148404" | "20070055633" | "20070250707" | "20070263596" | "20080032626" | "6398116" | "6839772" | "7248834").PN"	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:24
S98	58	biometric same reader same switch$3 same activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S99	0	S97 and S98	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S100	316	biometric same switch$3 same activat $3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S101	2	S97 and S100	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S102	2	"20060219776".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/06 21:41
S103	0	(rfid (radio adj frequency adj identification)) same biometric same (single adj sign adj on) same authenticat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:44
S104	461	(rfid (radio adj frequency adj identification)) same biometric same authenticat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:44
S105	7	(single adj sign adj on)	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:44
S106	0	S104 and S105	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:45

S107	34040	(rfid (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:45
S108	0	S105 and S107	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:45
S109	3	(password$1 (pass adj word$1) code pin (personal adj identification adj number)) same (internet adj atomic adj clock)	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:48
S110	29	(internet adj atomic adj clock)	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:50
S111	3	S104 and S110	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:50
S112	2	"20040188519".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:48
S113	147889	("20020073340" | "20020095608" | "20030141365" | "20030169152" | "20040188519" | "20040201457" | "20040230831" | "20040073726" | "20060161789" | "20060148404" | "20070055633" | "20070250707" | "20070263596" | "20080032626" | "6078908" | "6592031" | "6639957" | "6398116" | "6839772" | "7248834")".PN"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:50
S114	15632	235/451,492,375,380.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:53
S115	164	S113 and S114	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:53
S116	62	S115 and ((rfid (radio adj frequency adj identification) contactless noncontact))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:54
S117	64	("20010043702" | "20010054148" | "20020011516" | "20020073340" | "20020095608" | "20030000267" | "20030028797" | "20030087601" | "20030102380" | "20030141365" | "20030169152" | "20030236821" | "20040073726" | "20040129787" | "20040188519" | "20040201457" | "20040230831" | "20050035200" | "20050109841" | "20050274803" | "20060148404" | "20060161789" | "20060206582" | "20060208066" | "20070055633" | "20070250707" |	US-PGPUB; USPAT; USOCR	OR	ON	2009/11/18 09:56

		"20070263596" | "20080032626" | "4367965" | "5761648" | "6067235" | "6078908" | "6085320" | "6148354" | "6168077" | "6189098" | "6240184" | "6283658" | "6342839" | "6370603" | "6385677" | "6398116" | "6505773" | "6543690" | "6567273" | "6592031" | "6639957" | "6658516" | "6694399" | "6724680" | "6744634" | "6748541" | "6752321" | "6763399" | "6772956" | "6798169" | "6801956" | "6813164" | "6839772" | "6848045" | "6876420" | "6879597" | "6983888" | "7248834").PN. OR ("7597250").URPN.				
S118	0	"6592031".pn. and (wireless same network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 08:35
S119	1	"6592031".pn. and (network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 08:35
S120	2	"6592031".pn. and (computer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 08:36
S121	0	"6592031".pn. and (bluetooth zigbee wibree)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 10:58
S122	9	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same (deactivat$3 (log$1 adj off) (de adj activat$3)) same (bluetooth zigbee wibree)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:00
S123	1	("20010054148", "20050035200", "20040188519").pn. and (bluetooth zigbee wibree)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:13
S124	1	S123 and deactivat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:14
S125	0	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3) same clip$4 same (lanyard cord)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:28
S126	0	((((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3)) same clip $4 same (lanyard cord)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29

S127	325	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29
S128	12787	clip$4 same (lanyard cord)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29
S129	1	S127 and S128	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29
S130	490	card$1 same (contactless (non adj contact) rfid) same (slot recess) same reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:33
S131	2	S128 and S130	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:33
S132	70855	(slot recess) same neck	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:36
S133	4	S130 and S132	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:36
S134	57497	(slot recess) same hang$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:37
S135	9	S130 and S134	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:37
S136	5	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3) same clip$4	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:39
S137	13889	235/375,380,451,492,487.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:40
S138	13834	clip$3 same hang$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:40
S139	20	S137 and S138	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:45
S140	0	S139 and contactless	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:46
S141	42	S137 and lanyard	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:55
S142	15	S141 and clip$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 12:38

S143	222	(rfid (radio adj frequency adj identification)) same reader same antenna same (perimeter boundary outer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/15 08:47
S144	101	((rfid (radio adj frequency adj identification) (contact adj less) (non adj contact)) adj reader) same antenna same (perimeter boundary outer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/15 08:49
S145	0	((rfid (radio adj frequency adj identification) (contact adj less) (non adj contact)) adj (adapter holder)) same antenna same (perimeter boundary outer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/15 09:15
S146	0	((rfid (radio adj frequency adj identification) (contact adj less) (non adj contact)) adj (adapter)) same antenna same (perimeter boundary outer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/15 09:16
S147	5699	235/451,492,486.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2010/05/15 09:16
S148	14	S143 and S147	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/15 10:06
S149	17532	reader with antenna$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/17 09:48
S151	6556	(rfid (radio adj frequency adj identification)) with reader with antenna$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/17 09:49
S152	33682	antenna with coil	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/17 09:51
S153	582	S151 same S152	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/17 09:51
S154	14598	235/375,380,451,492,487.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2010/05/17 10:02

S155	76	S153 and S154	US-PGPUB; USPAT; USOCR	OR	ON	2010/05/17 10:03
S156	1	"20080303633".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2010/05/17 10:34
S157	1	"7070112".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2010/05/17 10:41

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S158	1611	(rfid (radio adj frequency adj identification)) with reader with antenna$1	USPAT; UPAD	OR	ON	2010/05/17 18:02
S159	76	(card same (contactless (contact adj less))) same fob	USPAT; UPAD	OR	ON	2010/05/17 18:04
S160	21	S158 and S159	USPAT; UPAD	OR	ON	2010/05/17 18:04

5/17/2010 10:10:49 PM
C:\Documents and Settings\tvo3\My Documents\EAST\Workspaces\11420747.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11779299	FINN, DAVID
	Examiner	**Art Unit**
	Tuyen K Vo	2887

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	12/14/2009								
1	1	✓								
2	2	✓								
3	3	✓								
4	4	✓								
11	5	✓								
12	6	✓								
13	7	✓								
14	8	✓								
15	9	✓								
5	10									
6	11									
7	12									
8	13									
9	14									
10	15									

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11779299	FINN, DAVID
	Examiner	**Art Unit**
	Tuyen K Vo	2887

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
235	492	G 0 6 K 19 / 06 (2006.01.01)	
		G 0 6 K 7 / 08 (2006.01.01)	

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
235	375	380	451	487	492

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1														
2	2														
3	3														
4	4														
11	5														
12	6														
13	7														
14	8														
15	9														
5	10														
6	11														
7	12														
8	13														
9	14														
10	15														

/Tuyen K Vo/ Examiner.Art Unit 2887	05/17/2010	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
/Thien Minh Le/	5/18/2010	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11779299	FINN, DAVID
	Examiner	Art Unit
	Tuyen K Vo	2887

SEARCHED			
Class	Subclass	Date	Examiner
235	375, 380, 451, 487, 492	12/14/2009	tkv
	Text Search	05/17/2010	tkv

SEARCH NOTES		
Search Notes	Date	Examiner
EAST	12/14/2009	tkv
Search on related case 11/420,747	11/18/2009	tkv
Updated Search	05/15/2010	tkv
Consulted with Thien Le, Primary	05/17/2010	tkv

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
235	375, 380, 451, 487, 492	05/17/2010	tkv

/T. K. V./ Examiner.Art Unit 2887	

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

63397 7590 05/26/2010

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Gerald E. Linden	(Depositor's name)
Gerald E Linden	(Signature)
May 26 2010	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/779,299	07/18/2007	David Finn	FINN-C18	1938

TITLE OF INVENTION: PORTABLE IDENTITY CARD READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	08/26/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
VO, TUYEN KIM	2887	235-492000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Gerald E. Linden
2 Dwight A. Stauffer
3 X

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: DPD Patent Trust Ltd.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Lower Churchfield, Tourmakeady, Co. Mayo, IRELAND

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached. Pd ONLINE
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature Gerald E Linden Date 5-27-2010

Typed or printed name Gerald E Linden Registration No. 30282

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Confirmation No. 1938

In re	:	Application of FINN
For	:	PORTABLE IDENTITY CARD READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS
Serial No.	:	11/779,299
Filed	:	7/18/2007
Group Art Unit	:	2887
Examiner	:	Vo
Our Docket No.	:	C18

May 27, 2010

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

MISC TRANSMITTAL

Enclosed is "Part B – Fee(s) Transmittal"

Item 2

Gerald E. Linden

Dwight A. Stauffer

Item 3

DPD Patent Trust Ltd. (an Irish corporation)
Lower Churchfield, Tourmakeady, Co. Mayo, Ireland
Assignment Recordation 019713/0627

For the Applicant,
/Gerald E. Linden/ May 27, 2010
Gerald E. Linden date
Reg. 30282
561 983 6292

Electronic Patent Application Fee Transmittal

Application Number:	11779299
Filing Date:	18-Jul-2007
Title of Invention:	PORTABLE IDENTITY CARD READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS
First Named Inventor/Applicant Name:	David Finn
Filer:	Gerald Linden
Attorney Docket Number:	FINN-C18

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	755	755
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1055**

Electronic Acknowledgement Receipt	
EFS ID:	7696576
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	PORTABLE IDENTITY CARD READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	FINN-C18
Receipt Date:	26-MAY-2010
Filing Date:	18-JUL-2007
Time Stamp:	23:40:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1055
RAM confirmation Number	5747
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Issue Fee Payment (PTO-85B)	IF_PartB_abx.pdf	1690633 5b8d9df697d78599c6b8d7e489aaf22b10c7c397	no	1
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	TRANS_May27.pdf	15961 e126f89c96ee4e89ba507298c5c45a5cc97602ac	no	1
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	31609 cd1b1ae424b7ff0790093ae3b225cb8bad504b4e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1738203		

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Confirmation No. 1938

In re	:	Application of FINN
For	:	PORTABLE IDENTITY CARD READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS
Serial No.	:	11/779,299
Filed	:	7/18/2007
Group Art Unit	:	2887
Examiner	:	Vo
Our Docket No.	:	C18

Apr 28, 2010

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

This is in response to an Office action dated 1/28/2010. Due 4/28/2010.

Please amend the above-referenced application as follows:

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims begin on page 3 of this paper.

Remarks/Arguments begin on page 6 of this paper.

Amendments to the Specification

At page 22, typographical error

A contactless ID card 110 may be disposed in a recess (receptacle) 108 on the front surface 104 of the reader body 102. Grooves or barbs may be provided to hold the ID card 110 in place. Alternatively, the user can clip their ID card also to the lanyard, so as to be in close proximity to the reader body 102. The reader 100 and the card 110 are used in combination. The contactless ID card 110 may conform to ISO 7810 standard, and may be generally ~~retangular~~ rectangular.

At page 23, typographical error

FIG. 2 illustrates how the contactless fobs 120 and 130 can communicate in contactless mode with the reader 100. Two antenna coils 122 and 132 are positioned in the reader body 102 to communicate with the two contactless fobs 120 and 130, respectively, in a contactless mode. In addition, there is an antenna 112 positioned around the perimeter of the reader body 102 which can act as a compensating antenna or to communicate with the ID card 110. No antenna is needed for the SD card 140, since it uses a contact interface. An additional antenna (not shown) may be included as a ~~as a~~ stripe of metal on the motherboard of the reader, for communicating via wireless such as with a wireless token (see 372, below) plugged into a user's computer (see 370, below).

Abstract, page 32, typographical error

A portable RFID reader apparatus having a contactless interface and slots or recesses for [[for]] insertion of contactless smart card fobs, including ID card, and having a wireless interface for communicating with a token plugged into a computer, provides physical and logical access.

Amendments to the Claims

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

Listing of Claims:

1. (currently amended) A portable RFID reader / card system for physical access or logical access comprising:

a generally rectangular reader body;

circuitry disposed within the reader body; ~~portion; and~~

a contactless ID card disposed in close proximity to the reader body ~~portion~~;

an antenna positioned around the perimeter of the reader body which can act as a compensating antenna or to communicate with the contactless ID card;

at least one antenna coil disposed in the reader body for communicating with corresponding at least one contactless fob inserted into the reader body in a contactless mode.

2. (original) The portable RFID reader / card system of claim 1, wherein:

the circuitry is arranged to communicate with the contactless ID card in a contactless mode and with an external reader in a wireless mode.

3. (original) The portable RFID reader / card system of claim 2, wherein:

the contactless ID card is disposed in a recess in a surface of the body portion.

4. (original) The portable RFID reader / card system of claim 2, wherein:

the contactless ID card is clipped to a lanyard which is attached to the body portion.

5. (currently amended) A method of using a contactless ID card for physical entry comprising:

disposing the ID card in close proximity to a portable reader system; and

presenting the combination of card and reader apparatus to a mullion reader;

wherein the portable reader system comprises:

a generally rectangular reader body;

circuitry disposed within the reader body; ~~portion; and~~

a contactless ID card disposed in close proximity to the reader body ~~portion~~;

an antenna positioned around the perimeter of the reader body which can act as a compensating antenna or to communicate with the contactless ID card;

at least one antenna coil disposed in the reader body for communicating with corresponding at least one contactless fob inserted into the reader body in a contactless mode.

6. (currently amended) A method of using a contactless ID card for logical access comprising:

disposing the ID card in close proximity to a portable reader system; and

presenting the combination of card and reader apparatus to a wireless token associated with a personal computer;

wherein the portable reader system comprises:

a generally rectangular reader body;

circuitry disposed within the reader body; ~~portion; and~~

a contactless ID card disposed in close proximity to the reader body ~~portion~~;

an antenna positioned around the perimeter of the reader body which can act as a compensating antenna or to communicate with the contactless ID card;

at least one antenna coil disposed in the reader body for communicating with corresponding at least one contactless fob inserted into the reader body in a contactless mode.

7. (original) The method of claim 6, wherein:

when the user is in the vicinity of their computer, a communication event is opened up between the wireless token and combination of reader and ID card, thereby allowing the user to access a network after checking the credentials on the proximity (ID) card via the reader / card system.

8. (currently amended) The method of claim 7, further comprising:

when the user moves away from their computer, the communication signal between the reader / card system and the wireless token deteriorates, and the computer automatically logs-off from the network or goes into password protected security ~~mode. Once~~ mode, once the reader / card system carried by the user is out of range of the Zigbee / Bluetooth.

9. (original) The method of claim 7, wherein the token uses a standard selected from the group consisting of Zigbee, Bluetooth, and Wibree.

Please enter the following - -

10. (new) The portable RFID reader / card system of claim 1, further comprising:
a contact interface for an SD card inserted into the reader.

11. (new) The portable RFID reader / card system of claim 1, wherein:
the at least one antenna coil comprises two antenna coils for communicating with corresponding two contactless fobs inserted into the reader body in the contactless mode.

12. (new) The portable RFID reader / card system of claim 1, further comprising:
an additional antenna for communicating via a wireless token plugged into a user's computer.

13. (new) The portable RFID reader / card system of claim 1, wherein the circuitry comprises:
a contactless interface; and
a wireless interface.

14. (new) The portable RFID reader/card system of claim 13, wherein:
the contactless interface is selected from the group consisting of ISO 14443, ISO 15693, NFC, and any similar interface.

15. (new) The portable RFID reader/card system of claim 13, wherein:
the wireless interface is selected from the group consisting of IEEE 802.11, Bluetooth, Zigbee, Wibree, and any similar interface. - -

REMARKS

Status

Claims 1-9 are pending.

Claims 1-9 are rejected

Independent claim 1: A portable RFID reader / card system

Independent claim 5: A method of using a contactless ID card for physical entry

Independent claim 6: A method of using a contactless ID card for logical access

Claim Objections

Claim 8	changes recommended,
Applicant's Response:	amended herewith

Claim Rejections

Claims 1-3, 5-7	§102 over Klatt 6592031
	Klatt: Figs 5a, 5b col 1, lines 25-27 col 5, lines 18-67
Claim 4	§103 over Klatt in view of Lee 6809646
	Lee: Fig 1 and col 2 lines 44-55
Claims 8,9	§103 over Klatt in view of Cassone 20040188519
	Cassone: "P" Fig. 6, [0095,0099,0105,0106]

The Invention, Generally

A portable RFID reader apparatus having a contactless interface and slots or recesses for insertion of contactless smart card fobs, including ID card, and having a wireless interface for communicating with a token plugged into a computer, provides physical and logical access.

Traversing the Rejection

The "main" reference is Klatt, used as §102 against independent **claims 1, 5 and 6.**

Klatt (6592031) discloses a PC card authentication system has a PC card having a PC card housing with a plug connector at one end thereof configured to be inserted into a computer slot of a computer and to provide electrical contact with the computer. Electronic components

are mounted in the PC card housing and are connected to the plug connector. A sensor is provided for detecting biometric data of a person for the purpose of authenticating the identity of a person. More particularly:

> Klatt's invention relates to an authentication system for PC cards, especially according to the PCMCIA standard, comprised of a housing shaped like a plug-in card for receiving electronic components such as a chip card reader, a memory expansion, a drive, or a modem wherein the housing is provided at one end thereof with a plug connector for electrically connecting the PC card to a computer. (col 1)
>
> Especially the use of PC cards as readers for chip cards has become more and more common. This is so because the chip cards as so-called smart cards are used increasingly for identity checks. These applications relate especially to the area of on-line banking, such as Internet banking according to the HBCI standard, pay TV, or access control to data networks. The identification and authorization for authorized users can be initiated in connection with a code number such as a PIN to be input by the user. (col 1)
>
> An alternative possibility of contacting chip cards 9 and PC cards 1 is represented in FIGS. 5a and 5b. Contacting of chip card 9 and PC card 1 is realized without physical contact by radio-technological means. For this purpose, the printed circuit board 10 has an areal antenna 20 which cooperates with an areal antenna 21 on the chip card 9 in order to transmit the required electrical energy from the PC card 1 onto the chip card 9. The sensor 5 on the chip card 9 as well as the cryptographic processor arranged also on the chip card 9 are supplied with electrical energy by the areal antenna 21. The areal antennas 20, 21 are embodied at the same time as a sending and receiving antenna. As is especially illustrated in FIG. 5a, on the printed circuit board 10 at the end opposite the plug connector 3 a sending and receiving unit 22 is provided which cooperates radio-technologically with the sending and receiving unit 21 of the chip card 9. The energy supply is realized preferably via an integrated battery in the chip card 9. This allows a radio-technological data transmission between PC card 1 and one or more chip cards 9 across a great distance. Alternatively, an opto-electronic coupling, for example, by infrared coupling, is possible. (col 5)

By arranging the sensor 5 for detecting biometric data either on the chip card 9 or on the PC card 1, an authentication system is provided that allows determination of the authenticity of persons or groups of persons. Based on the individual features contained in the biometric data it is possible in a simple manner to realize an unambiguous and reliable identity check which, by excluding unauthorized access, is especially suitable with respect to the requirements of mobile applications of PC cards. By providing a cryptographic processor 14 it is also possible to transform the detected biometric data by a complex cryptographic system into data which are inaccessible to unauthorized persons, while providing persons authorized to use the system the required information for encoding and decoding the data. Accordingly, the inventive authentication system is especially suitable for chip card readers in the form of PC cards which in connection with smart cards allow for a controlled and safe access to data networks or similar facilities. By identifying groups of persons, for example, by successive detection of multiple fingerprints, for which purpose e.g. a plurality of sensors can be arranged on the chip card 9 or the PC card 1, multiple encoding steps can be realized, depending on the desired safety level. A high level of safety is moreover realized in that when using a sensor 5 for detecting biometric data on a slide 4, the movement of the slide 4 can be controlled for an identity check by the provider when communication with a computer via the PC card 1 is established. (col 5)

The <u>invention</u> is directed to a portable card reader 100 which may provide for physical access or logical access. More particularly,

A contactless ID card 110 may be disposed in a recess (receptacle) 108 on the front surface 104 of the reader body 102. Grooves or barbs may be provided to hold the ID card 110 in place. Alternatively, the user can clip their ID card also to the lanyard, so as to be in close proximity to the reader body 102. The reader 100 and the card 110 are used in combination. The contactless ID card 110 may conform to ISO 7810 standard, and may be generally rectangular. (page 22)

FIG. 1 illustrates how a user can insert two contactless fobs 120 and 130 into the reader 100 for applications such as identification, payment, loyalty, ticketing, couponing etc. In addition, an SD memory stick 140 can be inserted into the reader 100 for the purpose of storing data. The data can be transferred to the memory stick in wireless mode from

the host computer or the reader can be connected directly to a USB port of the host computer using a cable. Not shown is a mini USB socket in the reader. (page 22-23)

FIG. 2 illustrates how the contactless fobs 120 and 130 can communicate in contactless mode with the reader 100. Two antenna coils 122 and 132 are positioned in the reader body 102 to communicate with the two contactless fobs 120 and 130, respectively, in a contactless mode. In addition, there is an antenna 112 positioned around the perimeter of the reader body 102 which can act as a compensating antenna or to communicate with the ID card 110. No antenna is needed for the SD card 140, since it uses a contact interface. (page 23)

An additional antenna (not shown) may be included as a stripe of metal on the motherboard of the reader, for communicating via wireless such as with a wireless token (see 372, below) plugged into a user's computer (see 370, below). (page 23)

A portable reader apparatus 300 (compare 100), with a plurality of contactless cards 310 (compare 110) and 330 (compare 120 and/or 130) inserted therein, and extended memory 340 (compare 130) inserted therein, constitute what may be called a "reader/card system" 350. (page 23)

For physical access, a user presents his reader/card system 350 near a wall reader 360 which is connected to a facility computer 362, and access to the facility may be provided and logged in. This is in contactless (close proximity) mode, as indicated by the two-headed arrow 366. (page 23)

For logical access, a user is in proximity with his computer 370, and a wireless link is provided between the reader/card system 350 and a token 372 plugged into the computer 370. This is in wireless (vicinity) mode. The user can then use the computer, including accessing other networked computers 374, as indicated by the arrow 376. (page 23)

There has thus been described herein a portable RFID reader / card system (combination of reader and card) in the form of a card body structure with a slot to accommodate the attachment of a lanyard and grooves on each side of the housing to allow the bearer to slide in their proximity card for physical access control. (page 24)

For logical access the portable reader / card system communicates in wireless mode with a Zigbee / Bluetooth / Wibree USB token inserted into (associated with) a USB port of the user's work station / personal computer. (page 25)

At page 26, description of Fig. 4, including contactless Interfaces 412 and wireless interfaces 418

Claim 1 is amended to distinguish over Klatt, including some of the features described above. Also, new dependent claims 10,11.

Claims 5 and 6 are amended to bring into conformity with **claim 1.**

Claims / Claim count

Highest number previously paid for

20 total, 3 independent

3 independent

The claim count is unchanged.

Total number of claims = 15

Total independent claims = 3

Conclusion

The claims should be allowed.

No new matter is entered by this amendment.

No fees are necessitated.

For the Applicant,
/Gerald E. Linden/ April 28, 2010
Gerald E. Linden date
Reg. 30282
561 983 6292

Electronic Acknowledgement Receipt	
EFS ID:	7502274
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	28-APR-2010
Filing Date:	18-JUL-2007
Time Stamp:	05:17:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMD_april_2010.pdf	51511 717c4c60e409fa6e1f0c629edc2965c2edbb17ab	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Specification	2	2
	Claims	3	5
	Applicant Arguments/Remarks Made in an Amendment	6	10
Warnings:			
Information:			
	Total Files Size (in bytes):	51511	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/779,299	07/18/2007	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ 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))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	04/28/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 15	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

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

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

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

Legal Instrument Examiner:
/WANDA LAWSON/

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/779,299	07/18/2007	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ 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))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	04/28/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 15	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

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

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

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

Legal Instrument Examiner:
/WANDA LAWSON/

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/779,299	07/18/2007	David Finn	Finn-C18	1938

63397 7590 01/28/2010

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121

EXAMINER	
VO, TUYEN KIM	
ART UNIT	PAPER NUMBER
2887	

NOTIFICATION DATE	DELIVERY MODE
01/28/2010	ELECTRONIC

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

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

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

GELPATENTS@YAHOO.COM

Office Action Summary	Application No.	Applicant(s)	
	11/779,299	FINN, DAVID	
	Examiner	Art Unit	
	Tuyen Kim Vo	2887	

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

Period for Reply

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

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

Status

1)☐ Responsive to communication(s) filed on _____.

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) 1-9 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) 1-9 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ 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 18 July 2007 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/SB/08) Paper No(s)/Mail Date 08/02/2007; 08/03/2007; 08/27/2007 & 03/09/2009.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 8 is objected to because of the following informalities:

Re claim 8, line 4, substitute “mode. Once” to - - mode, once - -. Also, need to add period, -- . -- at the end of the claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

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

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

3. Claims 1-3 and 5-7 are rejected under 35 U.S.C. 102(b) as being anticipated by Klatt (US 6,592,031).

Re claim 1, Klatt teaches a portable RFID reader/card system comprising: a generally rectangular body (figs. 5a and 5b); circuitry (10) disposed within the body portion; and a contactless ID card (9) disposed in close proximity to the body portion. See column 5, lines 18-40.

Re claim 2, Klatt further teaches the circuitry is arranged to communicate with the contactless ID card in a contactless mode (see column 5, lines 29-37) and with an external reader in a wireless network (the circuitry having antenna 20 which implies wireless communication, see fig. 5a).

Re claim 3, Klatt further teaches the contactless ID card is disposed in a recess (insertion channel 8) in a surface of the body portion (see figs. 5a).

Re claims 5 and 6, Klatt teaches a system and method for physical entry and logical access using a contactless card (figs. 5a and 5b), comprising: disposing the ID card (9) in a close proximity to a portable reader system (1); and presenting the combination of card and reader apparatus to a mullion reader or a wireless token associated with a personal computer (see column 1, lines 25-57 and column 5, lines 18-67).

Re claim 7, Klatt further teaches when the user is in the vicinity of their computer, a communication event is opened up between the wireless token and combination of reader and ID card (the circuitry having antenna 20 which implies wireless communication, see fig. 5a), thereby allowing the user to access a network after checking the credential on the proximity (ID) card via the reader/card system (see column 5, lines 40-67).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Klatt in view of Lee (US 6,809,646).

Re claim 4, Klatt teaches all subject matter claimed as applied above except for the card is clipped to a lanyard as claimed.

Lee teaches RFID device including an aperture 102 with an attachment clip, lanyard, etc., for attaching the device to a person or another object to be identified (see fig. 1 and column 2, lines 44-55).

In view of Lee's teachings, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Klatt to provide an aperture with an attachment clip, lanyard for attaching the card to an object or another device as taught by Lee so that the card can be attached or worn by the user.

6. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klatt in view of Cassone (US 2004/0188519).

Re claims 8 and 9, Klatt teaches all subject matter claimed as applied above except for deactivating when the user moves away or is out of range.

Cassone teaches portable device including Bluetooth communication which, of course, the communications will be lost (deactivated) when the portable device (P, fig. 6) is moved away or out of range (See [0095], [0099], [0105], [0106]).

In view of Cassone's teachings, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Klatt to provide Bluetooth communications as taught by Cassone since it is just an alternative way of using different types of communication means.

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tuyen Kim Vo whose telephone number is (571)270-1657. The examiner can normally be reached on Monday - Friday, 7:30a.m. - 5:00p.m., EST.

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

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

/T. K. V./
Examiner, Art Unit 2887

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

Notice of References Cited	Application/Control No. 11/779,299	Applicant(s)/Patent Under Reexamination FINN, DAVID	
	Examiner Tuyen Kim Vo	Art Unit 2887	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,809,646	10-2004	Lee, Donny V.	340/572.1
*	B	US-6,592,031	07-2003	Klatt, Dieter	235/382
*	C	US-2001/0054148	12-2001	Hoornaert et al.	713/172
*	D	US-2004/0188519	09-2004	Cassone, Jean	235/382
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11779299	FINN, DAVID
	Examiner	Art Unit
	Tuyen K Vo	2887

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	12/14/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11779299	FINN, DAVID
	Examiner	Art Unit
	Tuyen K Vo	2887

SEARCHED			
Class	Subclass	Date	Examiner
235	375, 380, 451, 487, 492	12/14/2009	tkv

SEARCH NOTES		
Search Notes	Date	Examiner
EAST	12/14/2009	tkv
Search on related case 11/420,747	11/18/2009	tkv

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

/T. K. V./ Examiner.Art Unit 2887	

Note: this is not an EFS form

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11779299** conf 1938
	Filing Date	**07/18/2007**
	First Named Inventor	**Finn**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Art Unit	
	Examiner Name	Tuyen Kim Vo
Sheet 1 OF 2	Practitioner Docket No.	**C18**

U.S. PATENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY -or- MM/YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	4014602	03-29-1977	Ruell	
	2	4897644	01-30-1990	Hirano	
	3	5034648	07-23-1991	Gastgeb	
	4	5084699	01-28-1992	DeMichele	
	5	5376778	12-27-1994	Kreft	
	6	5399847	03-21-1995	Droz	
	7	5696363	12-9-1997	Larchevesque	
	8	5741392	04-12-1998	Droz	
	9	6111288	08-29-2000	Watanabe, et al.	
	10	6343744	02-05-2002	Shibata, et al.	
	11	6424029	07-23-2002	Giesler	
	12	6522308	02-18-2003	Mathieu	
	13	6575374	06-10-2003	Boyadjian , et al.	
	14	6879424	04-12-2005	Vincent, et al.	
	15	7054050	05-30-2006	Vincent, et al.	
	16	7093499	08-22-2006	Baudendistel	
	17	7145432	12-05-2006	Lussey , et al.	

U.S. PATENT APPLICATION PUBLICATIONS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY -or- MM/YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	A1	20030132301	07-17-2003	Selker	
	A2	20060255903	11-16-2006	Lussey et al.	
	A3	20070290051	12-20-2007	Bielmann et al.	

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	F1	CA 2279176	07-30-1998	Rietzler Manfred See also WO98/33142	
	F2	DE 10140662	03-20-2003	Osterwald et al.	
	F3	DE 19542900	05-22-1997	Michalk et al	
	F4	DE 19742126	03-25-1999	Hoedeau et al	
	F5	FR 2728710	06-28-1996	Larchevesque et al	
	F6	WO98/20450	05-14-1998	Austria Card GmbH	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

Note: this is not an EFS form

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11779299** conf 1938
	Filing Date	**07/18/2007**
	First Named Inventor	**Finn**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Art Unit	
	Examiner Name	
Sheet 2 OF 2	Practitioner Docket No.	**C18**

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	N1	-none cited at this time-	T

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

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. 1938

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/779,299	07/18/2007	235	2887	Finn-C18

APPLICANTS

David Finn, Tourmakeady, IRELAND;

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

This application is a CIP of 11/420,747 05/27/2006 PAT 7,597,250
and claims benefit of 60/832,799 07/24/2006
and is a CIP of 11/355,264 02/15/2006
and is a CIP of 10/990,296 11/16/2004 PAT 7,213,766

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
07/28/2007

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /TUYEN KIM VO/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		IRELAND	2	9	3

ADDRESS

GERALD E. LINDEN
C/O STAUFFER
1006 MONTFORD RD.
CLEVELAND HEIGHTS, OH 44121
UNITED STATES

TITLE

Portable Identity Card Reader System For Physical and Logical Access

FILING FEE RECEIVED		
425	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"6592031".pn. and (bluetooth zigbee wibree)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 10:58
L2	9	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same (deactivat$3 (log$1 adj off) (de adj activat$3)) same (bluetooth zigbee wibree)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:00
L3	1	("20010054148", "20050035200", "20040188519").pn. and (bluetooth zigbee wibree)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:13
L4	1	3 and deactivat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:14
L5	0	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3) same clip$4 same (lanyard cord)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:28
L6	0	((((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3)) same clip $4 same (lanyard cord)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29
L7	325	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29
L8	12787	clip$4 same (lanyard cord)	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29
L9	1	7 and 8	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:29
L10	490	card$1 same (contactless (non adj contact) rfid) same (slot recess) same reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:33
L11	2	8 and 10	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:33
L12	70855	(slot recess) same neck	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:36

L13	4	10 and 12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:36
L14	57497	(slot recess) same hang$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:37
L15	9	10 and 14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 11:37
L16	5	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3) same clip$4	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:39
L17	13889	235/375,380,451,492,487.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:40
L18	13834	clip$3 same hang$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:40
L19	20	17 and 18	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:45
L20	0	19 and contactless	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:46
L21	42	17 and lanyard	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 11:55
L22	15	21 and clip$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/12/14 12:38
S1	6	(rfid (radio adj frequency adj identification)) same reader same (contactless (non adj contact)) same (slot recess) same fob	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:11
S2	14	(rfid (radio adj frequency adj identification)) same reader same (slot recess) same fob	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:13
S3	41	("20010043702" | "20010054148" | "20020011516" | "20030000267" | "20030028797" | "20030087601" | "20030102380" | "20030236821" | "3941489" | "4367965" | "5761648" | "6067235" | "6085320" | "6148354" | "6168077" | "6189098" | "6240184" | "6283658" | "6370603" | "6385677" | "6505773" | "6543690" | "6567273" | "6658516" | "6676420" | "6694399" | "6724680" | "6748541" | "6752321" | "6763399" | "6772956" | "6798169" | "6801956" | "6848045" | "6876420" |	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:16

		"6879597" | "6983888").PN. OR ("7213766").URPN.				
S4	30	S3 and card	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:20
S5	2	S4 and (contactless (non adj contact))	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:23
S6	30	("6116927" | "6190184" | "6375479" | "6439900").PN. OR ("6676420"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:25
S7	2	S6 and (contactless (non adj contact))	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:30
S8	2	S6 and rfid	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 14:30
S9	17	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same (slot recess) same fob	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:31
S10	1003	card$1 same (contactless (non adj contact) rfid) same (slot recess)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48
S11	362	card$1 same (contactless (non adj contact) rfid) same (slot recess) same reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48
S12	4808	235/451,492.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48
S13	41	S11 and S12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/01 14:48
S14	83	("4443027" | "4614861" | "4641374" | "4684791" | "4700055" | "4749982" | "4851654" | "4877945" | "5180902" | "5272319" | "5276311" | "5367572" | "5434395" | "5521362" | "5530232" | "5534683" | "5544246" | "5741184").PN. OR ("6012636").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:01
S15	27	S14 and (contactless (non adj contact))	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:02

S16	69	("20010000405" | "20010045458" | "20010053239" | "20020017558" | "20020025062" | "20020060243" | "20020073315" | "20020095389" | "20020123972" | "20020128980" | "20020130187" | "20020138438" | "20020148892" | "20020150282" | "20020153424" | "20020158747" | "20020164057" | "20020166891" | "20020178124" | "20020180584" | "20030028481" | "20030031321" | "20030046249" | "20030083954" | "20030093385" | "20030116621" | "20030116630" | "20030218065" | "20040029409" | "20040199469" | "3868057" | "4529870" | "4879645" | "5239166" | "5484997" | "5530232" | "5559885" | "5578808" | "5623552" | "5657389" | "5680205" | "5770849" | "5787186" | "5796832" | "5907149" | "5987155" | "6012039" | "6012636" | "6182892" | "6193152" | "6213391" | "6219439" | "6270011" | "6293462" | "6325285" | "6334575" | "6335688" | "6422462" | "6424249" | "6454173" | "6457640" | "6464146" | "6505772" | "6631201" | "6698654").PN. OR ("6983882").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:34
S17	7	S16 and contactless	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:37
S18	1	"20040188519".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 15:42
S19	7	S16 and ((non adj contact) contactless)	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:17
S20	234	(((non adj contact) contactless rfid (radio adj identification)) adj reader) with (slot recess insert$3)	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:25
S21	6418	((non adj contact) contactless) same card	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:25
S22	21	S20 same S21	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:25
S23	11	S22 and rfid	US-PGPUB; USPAT; USOCR	OR	ON	2008/12/01 16:31
S24	2	"20060219776".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 17:40
S25	1	"20060219776".pn. and (SD same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 17:41

S26	2	"20060219776".pn. and rfid	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:23
S27	84	(rfid (radio adj frequency adj identification)) same ((dual multiple multi plurality plural) adj interface$1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:27
S28	9405	235/492,451,380.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:27
S29	8	S27 and S28	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:27
S30	1	"20040188519".pn. and contactless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 18:55
S31	1	"20040188519".pn. and activat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:16
S32	1	"20060219776".pn. and (electronic same immobilizer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:23
S33	3	(pda (personal adj digital adj assistan $2)) same electronic same immobilizer	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:32
S34	24	(pda (personal adj digital adj assistan $2) rfid) same electronic same immobilizer	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:35

S35	2	"20060219776".pn. and nfc	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/03 19:59
S36	1	"20060219776".pn. and synchronize	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 09:15
S37	40	(transaction with (authenticat$3 or authoriz$5 or verif$5) with (number)) same (((one near time) or (single near use)) near2 (password or key code))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:46
S38	4	(transaction near (authenticat$3 or authoriz$5 or verif$5) near (number)) same (((one near time) or (single near use)) near2 (password or key code))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:47
S39	6	(synchroniz$5 or simultaneous$2) with (internet near atomic near clock)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:51
S40	0	(single near (sign adj (on in))) with (fingerprint or biometric)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 10:59
S41	1	(single near (sign adj (on in))) with (multiple plural$3) with (network or (web near (site or page)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:00
S42	0	(electronic$3 with immobilizer) near ((rfid (radio adj frequency identification)) adj (reader)) near car	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:07
S43	0	(electronic$3 with immobilizer) near ((rfid (radio adj frequency identification)) adj (reader))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:07

S44	0	(electronic$3 near immobilizer) near ((rfid (radio adj frequency identification)) adj (reader))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:08
S45	1	(electronic$3 near immobilizer) same (rfid (radio adj frequency adj identification)) same authenticat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:08
S46	8	(electronic$3 near immobilizer) same (rfid (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:09
S47	200	(electronic$3 near immobilizer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:09
S48	53	S47 and (rfid (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:10
S49	3	S48 and authenticat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:10
S50	12	(reader adaptor) near ((plural$3 different multiple (multi adj ple)) adj (recess$2 slot$2)) near card$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:36
S51	0	S50 and (rfid or (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/12/04 11:39
S52	10	("20040188519" | "20040201457" | "20040230831" | "6078908" | "6639957").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 19:12

S53	424	card$1 same (contactless (non adj contact) rfid) same (slot recess) same reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 19:19
S54	52	(contactless (non adj contact) rfid) same (slot recess) same reader same biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 19:20
S55	70	("20010000405" | "20010045458" | "20010053239" | "20020017558" | "20020025062" | "20020060243" | "20020073315" | "20020095389" | "20020123972" | "20020128980" | "20020130187" | "20020138438" | "20020148892" | "20020150282" | "20020153424" | "20020158747" | "20020164057" | "20020166891" | "20020178124" | "20020180584" | "20030028481" | "20030031321" | "20030046249" | "20030083954" | "20030093385" | "20030116621" | "20030116630" | "20030218065" | "20040029409" | "20040199469" | "3868057" | "4529870" | "4879645" | "5239166" | "5484997" | "5530232" | "5559885" | "5578808" | "5623552" | "5657389" | "5680205" | "5770849" | "5787186" | "5796832" | "5907149" | "5987155" | "6012039" | "6012636" | "6182892" | "6193152" | "6213391" | "6219439" | "6270011" | "6293462" | "6325285" | "6334575" | "6335688" | "6422462" | "6424249" | "6454173" | "6457640" | "6464146" | "6505772" | "6631201" | "6698654").PN. OR ("6983882").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:24
S56	35	biometric and S55	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:25
S57	6	S56 and contactless	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:31
S58	62	("4614861" | "4972476" | "5180906" | "5235680").PN. OR ("5770849"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:33
S59	16	biometric and S58	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:34
S60	1188	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:49
S61	438962	switch$3 with power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:49
S62	158	S60 and S61	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:49
S63	4674	235/451,492.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:50

S64	7617	340/572.$.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:51
S65	11980	S63 S64	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:51
S66	101	S60 and S65	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 19:51
S67	241	(contactless (non adj contact) rfid (radio adj frequency adj identification)) with reader with biometric with card	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:03
S68	31596	switch$3 with power with activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:04
S69	2	S67 and S68	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:04
S70	2	(contactless (non adj contact) rfid (radio adj frequency adj identification)) with reader with biometric with switch$3 with power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:08
S71	15	(contactless (non adj contact) rfid (radio adj frequency adj identification)) with reader with biometric with switch$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/11 20:08
S72	4482	finn.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 20:11
S73	19556	rfid with reader	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 20:11
S74	28	S72 and S73	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/11 20:11
S75	107	("4443027" | "4614861" | "4641374" | "4684791" | "4700055" | "4749982" | "4851654" | "4877945" | "5180902" | "5272319" | "5276311" | "5367572" | "5434395" | "5521362" | "5530232" | "5534683" | "5544246" | "5741184").PN. OR ("6012636").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:35
S76	1212	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:36
S77	12	S75 and S76	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:36
S78	205	biometric same sensor same (activat $3 (turn adj on)) same power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:40
S79	70	S76 and S78	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:40

S80	127	selker.in.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:44
S81	2084	biometric same activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:44
S82	0	S80 and S81	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:44
S83	511	reader same biometric same activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S84	2857849	power battery	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S85	174	S83 same S84	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S86	30798	rfid	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S87	55	S85 same S86	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 11:46
S88	1	"6012636".pn. and activat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 11:50
S89	1195	biometric with activat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 11:52
S90	10	biometric with activat$3 with contactless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 11:52
S91	43	biometric with activat$3 with power	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/28 13:22
S92	110263	power with activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:28
S93	1212	(contactless (non adj contact) rfid (radio adj frequency adj identification)) same reader same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:29
S94	156	S92 and S93	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:29
S95	5	S92 same S93	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:29
S96	169	reader same biometric same activat$3 same power	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 13:30

S97	118479	("20030141365" | "20030169152" | "20040073726" | "20060148404" | "20070055633" | "20070250707" | "20070263596" | "20080032626" | "6398116" | "6839772" | "7248834")".PN"	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:24
S98	58	biometric same reader same switch$3 same activat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S99	0	S97 and S98	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S100	316	biometric same switch$3 same activat $3	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S101	2	S97 and S100	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/28 16:25
S102	2	"20060219776".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/08/06 21:41
S103	0	(rfid (radio adj frequency adj identification)) same biometric same (single adj sign adj on) same authenticat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:44
S104	461	(rfid (radio adj frequency adj identification)) same biometric same authenticat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:44
S105	7	(single adj sign adj on)	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:44
S106	0	S104 and S105	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:45
S107	34040	(rfid (radio adj frequency adj identification))	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:45
S108	0	S105 and S107	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:45
S109	3	(password$1 (pass adj word$1) code pin (personal adj identification adj number)) same (internet adj atomic adj clock)	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:48
S110	29	(internet adj atomic adj clock)	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:50
S111	3	S104 and S110	US-PGPUB; USPAT; USOCR	OR	ON	2009/08/06 21:50
S112	2	"20040188519".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:48

S113	147889	("20020073340" | "20020095608" | "20030141365" | "20030169152" | "20040188519" | "20040201457" | "20040230831" | "20040073726" | "20060161789" | "20060148404" | "20070055633" | "20070250707" | "20070263596" | "20080032626" | "6078908" | "6592031" | "6639957" | "6398116" | "6839772" | "7248834")". PN"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:50
S114	15632	235/451,492,375,380.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:53
S115	164	S113 and S114	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:53
S116	62	S115 and ((rfid (radio adj frequency adj identification) contactless noncontact))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/18 09:54
S117	64	("20010043702" | "20010054148" | "20020011516" | "20020073340" | "20020095608" | "20030000267" | "20030028797" | "20030087601" | "20030102380" | "20030141365" | "20030169152" | "20030236821" | "20040073726" | "20040129787" | "20040188519" | "20040201457" | "20040230831" | "20050035200" | "20050109841" | "20050274803" | "20060148404" | "20060161789" | "20060206582" | "20060208066" | "20070055633" | "20070250707" | "20070263596" | "20080032626" | "4367965" | "5761648" | "6067235" | "6078908" | "6085320" | "6148354" | "6168077" | "6189098" | "6240184" | "6283658" | "6342839" | "6370603" | "6385677" | "6398116" | "6505773" | "6543690" | "6567273" | "6592031" | "6639957" | "6658516" | "6694399" | "6724680" | "6744634" | "6748541" | "6752321" | "6763399" | "6772956" | "6798169" | "6801956" | "6813164" | "6839772" | "6848045" | "6876420" | "6879597" | "6983888" | "7248834"). PN. OR ("7597250").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/11/18 09:56
S118	0	"6592031".pn. and (wireless same network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 08:35

S119	1	"6592031".pn. and (network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 08:35
S120	2	"6592031".pn. and (computer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/12/14 08:36

EAST Search History (Interference)

<This search history is empty>

12/14/2009 1:38:07 PM
C:\Documents and Settings\tvo3\My Documents\EAST\Workspaces\11420747.wsp

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11799299
Filing Date	2007-07-18
First Named Inventor	Finn
Art Unit	
Examiner Name	Tuyen Kim Vo
Attorney Docket Number	Finn-c18

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6398116		2002-06-04	Kreft	
	2	6839772		2005-01-04	Kowalski et al.	
	3	7248834		2007-07-24	Matsuo et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030141365		2003-07-21	Sowa et al.	
	2	20030169152		2003-09-11	Charrat et al.	
	3	20040073726		2004-04-15	Margalit et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

Receipt date: 03/09/2009	Application Number	11799299 11779299 - GAU: 2887
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2007-07-18
	First Named Inventor	Finn
	Art Unit	
	Examiner Name	
	Attorney Docket Number	Finn-c18

	4	20060148404		2006-07-06	Wakim	
	5	20070055633		2007-03-08	Cheon et al.	
	6	20070250707		2007-10-25	Noguchi	
	7	20070263596		2007-11-15	Carrat	
	8	20080032626		2008-02-07	Chen	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	DE 100 60 866 C1	DE		2002-02-05	AmaTech AG (Finn)		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

EFS Web 2.1.10

Receipt date: 03/09/2009	Application Number	11799299 11779299 - GAU: 2887
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2007-07-18
	First Named Inventor	Finn
	Art Unit	
	Examiner Name	
	Attorney Docket Number	Finn-c18

EXAMINER SIGNATURE			
Examiner Signature	/Tuyen Kim Vo/	Date Considered	12/14/2009

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

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

Note: this is not an EFS form
Filename: C18_substitute_IDS_USonly

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	Tuyen Kim Vo
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

U.S. PATENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	US 4,367,965	01-11-1983	Speitel et al.	
	2	US 5,761,648	06-02-1998	Golden et al.	
	3	US 6,067,235	05-23-2000	Finn et al.	
	4	US 6,085,320	07-04-2000	Kaliski, Jr.	
	5	US 6,148,354	11-14-2000	Ban et al.	
	6	US 6,168,077	01-02-2001	Gray et al.	
	7	US 6,189,098	02-13-2001	Kaliski, Jr.	
	8	US 6,240,184	05-29-2001	Huynh et al.	
	9	US 6,283,658	09-04-2001	Estevez et al.	
	10	US 6,342,839	01-29-2002	Curkendall et al.	
	11	US 6,370,603	04-09-2002	Silverman et al.	
	12	US 6,385,677	05-07-2002	Yao	
	13	US 6,505,773	01-14-2003	Palmer et al.	
	14	US 6,543,690	04-08-2003	Leydier et al.	
	15	US 6,567,273	05-20-2003	Liu et al.	
	16	US 6,658,516	12-02-2003	Yao	
	17	US 6,694,399	02-17-2004	Leydier et al.	
	18	US 6,724,680	04-20-2004	Ng et al.	
	19	US 6,744,634	06-01-2004	Yen	
	20	US 6,748,541	06-08-2004	Margalit et al.	
	21	US 6,752,321	06-22-2004	Leaming	
	22	US 6,763,399	07-13-2004	Margalit et al.	
	23	US 6,772,956	08-10-2004	Leaming	
	24	US 6,798,169	09-28-2004	Stratmann et al.	
	25	US 6,801,956	10-05-2004	Feuser et al.	
	26	US 6,813,164	11-02-2004	Yen	
	27	US 6,848,045	01-25-2005	Long et al.	
	28	US 6,876,420	04-05-2005	Hong et al.	
	29	US 6,879,597	04-12-2005	Tordera et al.	
	30	US 6,983,888	01-10-2006	Weng	

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINNN, David**
	Art Unit	
	Examiner Name	
Sheet 2 OF 2	Practitioner Docket No.	**FINN-C18**

U.S. PATENT APPLICATION PUBLICATIONS

Exam. Initials	Cite No.	Publication Number.	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
	A1	US 2001 0043702	11-22-2001	Elteto et al.	
	A2	US 2001 0054148	12-20-2001	Hoornaert	
	A3	US 2002 0011516	01-31-2002	Lee	
	A4	US 2003 0000267	01-02-2003	Jacob et al.	
	A5	US 2003 0028797	02-06-2003	Long et al.	
	A6	US 2003 0087601	05-08-2003	Agam et al.	
	A7	US 2003 0102380	06-05-2003	Spencer	
	A8	US 2003 0236821	12-25-2003	Jiau	
	A9	US 2005 0274803	12-15-2005	Lee	(HK 04104126.5)
	A10	US 2005 0109841	05-26-2005	FINN	a related application (c4)

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

Note: this is not an EFS form
Filename: C18_substitute_IDS_Foreign_rev

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	Tuyen Kim Vo
Sheet 1 OF 1	Practitioner Docket No.	**FINN-C18**

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	DE19631050	02-05-1998	Bergler et al.	Drawings
	2	HK 1063994			
	3	HK 1063995			
	4	JP2004246720	09-02-2004	Sazawa et al.	Drawings
	5	WO99 052051	10-14-1999	International Business Machines	
	6	WO99 038062	07-29-1999	Kobil Computer GMBH	Abs.(Engl), Dwg.
	7	WO00 036252	06-22-2000	Jacob	Abs.(Engl), Dwg.
	8	WO00 042491	07-20-2000	Rainbow Technologies, Inc.	
	9	WO00 065180	11-02-2000	Muller et al.	Abs.(Engl), Dwg.
	10	WO00 075755	12-14-2000	Eutron Infosecurities	
	11	WO01 014179	03-01-2001	Wittwer et al.	Abs.(Engl), Dwg.
	12	WO01 038673	03-31-2001	Wittwer et al.	Abs.(Engl), Dwg.
	13	WO01 039102	11-02-2001	Muller et al.	
	14	WO01 048339	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.
	15	WO01 048342	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.
	16	WO01 061692	08-23-2001	Trek Technology	
	17	WO01 088693	11-22-2001	Seysen	Abs.(Engl), Dwg.
	18	WO01 096990	12-20-2001	Rainbow Technologies, Inc.	
	19	WO03 014887	02-20-2003	Activcard Ireland	
	20	WO03 034189	04-23-2003	Activcard Ireland	
	21	WO04 002058	12-31-2003	Gemplus	Abs.(Engl), Dwg.
	22	WO04 081706	09-23-2004	Digisafe Ltd.	
	23	WO04 081769	09-24-2004	Axalto SA	
	24	WO05 022288	2005-03-10	Alladin Knowledge Systems	

/Tuyen Kim Vo/ 12/14/2009

Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

Note: this is not an EFS form
Filename: C18_substitute_IDS_NPL

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	Tuyen Kim Vo
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	1	*ACR38CT Contactless SIM Tracker Technical Specification*, Advanced Card Systems Ltd., Hong Kong.	T
	2	*ACR38DT Dual Key Technical Specifications*, Version 1.3, September 2004, Advanced Card Systems Ltd., Hong Kong.	T
	3	*Dallas Semiconductor DS1490F 2-in-1 Fob*, Dallas Semiconductor, Dallas TX.	T
	4	*Dallas Semiconductor DS9490R-DS9490B USB to 1-Wire/iButton Adaptor*, Maxim I-C, Sunnyvale CA.	T
	5	*Matsushita blends FERAM technology with smart cards*, HARA, YOSHIKO, EE Times, October 1, 2004, CMP Media, Manhasset NY.	T
	6	*Japan's Matsushita developing memory cards with smart chip function*, October 1, 2004, Mercury News, San Jose CA.	T
	7	*OTi-6828 Flash Disk Controller*, Ours Technology Inc., Taiwan.	T
	8	*Panasonic Develops RFID smartSD Card*, October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	*Panasonic Develops Industry's First SD Memory Card with Contacless Smart Card Capabilities*, October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	*Panasonic's Smart SD adds RFID to the mix*, ROJAS, PETER, October 4, 2004, Engadget LLC, New York NY.	T

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

	11	*Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply*, November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	*Digital Rights pits SIMS against Flash Cards, Card Technology*, BALABAN, DAN, November 2004, pp 24, 25, 26, 28, 30, Card Technology, Chicago IL.	T
	13	*Smart MX P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3*, October 2004, Koninklijke Philips Electronics NV, The Netherlands	T
	14	*Vodafone KK Develops Contactless Smart Card Mobile Handset*, May 6, 2004, HiTEK Magazine, Dubai	T
	15	*SmartSD Card Structure,* Panasonic	T

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

Note: this is not an EFS form
Filename: C18_substitute_IDS_Usonly_August

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**July 18, 2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

U.S. PATENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	6070240	05-30-2000	Xydis	
	2	6172430	01-09-2001	Schmitz et al.	
	3	6181024	01-30-2001	Geil et al.	
	4	6307471	10-23-2001	Xydis	
	5	6341727	01-29-2002	Canard et al.	
	6	6456958	09-24-2002	Xydis	
	7	6560711	05-06-2003	Given et al.	
	8	6745042	06-01-2004	Xydis	
	9	6763315	07-13-2004	Xydis	
	10	6913196	07-05-2005	Morrow et al.	
	11	6963794	11-08-2005	Geber et al.	
	12	6992562	01-31-2006	Fuks et al.	
	13	7034238	04-25-2006	Uleski et al.	
	14	7042332	05-09-2006	Takamura et al.	
	15	7150397	12-19-2006	Morrow et al.	

U.S. PATENT APPLICATION PUBLICATIONS

Exam. Initials	Cite No.	Publication Number.	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
	A1	US 20020065625	05-30-2002	Xydis	
	A2	US 20020069030	06-06-2002	Xydis	
	A3	US 20020104012	08-01-2002	Xydis	
	A4	US 20050044424	02-24-2005	Xydis	
	A5	US 20050269402	12-08-2005	Spitzer et al.	
	A6	US 20060186209	08-24-2006	Narend	
	A7	US 20060213982	09-28-2006	Cannon et al.	
	A8	US 20060226217	10-12-2006	Narend et al.	
	A9	US 20060230437	10-12-2006	Boyer et at.	
	A10	US 20060273176	12-07-2006	Audebert et al.	
	A11	US 20010054148	12-20-2001	Hoonaert et al.	

/Tuyen Kim Vo/ 12/14/2009
Examiner Signature Date Considered

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.K.V./

PTO/SB/08a (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	11799299
	Filing Date	2007-07-18
	First Named Inventor	Finn
	Art Unit	
	Examiner Name	
	Attorney Docket Number	Finn-c18

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6398116		2002-06-04	Kreft	
	2	6839772		2005-01-04	Kowalski et al.	
	3	7248834		2007-07-24	Matsuo et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030141365		2003-07-21	Sowa et al.	
	2	20030169152		2003-09-11	Charrat et al.	
	3	20040073726		2004-04-15	Margalit et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11799299
	Filing Date	2007-07-18
	First Named Inventor	Finn
	Art Unit	
	Examiner Name	
	Attorney Docket Number	Finn-c18

	4	20060148404		2006-07-06	Wakim	
	5	20070055633		2007-03-08	Cheon et al.	
	6	20070250707		2007-10-25	Noguchi	
	7	20070263596		2007-11-15	Carrat	
	8	20080032626		2008-02-07	Chen	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	DE 100 60 866 C1	DE		2002-02-05	AmaTech AG (Finn)		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	11799299
	Filing Date	2007-07-18
	First Named Inventor	Finn
	Art Unit	
	Examiner Name	
	Attorney Docket Number	Finn-c18

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	11799299
	Filing Date	2007-07-18
	First Named Inventor	Finn
	Art Unit	
	Examiner Name	
	Attorney Docket Number	Finn-c18

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Gerald E. Linden/	Date (YYYY-MM-DD)	2009-03-09
Name/Print	Gerald E. Linden	Registration Number	30282

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	4924490
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	09-MAR-2009
Filing Date:	18-JUL-2007
Time Stamp:	03:41:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	abx_DE_10060866_C1.pdf	748213 3371c94a62633f82d1964012c0ad0988b7c301b5	no	10

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Filed (SB/08)	IDS_c18_SB_08a.pdf	828791 6e45bc540ba76e7aee2adfa5ad2b3c84391118fe	no	5
Warnings:					
Information:					
			Total Files Size (in bytes):	1577004	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 100 60 866 C 1**

(51) Int. Cl.[7]:
G 06 F 3/033
G 06 K 11/18
G 06 K 19/077

(21) Aktenzeichen: 100 60 866.3-53
(22) Anmeldetag: 6. 12. 2000
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 2. 5. 2002

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
AmaTech AG, 87459 Pfronten, DE

(74) Vertreter:
Patentanwälte Böck + Tappe Kollegen, 97074 Würzburg

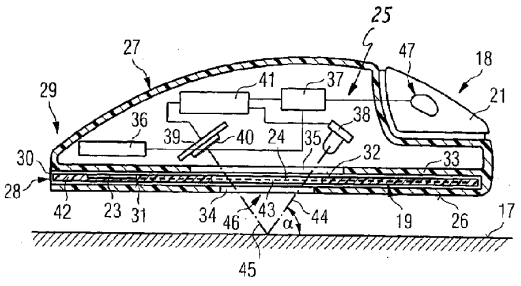
(72) Erfinder:
Finn, David, 87629 Füssen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 195 19 124 A1
DE 200 08 783 U1
EP 06 92 771 A2

(54) Handgehaltenes Peripheriesystem zur Eingabe von Daten in eine Computereinrichtung sowie Peripherieeinrichtung und Karteneinrichtung hierzu

(57) Die Erfindung betrifft ein handgehaltenes Peripheriesystem zur Eingabe von Daten in eine Computereinrichtung, umfassend einerseits eine Peripherieeinrichtung (18), insbesondere Computer-Maus, mit einem Gehäuse (27), einer im Gehäuse (27) angeordneten Navigationseinrichtung zur Erfassung von Navigationsdaten einer Relativbewegung des Gehäuses (27) auf einem Untergrund (17), einer Datenübertragungseinrichtung zur Datenübergabe von Navigationsdaten an die Computereinrichtung, einer Aufnahmeeinrichtung (28) zur Aufnahme einer Karteneinrichtung (19) sowie einer Leseeinrichtung (36), und umfassend andererseits eine Karteneinrichtung (19) mit einer Chipeinrichtung (23), wobei die Leseeinrichtung (36) zum Einlesen von in der Chipeinrichtung (23) gespeicherten Daten dient, wobei die Navigationseinrichtung eine optische Sensoreinrichtung aufweist, mit einer Lichtemissionseinrichtung (38) und einer Detektoreinrichtung (39), das Gehäuse (27) mit einem zumindest in einem ersten Transparenzbereich (34, 35) optisch durchlässigen Gehäuseboden (26) versehen ist und die Aufnahmeeinrichtung (28) derart zwischen der Detektoreinrichtung (39) und dem Gehäuseboden (26) angeordnet ist, dass die Karteneinrichtung (18) mit einem zweiten Transparenzbereich (43) im optischen Strahlengang (44, 45) zwischen der Lichtemissionseinrichtung (38) und der Detektoreinrichtung (39) angeordnet ist, sowie Karteneinrichtung (19) zur Verwendung in einem handgehaltenen Peripheriesystem.



DE 100 60 866 C 1

DE 100 60 866 C 1

Beschreibung

[0001] Die Erfindung betrifft ein handgehaltenes Peripheriesystem zur Eingabe von Daten in eine Computereinrichtung, umfassend einerseits eine Peripherieeinrichtung und andererseits eine Karteneinrichtung mit einer Chipeinrichtung gemäß dem Oberbegriff des Anspruch 1. Ferner betrifft die Erfindung die handgehaltene Peripherieeinrichtung sowie die Karteneinrichtung zur Verwendung im vorgenannten Peripheriesystem gemäß den Oberbegriffen des Anspruchs 3 bzw. 12.

[0002] Ein handgehaltenes Peripheriesystem der eingangs genannten Art ist aus der DE 200 08 783 U1 bekannt. Das bekannte Peripheriesystem umfasst eine fachsprachlich auch unter dem Begriff "Computer-Maus" bekannte, handgehaltene Peripherieeinrichtung sowie eine Karteneinrichtung, die mittels einer in der Peripherieeinrichtung vorgesehenen schlitzartigen Aufnahmeeinrichtung mit der Peripherieeinrichtung kombinierbar ist. Die Karteneinrichtung verfügt über eine als Chipeinrichtung ausgebildete Datenspeichereinrichtung, deren Daten über eine in der Computer-Maus vorgesehene Leseeinrichtung eingelesen und mittels einer Datenübertragungseinrichtung an die Computereinrichtung übertragbar sind. Bei dem bekannten handgehaltenen Peripheriesystem ist zur Erfüllung der "Maus-Funktion" eine Navigationseinrichtung zur Erfassung von Navigationsdaten einer Relativbewegung des Gehäuses auf einem Untergrund und eine Datenübertragungseinrichtung zur Datenübertragung der Navigationsdaten an die Computereinrichtung vorgesehen, wobei die Navigationseinrichtung eine mechanische Sensoreinrichtung, nämlich einen sogenannten "Mausball", aufweist.

[0003] Aus der DE 195 19 124 A1 ist eine optische Computer-Maus zur Dateneingabe in ein Computersystem bekannt, bei der die Positionsdaten der Maus auf einem Untergrund optisch erfasst und an das angeschlossene Computersystem übertragen werden.

[0004] Die EP 0 692 771 A2 offenbart eine Chipkarte, die aus einem insgesamt transparenten Material hergestellt sein kann.

[0005] Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein handgehaltenes Peripheriesystem umfassend eine handgehaltene Peripherieeinrichtung und eine Karteneinrichtung bereitzustellen, das die Ausgestaltung der Peripherieeinrichtung als optische Maus bei gleichzeitiger Integration einer Chipkarte als Datenspeichereinrichtung ermöglicht.

[0006] Diese Aufgabe wird durch ein handgehaltenes Peripheriesystem mit den Merkmalen des Anspruchs 1 gelöst.

[0007] Das erfindungsgemäße handgehaltene Peripheriesystem weist eine optische Sensoreinrichtung mit einer Lichtemissionseinrichtung und einer Detektoreinrichtung auf. Diese Sensoreinrichtung ermöglicht erfindungsgemäß in Kombination mit einer Karteneinrichtung, die mit einem Transparenzbereich versehen ist, und einer Anordnung der Karteneinrichtung in einer Aufnahmeeinrichtung zwischen der Detektoreinrichtung und dem Gehäuseboden, der in einem Transparenzbereich optisch durchlässig gestaltet ist, derart, dass die Karteneinrichtung mit ihrem Transparenzbereich im optischen Strahlengang zwischen der Lichtemissionseinrichtung und der Detektoreinrichtung angeordnet ist, eine ihrer Bestimmung gemäße funktionssichere Peripherieeinrichtung bei gleichzeitiger Anordnung der Karteneinrichtung innerhalb des Gehäuses ohne störende Beeinflussung der Bedienoberfläche der Computer-Maus.

[0008] Die vorliegende Erfindung weist somit eine besonders vorteilhafte Kombination der neuesten Computer-Maus-Technologie, wie sie beispielsweise aus der

DE 195 19 124 A1 bekannt ist, mit der aus der vorgenannten DE 200 08 783 U1 bekannten Integration einer Leseeinrichtung und einer Karteneinrichtung in eine Computer-Maus auf, ergänzt durch die weitere Kombination mit einer Karteneinrichtung, die einen Transparenzbereich aufweist, und so eine Anordnung im Gehäuse der Computer-Maus ermöglicht, die weder die Funktion der Navigationseinrichtung noch die Bedienoberfläche der Computer-Maus beeinträchtigt.

[0009] Darüber hinaus ermöglicht die Anordnung der Karteneinrichtung im optischen Strahlengang zwischen der Lichtemissionseinrichtung und der Detektoreinrichtung eine Anordnung parallel zum Gehäuseboden, der funktionsbedingt eben zum Untergrund ausgebildet ist, so dass die Anordnung der Karteneinrichtung, deren Volumen im wesentlichen durch die ebene Erstreckung der Karteneinrichtung definiert ist, im Gehäuse der Computer-Maus im wesentlichen auch ohne Auswirkung auf das Bauvolumen der Computer-Maus bleibt.

[0010] Als besonders vorteilhaft für den Betrieb des erfindungsgemäßen handgehaltenen Peripheriesystems erweist es sich, wenn die Karteneinrichtung als Informations- oder Datenträger für Betriebszustands- oder Konfigurationsdaten der Computereinrichtung dient, wobei die Daten über die Leseeinrichtung und die Datenübertragungseinrichtung zur Computereinrichtung übertragen werden.

[0011] Auf diese Art und Weise kann die Datenübertragung von der Karteneinrichtung zur Computereinrichtung beispielsweise dazu genutzt werden, um durch Einführen der Karteneinrichtung in das Gehäuse der Peripherieeinrichtung eine Screensaver-Funktion auszuschalten bzw. durch Entfernen der Karteneinrichtung aus dem Gehäuse der Peripherieeinrichtung die Screensaver-Funktion einzuschalten. Auch ist es möglich, über die Karteneinrichtung Zugriffsberechtigungen zu definieren, so dass in Abhängigkeit von der jeweils in das Gehäuse der Peripherieeinrichtung eingeführten Karte ein Zugriff auf bestimmte Hierarchieebenen der Dateiverwaltung der Computereinrichtung ermöglicht und auf andere Hierarchieebenen verweigert wird. Mittels der in das Gehäuse der Peripherieeinrichtung eingeführten Karteneinrichtung kann unter einer Mehrzahl von parallelen Konfigurationen der Computereinrichtung gewählt werden. Dies kann die Aktivierung oder Deaktivierung bestimmter Ports genauso betreffen wie eine Desktopkonfigurierung.

[0012] Darüber hinaus werden durch Einführen der Karteneinrichtung in das Gehäuse der Peripherieeinrichtung auf besonders komfortable Art und Weise Zugriffsmöglichkeiten oder Zugriffsfunktionen auch auf mit der lokalen Computereinrichtung beispielsweise via Internet verbundene externe Computereinrichtungen möglich. In diesem Zusammenhang kann die Karteneinrichtung im Rahmen des E-Commerce als Kreditkarte oder Autorisierungskarte, bspw. auch zur Auslösung von Signaturfunktionen, verwendet werden. Auch kann der Zugriff auf bestimmte Internetseiten ermöglicht oder auch verweigert werden.

[0013] Erfindungsgemäß weist eine Peripherieeinrichtung, die insbesondere zur Verwendung in dem erfindungsgemäßen handgehaltenen Peripheriesystem geeignet ist, die Merkmale des Anspruchs 3 auf.

[0014] Bei der erfindungsgemäßen handgehaltenen Peripherieeinrichtung, die gattungsgemäß fachsprachlich auch unter dem Begriff "Computer-Maus" bekannt ist, dient das Gehäuse zur Aufnahme einer Karteneinrichtung, die mit einer Chipeinrichtung versehen ist, und zur Aufnahme einer Leseeinrichtung zum Einlesen von in der Chipeinrichtung gespeicherten Daten, wobei eine Kartenaufnahme für die Karteneinrichtung zwischen der Detektoreinrichtung als Bestandteil einer optischen Sensoreinrichtung zur Erfassung

von Navigationsdaten und dem Gehäuseboden innerhalb des Gehäuses angeordnet ist.

[0015] Die erfindungsgemäße Peripherieeinrichtung ermöglicht somit eine platzsparende räumliche Integration der Karteneinrichtung in das Gehäuse, mit der Möglichkeit, die Karteneinrichtung, deren Volumen im wesentlichen durch die ebene Erstreckung des Kartenkörpers definiert ist, parallel zum Gehäuseboden anzuordnen. Diese besonders platzsparende Unterbringung ermöglicht grundsätzlich auch die gleichzeitige Anordnung mehrerer Karteneinrichtungen im Gehäuse der Peripherieeinrichtung, so dass auch nur gemeinschaftlich durch mehrere Karteninhaber ausführbare sicherheitsrelevante Funktionen, wie eine gemeinschaftliche elektronische Signatur, mit der Peripherieeinrichtung ausgelöst werden können.

[0016] Wenn darüber hinaus die Aufnahmeeinrichtung als Einschubaufnahme mit zwei entsprechend der Kartendicke voneinander beabstandet und parallel zueinander angeordneten Führungseinrichtungen ausgebildet ist, wobei die untere Führungseinrichtung durch den Gehäuseboden gebildet ist, ist die Ausbildung der Aufnahmeeinrichtung im Gehäuse auf besonders einfache Art und Weise möglich, da zur Ausbildung der unteren Führungseinrichtung der ohnehin am Gehäuse ausgebildete Gehäuseboden verwendbar ist.

[0017] Wenn das Gehäuse der Peripherieeinrichtung als Schwenkdeckelgehäuse mit einem am Gehäuseboden angeordneten Schwenkdeckel ausgebildet ist, derart, dass bei geöffnetem Schwenkdeckel eine Zugriffsöffnung zum Zugriff auf eine an der Oberseite des Gehäusebodens ausgebildete Kartenaufnahme definiert ist, ist eine allseitig umschließende Unterbringung der Karteneinrichtung im Gehäuse der Peripherieeinrichtung möglich, ohne dass ein Öffnungsschlitz in der Außenfläche des Gehäuses erkennbar wäre.

[0018] Wenn darüber hinaus der Schwenkdeckel oder der Gehäuseboden mit zumindest einem hülsenartigen Eingriffszapfen versehen ist, der zum Eingriff in eine zugeordnete Fensteröffnung in der Karteneinrichtung dient, ist die Ausbildung des Gehäuses nach Art eines Schwenkdeckelgehäuses möglich, wie es beispielsweise zur Aufnahme von Musikkassetten verwendet wird. Hierdurch besteht die Möglichkeit, der Peripherieeinrichtung insgesamt das Erscheinungsbild einer Musikkassettenhülle zu geben, in die vergleichbar mit dem Einlegen oder Herausnehmen einer Musikkassette die Karteneinrichtung eingelegt oder herausgenommen werden kann. Somit kann betreffend die Verwendung der erfindungsgemäßen Peripherieeinrichtung auch ein besonderer Anreiz für solche Benutzer geschaffen werden, die neben einem funktionssicheren Betrieb einer technischen Einrichtung auch zusätzliche "technische Spielereien" schätzen.

[0019] Als besonders vorteilhaft im technischen Betrieb der Peripherieeinrichtung erweist es sich, wenn das Gehäuse mit einer Indikatoreinrichtung zur Anzeige eines Betriebszustands der Computereinrichtung versehen ist. Ein derartiger Betriebszustand kann beispielsweise schon dadurch definiert sein, dass eine Datenverbindung zwischen der Karteneinrichtung und der Computereinrichtung besteht, so dass eine entsprechende Anzeigeeinrichtung bereits anzeigt, ob sich eine Karteneinrichtung im Gehäuse der Peripherieeinrichtung befindet oder nicht.

[0020] Darüber hinaus kann die Indikatoreinrichtung auch zur Bestätigung einer Zugriffsautorisierung dienen, so dass auf eine entsprechende Bildschirmmeldung auf dem Monitor der Computereinrichtung verzichtet werden kann.

[0021] Auch kann die Indikatoreinrichtung verwendet werden zur Anzeige einer Statusänderung betreffend eine externe, mit der Computereinrichtung verbundene weitere Computereinrichtung. So kann die Indikatoreinrichtung beispielsweise dem Benutzer der Computereinrichtung anzeigen, dass eine E-Mail für ihn vorliegt.

[0022] Die Indikatoreinrichtung kann beispielsweise als optische oder akustische Indikatoreinrichtung ausgebildet sein. Gegebenenfalls ergänzt durch einen Bewegungsmelder kann die Peripherieeinrichtung beispielsweise dem sich nähernden Benutzer über eine integrierte Lautsprechereinrichtung den Eingang einer E-Mail, beispielsweise mit der Meldung "you have mail", mitteilen.

[0023] Um besonderen ästhetischen Ansprüchen zu genügen, kann das Gehäuse der Peripherieeinrichtung zumindest teilweise transparent ausgeführt sein.

[0024] Die erfindungsgemäße Karteneinrichtung weist die Merkmale des Anspruchs 12 auf. Die erfindungsgemäße Karteneinrichtung, die insbesondere zur Verwendung im erfindungsgemäßen Peripheriesystem geeignet ist, weist einen im Kartenkörper ausgebildeten Transparenzbereich auf, wobei der Transparenzbereich als Fensteröffnung ausgebildet ist. Diese Fensteröffnung kann derart im Kartenkörper angeordnet sein, dass sie auf einer gemeinsamen optischen Achse mit dem Strahlengang der optischen Sensoreinrichtung der Navigationseinrichtung angeordnet ist. Hierdurch kann bereits durch die räumliche Anordnung des Transparenzbereichs im Kartenkörper eine "Schlüsselfunktion" ermöglicht werden, derart, dass bei einer Positionierung des Transparenzbereichs im Kartenkörper versetzt zum Strahlengang der Navigationseinrichtung die Computer-Maus nicht einsatzfähig ist.

[0025] In einem besonders einfachen Fall kann die Fensteröffnung als Durchgangsöffnung ausgebildet sein.

[0026] Wenn die Fensteröffnung mit einem Medium definierter Transparenz versehen ist, derart, dass die Transparenz des Mediums und die Wellenlänge des von der Lichtemissionseinrichtung emittierten Lichts und/oder der Empfangsbereich der Detektoreinrichtung aufeinander abgestimmt sind, kann die vorgenannte "Schlüsselfunktion" auch dadurch erfüllt werden, dass die Fensteröffnung nur für eine bestimmte Wellenlänge bzw. einen Wellenlängenbereich transparent ist oder die Transparenz der Fensteröffnung und der Empfangsbereich der Detektoreinrichtung für dieselbe Wellenlänge bzw. einen zumindest in einem Bereich übereinstimmenden Wellenlängenbereich gegeben ist.

[0027] Insbesondere betreffen das Erscheinungsbild der Karteneinrichtung erweist sich als vorteilhaft, wenn der Transparenzbereich einen Linsen- oder Irisbereich eines auf einer Kartenoberfläche abgebildeten Auges definiert.

[0028] Wenn der Kartenkörper der Karteneinrichtung zwei Transparenzbereiche aufweist, wobei der erste Transparenzbereich dem von der Lichtemissionseinrichtung emittierten, auf den Untergrund gerichteten Emissionsstrahlengang und der zweite Transparenzbereich dem vom Untergrund reflektierten auf die Detektoreinrichtung gerichteten Reflektionsstrahlengang zugeordnet ist, ist es möglich, das äußere Erscheinungsbild der Karte maßgeblich durch ein "Augenpaar" zu bestimmen, wobei beiden "Augen" eine technische Funktion zukommt.

[0029] Die vorgenannte "Augenpaar"-Lösung für die Gestaltung der Karteneinrichtung kann sich auch in dem Fall als vorteilhaft erweisen, dass für die Navigationseinrichtung zwei optische Sensoreinrichtungen verwendet werden, die jeweils unterschiedlichen Koordinatenachsen zugeordnet sind.

[0030] Nachfolgend werden bevorzugte Ausführungsformen des Peripheriesystems umfassend eine handgehaltene Peripherieeinrichtung und eine Karteneinrichtung anhand der Zeichnungen näher erläutert. Es zeigen:

[0031] **Fig.** 1 ein handgehaltenes Peripheriesystem in Kombination mit einer Computereinrichtung;

[0032] **Fig.** 2 das in **Fig.** 1 dargestellte handgehaltene Peripheriesystem in vergrößerter Einzeldarstellung;

[0033] **Fig.** 3 eine Schnittdarstellung des in **Fig.** 2 dargestellten Peripheriesystems längs dem Schnittlinienverlauf III-III in **Fig.** 2 umfassend eine als Computer-Maus ausgeführte Peripherieeinrichtung und eine Karteneinrichtung;

[0034] **Fig.** 4 die in **Fig.** 3 in die Peripherieeinrichtung eingesetzte Karteneinrichtung in Draufsicht;

[0035] **Fig.** 5 eine weitere Ausführungsform eines Peripheriesystems umfassend eine als Computer-Maus ausgebildete Peripherieeinrichtung und eine Karteneinrichtung;

[0036] **Fig.** 6 die gemäss **Fig.** 5 in die Peripherieeinrichtung eingesetzte Karteneinrichtung in Draufsicht;

[0037] **Fig.** 7 eine Schnittdarstellung der in **Fig.** 6 dargestellten Karteneinrichtung mit eingezeichnetem Strahlengang einer als optische Sensoreinrichtung ausgebildeten Navigationseinrichtung.

[0038] **Fig.** 1 zeigt ein handgehaltenes Peripheriesystem **10**, das über eine hier als Kabelverbindung ausgeführte Datenübermittlungseinrichtung **11** mit einer Computereinrichtung **12** umfassend eine Rechnereinheit **13** und einen Monitor **14** verbunden ist. Die Computereinrichtung **12** kann über eine weitere, beispielsweise als Internet-Verbindung ausgeführte Datenübermittlungseinrichtung **15** mit einer externen Rechnereinrichtung **16**, beispielsweise einem Host-Rechner eines Internetprovider, verbunden sein. Im vorliegenden Fall ist die Computereinrichtung **12** als Desktop-Rechner ausgebildet und befindet sich mit dem Peripheriesystem **10** auf einem gemeinsamen, hier als Tischplatte ausgebildeten Untergrund **17**.

[0039] **Fig.** 2 zeigt das handgehaltene Peripheriesystem **10** umfassend eine als Computer-Maus ausgebildete handgehaltene Peripherieeinrichtung **18** und eine in der Peripherieeinrichtung **18** angeordnete Karteneinrichtung **19**. Wie in **Fig.** 1 dargestellt, kann die Peripherieeinrichtung **18** bzw. das Peripheriesystem **10** über eine als Kabelverbindung ausgeführte Datenübermittlungseinrichtung **11** an die Computereinrichtung **12** angeschlossen sein oder beispielsweise auch über eine sogenannte Bluetooth-Schnittstelle als Datenübermittlungseinrichtung berührungslos mit der Computereinrichtung **12** verbunden sein.

[0040] Im vorliegenden Fall weist die beispielhaft dargestellte, als Computer-Maus ausgebildete Peripherieeinrichtung **18** zwei Maustasten **20** und **21** auf, genauso sind jedoch auch Ausführungen mit mehr oder weniger als zwei Maustasten möglich.

[0041] Bei der in der Peripherieeinrichtung **18** angeordneten Karteneinrichtung **19** handelt es sich im vorliegenden Fall um eine sogenannte kontaktlose Karte, die eine Transpondereinheit **22**, umfassend ein Chipmodul **23** und eine mit dem Chipmodul **23** verbundene Antennenspule **24**, aufweist.

[0042] Die Anordnung bzw. Aufnahme der Karteneinrichtung **19** in der Peripherieeinrichtung **18** sowie den grundsätzlichen Aufbau einer in die Peripherieeinrichtung **18** integrierten Navigationseinrichtung **25** zur Ausführung der Mauszeigerfunktion ist in **Fig.** 3 dargestellt.

[0043] Wie **Fig.** 3 zeigt, befindet sich die Karteneinrichtung **19** in einer an einem Gehäuseboden **26** eines Gehäuses **27** ausgebildeten Kartenaufnahme **28**. Die Kartenaufnahme **28** ist als Einschubaufnahme mit einer an einem rückwärtigen Endbereich **29** des Gehäuses **27** vorgesehenen Einschuböffnung **30** ausgebildet. In der Kartenaufnahme **28** ist die Karteneinrichtung **19** quasi sandwichartig zwischen dem einer Kartenunterseite **31** benachbarten Gehäuseboden **26** und einem einer Kartenoberseite **32** benachbarten Zwischenboden **33** angeordnet. Sowohl im Gehäuseboden **26** als auch im Zwischenboden **33** befindet sich eine, hier als Durchgangsöffnung ausgebildete Fensteröffnung **34** bzw. **35**, deren Funktion nachfolgend noch näher erläutert wird.

[0044] Neben der Navigationseinrichtung **25** befindet sich im Gehäuse **27** eine Leseeinrichtung **36** für den berührungslosen Datenabgriff von auf dem Chipmodul **23** gespeicherten Daten sowie eine Bluetooth-Schnittstelleneinrichtung **37** als Datenübermittlungseinrichtung für die Datenübermittlung zur Computereinrichtung **12** (**Fig.** 1).

[0045] Die Navigationseinrichtung **25** ist als optische Sensoreinrichtung ausgebildet umfassend eine hier als Leuchtdiode ausgebildete Lichtemissionseinrichtung **38** und eine Detektoreinrichtung **39**. Die Detektoreinrichtung **39** weist in einer Rasteranordnung eine Vielzahl einzelner Fotodetektoren **40** auf. Die Ansteuerung der Lichtemissionseinrichtung **38** sowie die Auswertung der Detektorsignale der Detektoreinrichtung **39** erfolgt über eine Mikroprozessoreinheit **41** der Navigationseinrichtung **25**, die zur Übertragung der von der Mikroprozessoreinheit **41** ermittelten Navigationsdaten an die Computereinrichtung **12** mit der Schnittstelleneinrichtung **37** verbunden ist.

[0046] Wie in **Fig.** 3 dargestellt, ist die Peripherieeinrichtung **18** mit ihrem Gehäuseboden **26** auf dem Untergrund **17** angeordnet. Nur aus Gründen der Übersichtlichkeit ist in der zeichnerischen Darstellung gemäß **Fig.** 3 ein Abstand zwischen dem Gehäuseboden **26** und dem Untergrund **17** vorgesehen. Wie aus **Fig.** 3 ersichtlich, weist die Karteneinrichtung **19** in ihrem Kartenkörper **42** ein Kartenfenster **43** auf, das zwischen den Fensteröffnungen **34** und **35** des Gehäuses **27** angeordnet ist, so dass zwischen dem Untergrund **17** und der Lichtemissionseinrichtung **38** einerseits und der Detektoreinrichtung **39** andererseits eine optische Verbindung besteht. Zur Ermittlung von Navigationsdaten, die letztendlich die Koordinaten eines Mauszeigers auf der Bildfläche des Monitors **14** (**Fig.** 1) der Computereinrichtung **12** definieren, wird von der Lichtemissionseinrichtung **38** Licht in einem Emissionsstrahlengang **44** unter einem vorgegebenen Einfallswinkel α auf den Untergrund **17** emittiert. Vom Untergrund **17** wird das Licht in einem Reflektionsstrahlengang **45** auf die Detektoreinrichtung **39** reflektiert. Die sich infolge einer Bewegung der Peripherieeinrichtung **18** gegenüber dem Untergrund **17** verändernden Reflektionseigenschaften werden durch die Rasteranordnung der Photodetektoren **40** in der Detektoreinrichtung **39** erfasst und mittels der Mikroprozessoreinheit **41** in entsprechende Wegkoordinaten umgerechnet. Diese werden als Navigationsdaten über die Schnittstelleneinrichtung **37** an die Computereinrichtung **12** übermittelt. Je nach Ausbildung der Navigationseinrichtung **25** kann es notwendig sein, den Koordinatenachsen der ebenen Bewegung separate Navigationseinrichtungen zuzuordnen, so dass beispielsweise neben der gemäß **Fig.** 3 auf der Längsachse der Peripherieeinrichtung **18** angeordneten Navigationseinrichtung eine weitere auf der Querachse angeordnete Navigationseinrichtung hinzuzufügen ist. Diese weitere Navigationseinrichtung kann dieselbe aus den Fensteröffnungen **34**, **35** und dem Kartenfenster **43** gebildete Fensteranordnung **46** oder eine weitere, hiervon getrennt ausgebildete Fensteranordnung nutzen.

[0047] Wie in **Fig.** 3 schematisch dargestellt, kann die Schnittstelleneinrichtung **37** nicht nur zur Datenübermittlung von der Peripherieeinrichtung **18** an die Computereinrichtung **12**, sondern auch zur Datenübermittlung von der Computereinrichtung **12** an die Peripherieeinrichtung **18** genutzt werden, um beispielsweise eine hier in einer Maustaste **21** als Leuchtdiode ausgebildete Indikatoreinrichtung **47** zu betätigen. Mittels der Indikatoreinrichtung **47** kann beispielsweise über die Verbindung der Computereinrichtung **12** zur externen Rechnereinrichtung **16** der Zugang einer Email angezeigt werden.

[0048] **Fig.** 4 zeigt die Karteneinrichtung **19** in einer Draufsicht, wobei zu erkennen ist, dass das Kartenfenster **43** als kreisrunde, transparente Öffnung ausgebildet ist. Das Kartenfenster **43** kann dabei als Durchgangsöffnung ausgebildet sein oder mit einem Medium definierter Transparenz versehen sein. Im vorliegenden Fall ist das Kartenfenster **43** derart in eine auf der Kartenoberseite abgebildete Augendarstellung **48** integriert, dass das Kartenfenster **43** die von einer Iris **49** umgebene Linse der Augendarstellung **48** bildet.

[0049] **Fig.** 5 zeigt ein handgehaltenes Peripheriesystem **50** mit einer Peripherieeinrichtung **51**, die zwar ebenso wie die Peripherieeinrichtung **18** des Peripheriesystems **10** (**Fig.** 2) als Computer-Maus mit Maustasten **52**, **53** ausgebildet ist. Jedoch ist die Peripherieeinrichtung **51** im Bereich einer Kartenaufnahme **54** gestaltet wie eine Musikkassettenhülle und weist daher in diesem Bereich ein Schwenkdeckelgehäuse **55** auf. Das Schwenkdeckelgehäuse **55** weist einen Gehäuseboden **56** und einen über eine Scharniereinrichtung **57** mit dem Gehäuseboden **56** verbundenen Schwenkdeckel **58** auf. Der Schwenkdeckel **58** ist mit einem Zwischenboden **59** versehen, an dem zum Gehäuseboden **56** gerichtete, hülsenartige Eingriffszapfen **60**, **61** ausgebildet sind. Bei einem Zuschwenken des Schwenkdeckels **58** gegen den Gehäuseboden **56** greifen die Eingriffszapfen **60**, **61** in Kartenfenster **62**, **63** einer mit ihrer Unterseite auf dem Gehäuseboden **56** angeordneten Karteneinrichtung **64** ein. In Überdeckung mit den Kartenfenstern **62**, **63** der Karteneinrichtung **64** sind, wie in **Fig.** 5 mit gestricheltem Linienverlauf dargestellt, im Gehäuseboden **56** Fensteröffnungen **65**, **66** angeordnet. Bei geschlossenem Schwenkdeckelgehäuse **55** ergibt sich somit insgesamt eine übereinander liegende Fensteranordnung **67** bzw. **68**, die sich jeweils aus einer Fensteröffnung **65** bzw. **66**, dem zugeordneten Kartenfenster **62** bzw. **63** und einem jeweils im Zwischenboden **59** angeordneten Hülsenfenster **69** bzw. **70** zusammensetzt.

[0050] Wie **Fig.** 5 ferner zeigt, befinden sich zwischen dem Zwischenboden **59** und dem Deckelboden **71** des Schwenkdeckels **58** Navigationseinrichtungen **72**, **73**, die jeweils einer Fensteranordnung **67**, **68** zugeordnet sind. Die Navigationseinrichtungen **72**, **73** umfassen jeweils, wie in **Fig.** 3 dargestellt, eine hier nicht näher dargestellte Lichtemissionseinrichtung und eine Detektoreinrichtung.

[0051] Als weitere Einrichtungen befinden sich im Schwenkdeckel **58**, wie in **Fig.** 5 schematisch dargestellt, eine Leseeinrichtung **74** zum berührungsfreien Datenabgriff von auf einem Chipmodul **75** gespeicherten Daten, das mit einer Antennenspule **76** zur Ausbildung einer Transpondereinheit **77** verbunden ist, und eine Schnittstelleneinrichtung **78**, die entsprechend der Schnittstelleneinrichtung **37** der Peripherieeinrichtung **18** (**Fig.** 3) ausgebildet sein kann.

[0052] **Fig.** 6 zeigt die Karteneinrichtung **64** in Draufsicht mit den beiden Kartenfenstern **62**, **63**. Wie **Fig.** 6 zeigt, weist die Karteneinrichtung **64** auf ihrer Oberfläche eine bildliche Darstellung eines Augenpaares **79** auf, wobei die Kartenfenster **62**, **63** so angeordnet sind, dass sie jeweils in der Darstellung des Augenpaares **79** eine Linse einer Augendarstellung **81** bilden.

[0053] **Fig.** 7 zeigt in einer schematischen Darstellung die Kombination einer gemäß **Fig.** 6 mit zwei Kartenfenstern **62**, **63** ausgestatteten Karteneinrichtung **64** mit einer Navigationseinrichtung **82**. Wie **Fig.** 7 zeigt, umfasst die Navigationseinrichtung **82** eine Lichtemissionseinrichtung **83** und eine Detektoreinrichtung **84**. Die Relativanordnung zwischen der Lichtemissionseinrichtung **83**, der Detektoreinrichtung **84** und den Kartenfenstern **62**, **63** der Karteneinrichtung **64** ist so gewählt, dass ein Emissionsstrahlengang **85** ausgehend von der Lichtemissionseinrichtung **83** durch das Kartenfenster **63** und eine Fensteröffnung **86** in einem Gehäuseboden **87** einer hier im weiteren nicht dargestellten Peripherieeinrichtung auf den Untergrund **17** auftrifft, und ein vom Untergrund **17** reflektierter Reflektionsstrahlengang **88** durch die Fensteröffnung **86** im Gehäuseboden **87** auf die Detektoreinrichtung **84** trifft.

Patentansprüche

1. Handgehaltenes Peripheriesystem zur Eingabe von Daten in eine Computereinrichtung umfassend einerseits eine Peripherieeinrichtung, insbesondere Computer-Maus, mit einem Gehäuse, einer im Gehäuse angeordneten Navigationseinrichtung zur Erfassung von Navigationsdaten einer Relativbewegung des Gehäuses auf einem Untergrund, einer Datenübertragungseinrichtung zur Datenübergabe von Navigationsdaten an die Computereinrichtung, einer Aufnahmeeinrichtung zur Aufnahme einer Karteneinrichtung sowie einer Leseeinrichtung, und umfassend andererseits eine Karteneinrichtung mit einer Chipeinrichtung, wobei die Leseeinrichtung zum Einlesen von in der Chipeinrichtung gespeicherten Daten dient, **dadurch gekennzeichnet**, dass die Navigationseinrichtung (**25**, **72**, **73**, **82**) eine optische Sensoreinrichtung aufweist mit einer Lichtemissionseinrichtung (**38**, **83**) und einer Detektoreinrichtung (**39**, **84**), das Gehäuse (**27**, **55**) mit einem zumindest in einem ersten Transparenzbereich (**34**, **35**; **65**, **66**; **86**) optisch durchlässigen Gehäuseboden (**26**, **56**, **87**) versehen ist, und die Aufnahmeeinrichtung (**28**, **54**) derart zwischen der Detektoreinrichtung und dem Gehäuseboden angeordnet ist, dass die Karteneinrichtung (**19**, **64**) mit einem zweiten Transparenzbereich (**43**, **62**, **63**) im optischen Strahlengang (**44**, **45**, **85**, **88**) zwischen der Lichtemissionseinrichtung und der Detektoreinrichtung angeordnet ist.

2. Betriebsverfahren für ein Peripheriesystem nach Anspruch 1, dadurch gekennzeichnet, dass die Karteneinrichtung (**19**, **64**) als Informations- oder Datenträger für Betriebszustands- oder Konfigurationsdaten der Computereinrichtung (**12**) dient, die über die Leseeinrichtung (**36**, **74**) und die Datenübertragungseinrichtung (**37**, **78**) zur Computereinrichtung übertragen werden.

3. Handgehaltene Peripherieeinrichtung zur Verwendung in einem handgehaltenen Peripheriesystem nach Anspruch 1, insbesondere Computer-Maus, mit einem Gehäuse, einer oberhalb einer optisch durchlässigen Fensteröffnung in einem Gehäuseboden angeordneten optischen Sensoreinrichtung mit einer Lichtemissionseinrichtung und einer Detektoreinrichtung zur Erfassung von Navigationsdaten einer Relativbewegung des Gehäuses auf einem Untergrund und einer Datenübertragungseinrichtung zur Datenübergabe von Navigationsdaten an die Computereinrichtung, dadurch gekennzeichnet, dass das Gehäuse (**27**, **55**) zur Aufnahme einer Karteneinrichtung (**19**, **64**) aufweisend eine Chipeinrichtung (**23**, **75**) und einer Leseeinrichtung (**36**, **74**) zum Einlesen von in der Chipeinrichtung gespeicherten Daten dient, wobei eine Kartenaufnahme (**28**, **54**) für die Karteneinrichtung zwischen der Detektoreinrichtung (**39**, **84**) und dem Gehäuseboden (**26**, **56**, **87**) innerhalb des Gehäuses angeordnet ist.

4. Peripherieeinrichtung nach Anspruch 3, dadurch gekennzeichnet, dass die Kartenaufnahme (**28**) als Einschubaufnahme mit zwei entsprechend der Kartendicke voneinander beabstandet und parallel zueinander angeordneten Führungseinrichtungen (**26**, **33**) ausge-

bildet ist, wobei die untere Führungseinrichtung durch den Gehäuseboden (**26**) gebildet ist.

5. Peripherieeinrichtung nach Anspruch 3, dadurch gekennzeichnet, dass das Gehäuse als Schwenkdeckelgehäuse (**55**) mit einem an einem Gehäuseboden (**56**) angeordneten Schwenkdeckel (**58**) ausgebildet ist, derart, dass bei geöffnetem Schwenkdeckel eine Zugriffsöffnung zum Zugriff auf die an der Oberseite des Gehäusebodens ausgebildete Kartenaufnahme (**54**) definiert ist.

6. Peripherieeinrichtung nach Anspruch 5, dadurch gekennzeichnet, dass der Schwenkdeckel (**58**) und der Gehäuseboden (**56**) mit zumindest einem hülsenartigen Eingriffszapfen (**60**, **61**) versehen ist, der zum Eingriff in eine zugeordnete Fensteröffnung (**62**, **63**) in der Karteneinrichtung (**64**) dient.

7. Peripherieeinrichtung nach einem der Ansprüche 3 bis 6, dadurch gekennzeichnet, dass das Gehäuse (**27**) mit einer Indikatoreinrichtung (**47**) zur Anzeige eines Betriebszustands der Computereinrichtung (**12**) versehen ist.

8. Peripherieeinrichtung nach Anspruch 7, dadurch gekennzeichnet, dass die Indikatoreinrichtung (**47**) zur Bestätigung einer Zugriffsautorisierung dient.

9. Peripherieeinrichtung nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass die Indikatoreinrichtung (**47**) zur Anzeige einer Statusänderung betreffend eine externe, mit der Computereinrichtung (**12**) verbundene weitere Computereinrichtung (**16**) dient.

10. Peripherieeinrichtung nach einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, dass die Indikatoreinrichtung (**47**) als optische oder akustische Indikatoreinrichtung ausgebildet ist.

11. Peripherieeinrichtung nach einem der Ansprüche 3 bis 10, dadurch gekennzeichnet, dass das Gehäuse (**27**, **55**) zumindest teilweise transparent ausgebildet ist.

12. Karteneinrichtung zur Verwendung in einem handgehaltenen Peripheriesystem nach Anspruch 1, mit einem Kartenkörper und mindestens einem im Kartenkörper ausgebildeten Transparenzbereich, dadurch gekennzeichnet, dass der Transparenzbereich (**43**, **62**, **63**) als Fensteröffnung ausgebildet ist.

13. Karteneinrichtung nach Anspruch 12, dadurch gekennzeichnet, dass die Fensteröffnung als Durchgangsöffnung ausgebildet ist.

14. Karteneinrichtung nach Anspruch 12, dadurch gekennzeichnet, dass die Fensteröffnung mit einem Medium definierter Transparenz versehen ist, derart, dass die Transparenz des Mediums und die Wellenlänge des von der Lichtemissionseinrichtung (**38**, **83**) emittierten Lichts und/oder der Empfangsbereich der Detektoreinrichtung (**39**, **84**) aufeinander abgestimmt sind.

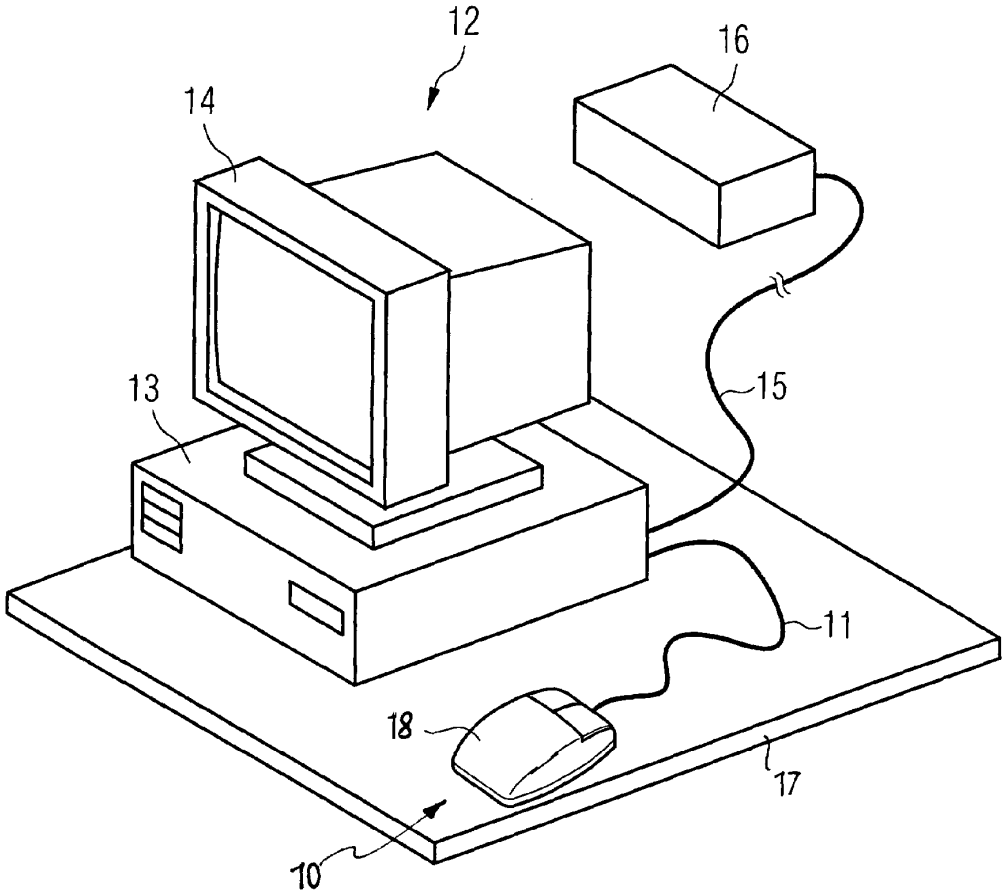
15. Karteneinrichtung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, dass der Transparenzbereich (**43**, **62**, **63**) einen Linsen- oder Irisbereich eines auf einer Kartenoberfläche abgebildeten Auges definiert.

16. Karteneinrichtung nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, dass der Kartenkörper zwei Transparenzbereiche (**62**, **63**) aufweist, wobei der erste Transparenzbereich (**63**) dem von der Lichtemissionseinrichtung (**83**) emittierten, auf den Untergrund (**17**) gerichteten Emissionsstrahlengang (**85**) und der zweite Transparenzbereich (**62**) dem vom Untergrund reflektierten, auf die Detektoreinrichtung (**84**) gerichteten Reflektionsstrahlengang (**88**) zugeordnet ist.

Hierzu 4 Seite(n) Zeichnungen

Nummer: **DE 100 60 866 C1**
Int. Cl.[7]: **G 06 F 3/033**
Veröffentlichungstag: 2. Mai 2002

FIG 1



202 180/99

Nummer: **DE 100 60 866 C1**
Int. Cl.[7]: **G 06 F 3/033**
Veröffentlichungstag: 2. Mai 2002

FIG 2

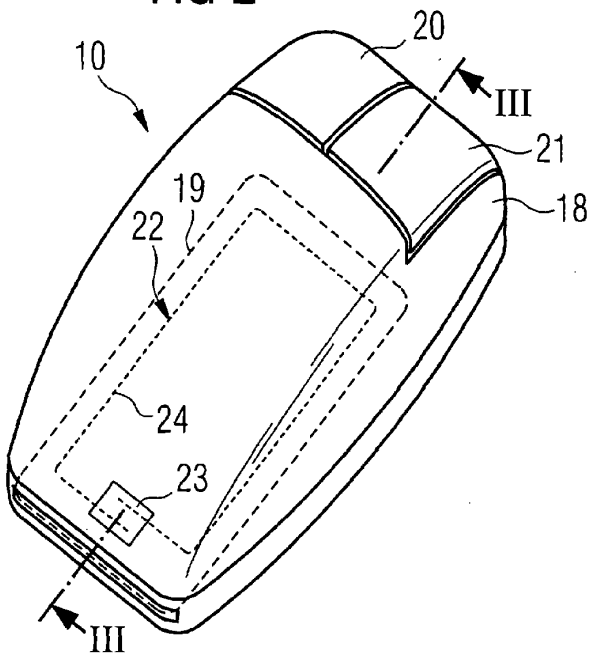
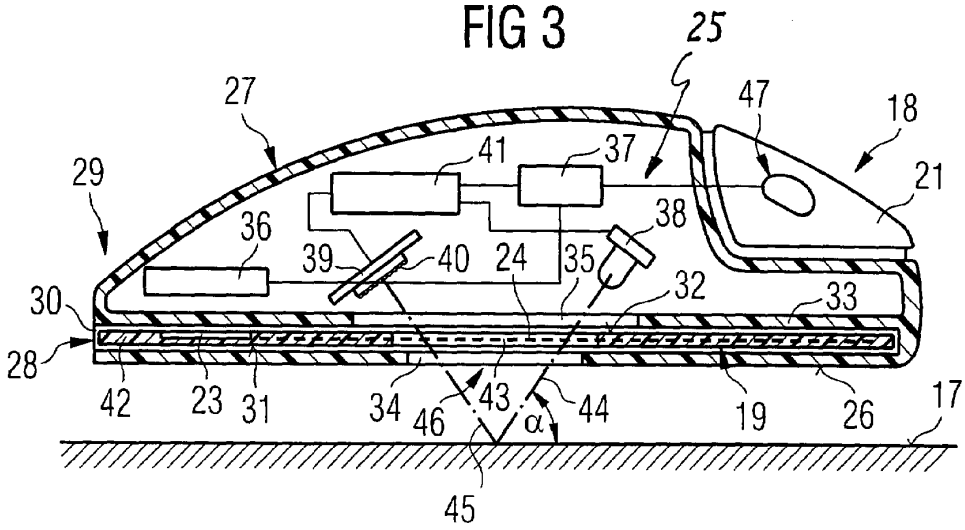


FIG 3



202 180/99

Nummer: **DE 100 60 866 C1**
Int. Cl.[7]: **G 06 F 3/033**
Veröffentlichungstag: 2. Mai 2002

FIG 4

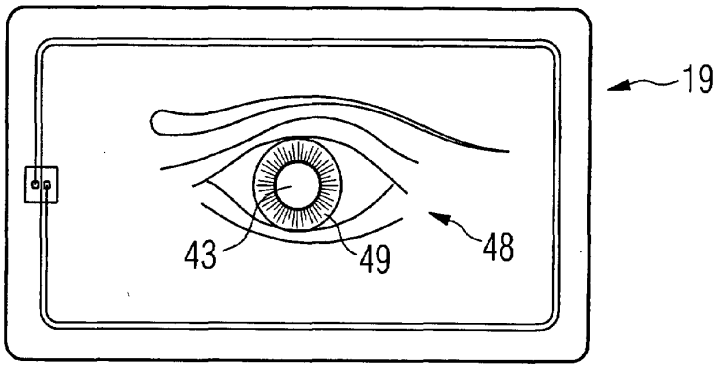
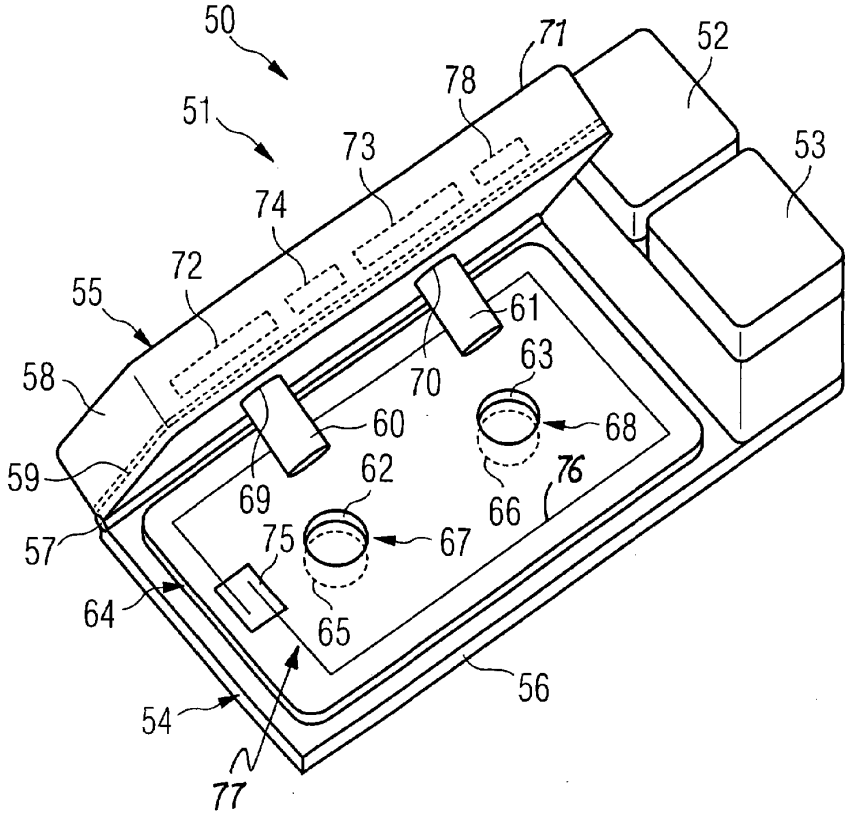


FIG 5



202 180/99

Nummer: **DE 100 60 866 C1**
Int. Cl.[7]: **G 06 F 3/033**
Veröffentlichungstag: 2. Mai 2002

FIG 6

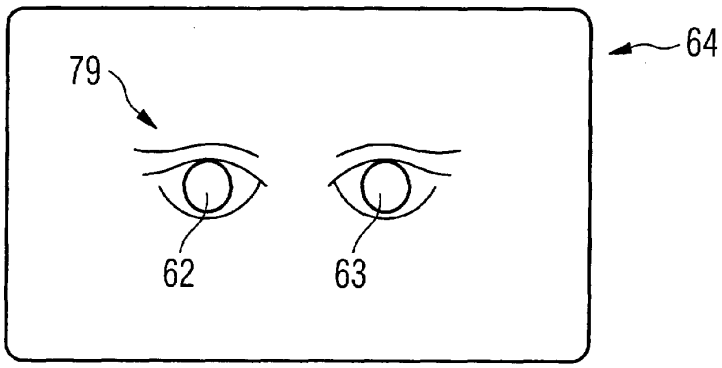
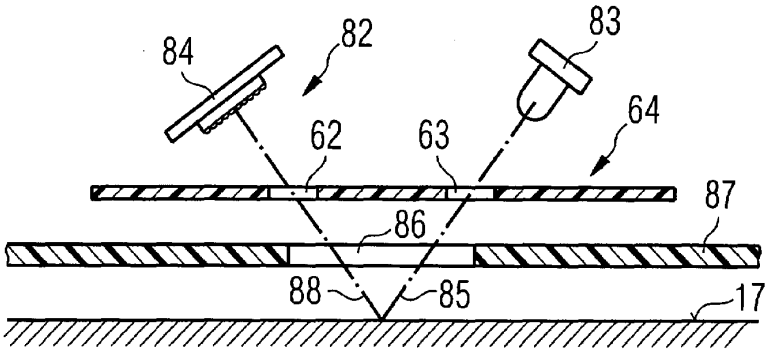


FIG 7



202 180/99

OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Demande-Application**

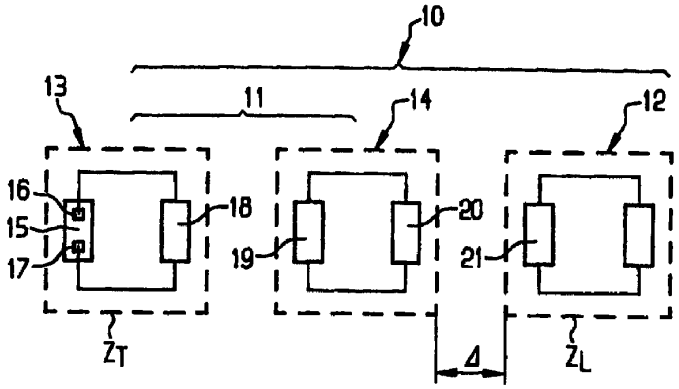
(21) (A1) **2,279,176**
(86) 1998/01/27
(87) 1998/07/30

(72) RIETZLER, MANFRED, DE
(72) WILM, ROBERT, DE
(71) AMATECH ADVANCED MICROMECHANIC & AUTOMATION TECHNOLOGY GMBH & CO. KG, DE
(71) PAV CARD GMBH, DE

(51) Int.Cl.[6] G06K 19/07
(30) 1997/01/28 (197 03 029.7) DE

(54) **MODULE DE TRANSMISSION POUR DISPOSITIF TRANSPONDEUR, ET DISPOSITIF TRANSPONDEUR ET PROCEDE PERMETTANT DE FAIRE FONCTIONNER UN DISPOSITIF TRANSPONDEUR**

(54) **TRANSMISSION MODULE FOR A TRANSPONDER DEVICE, TRANSPONDER DEVICE AND METHOD FOR OPERATING SAID DEVICE**



(57) L'invention concerne un module de transmission (14) pour la transmission de données sans contact entre une puce (15) et un dispositif de lecture (12) comprenant un montage à bobines qui comporte un élément de couplage (19) et au moins une bobine d'antenne (20) qui sont reliés électriquement l'un avec l'autre, l'élément de couplage servant à la réalisation d'un couplage inductif avec une bobine de transpondeur (18) reliée électriquement à la puce, et la bobine d'antenne servant à la réalisation d'une liaison avec le dispositif de lecture. L'élément de couplage, qui se présente sous la forme d'une bobine de couplage (19), et la bobine d'antenne (20) sont conçus différemment en ce qui concerne leurs paramètres de bobine influant sur l'impédance de bobine.

(57) The invention relates to a transmission module (14) for contactless transmission of data between a chip (15) and a reading device (12) with a coil arrangement comprising a coupling element (19) and at least one antenna coil (20) that are electrically interconnected, wherein said coupling element is used to produce inductive coupling with a transponder coil (18) which is electrically connected to the chip, and the antenna coil is used to enable connection to the reading device. The coupling element embodied as a coupling coil (19) and the antenna coil (20) are configured differently with respect to the coil parameters affecting coil impedance.

ABSTRACT

The invention relates to a transmission module (14) for contactless transmission of data between a chip (15) and a reading device (12) with a coil arrangement comprising a coupling element (19) and at least one antenna coil (20) that are electrically interconnected, wherein said coupling element is used to produce inductive coupling with a transponder coil (18) which is electrically connected to the chip, and the antenna coil is used to enable connection to the reading device. The coupling element embodied as a coupling coil (19) and the antenna coil (20) are configured differently with respect to the coil parameters affecting coil impedance.

Transmission module for a transponder device and also a transponder device and method of operating a transponder device

The present invention relates to a transmission module for contact-free data transmission between a chip and a reading device in accordance with Claim 1 or 2 and also to a transponder device comprising a transponder unit and a transmission module according to Claims 11, 12 or 13 and a method of operating a transponder device comprising a transponder unit and a transmission module according to Claim 16 or 17.

Transponder units, which in their simplest form comprise a chip and a transponder coil in contact with the terminal areas of the chip, are used to an increasing extent in quite different fields, wherein they uniformly serve, however, the purpose of ensuring a contact-free or wire-free communication between a reading device disposed more or less remotely from the transponder unit and the chip in order to make possible a data retrieval for the purpose of detecting data stored on the chip. Such transponder units are used, for example, in so-called contact-free chip cards, in coded labels or even for identifying animals for slaughter, in this case used as so-called injection transponders.

The different fields of application of transponder units result in some cases in transmission distances which are extremely mutually different between the respective transponder unit and the associated reading device, which distances accordingly require different operating voltages of the transponder units or of the chip comprised therein. In addition, it has hitherto been necessary to match the layout of the transponder unit to the reading device in each individual case, which, as a rule, makes an impedance matching between the transponder unit and the reading device necessary. From the above it becomes clear that even

on the basis of the two reading parameters, operating voltage and impedance, alone, a multiplicity of differently laid-out transponder units is necessary in order to ensure a reliable operation of the respective transponder unit as a function of the transmission distance and the nature of the associated reading device. These requirements are therefore an obstacle to a fundamentally desirable standardization in the layout of transponder units, which standardization would make possible an essentially cheaper production of transponder units.

The object of the present invention is therefore to make possible the design of a standardized transponder unit regardless of the transmission distance encountered in an individual case or of the respective type of reading device.

This object is achieved by a transmission module having the features of Claim 1 or 2.

According to the invention, a transmission module for the contact-free data transmission between a chip and a reading device is proposed which comprises a coil arrangement having a coupling element and at least one aerial coil which are electrically interconnected, wherein the coupling element serves to produce an inductive coupling to a transponder coil electrically connected to the chip and the aerial coil serves to produce a contact-free connection to the reading device. In this arrangement, the coupling element designed as coupling coil and the aerial coil are of different design in regard to at least one of their coil parameters which influence the coil impedance.

A transmission module which is constructed in this way and which can be combined with the transponder unit by means of inductive coupling consequently makes possible an impedance matching between the reading device and the transponder

unit. That means that, proceeding from a standardized transponder unit, matching can take place to a reading device impedance which is different from the impedance of the transponder unit in that the coupling coil is essentially identical in regard to its impedance to the impedance of the transponder unit, and the aerial coil connected electrically to the coupling coil is matched to the impedance of the reading device in regard to its impedance. Consequently, as a result of an appropriate design of the coil parameters of coupling coil and aerial coil, it is possible to combine one and the same transponder unit with reading devices differing from one another in regard to their impedance. Available as such coil parameters which influence the impedance of the respective coil in the design of the coupling element as coupling coil are, for example, the wire cross section of the coil, the length of the coil wire associated with the respective coil or even the material used to produce the coil wire.

According to the invention, a further possibility of matching a transponder unit to the particular conditions of the individual case in regard to different transmission distances is to provide, according to Claim 2, a transmission module for the contact-free data transmission between a chip and a reading device which comprises a coil arrangement having a coupling element and at least one aerial coil, wherein the coupling element serves to produce an inductive coupling to a transponder coil electrically connected to the chip and the aerial coil to produce a contact-free connection to the reading device, wherein the contact element designed as coupling coil is designed in such a way that the coupling coil serves as primary coil of a transformer formed with the associated transponder coil to induce an increased operating voltage in the chip of the transponder unit.

In the case of this achievement according to the invention, use is accordingly made of the inductive coupling between the coupling coil and the transponder coil in order to form from the coupling coil and the transponder coil a transformer with which the operating voltage in the transponder unit can be increased. Consequently, it becomes possible, proceeding from a transponder unit with a standardized layout, to span different transmission distances as a result of the fact that correspondingly differently laid-out transmission modules are used in such a way that a suitable ratio of the number of turns between the coupling coil and the transponder coil determines the transformation ratio necessary to overcome the respective transmission distance.

In addition to the abovementioned possibility of achieving an increased operating voltage in the transponder unit by a suitable specification of the number of turns/transformation ratio, there is also the possibility of amplifying quite generally the magnetic field of the coupling coil by means of a suitable amplification device in order thereby to achieve a correspondingly increased induction and a voltage increase, associated therewith, in the transponder unit. Such an amplification device may be formed from a voltage source which increases or generates the voltage applied to the coupling coil, that is to say, for instance, by a battery disposed in the transmission module and in contact with the coupling coil. This makes it possible to form an active transmission module which has its own voltage supply.

A further possibility for achieving an amplification effect is to provide the coupling coil with a core made of a permeable material, in particular ferrite, which core increases the magnetic field strength of the coupling coil. The amplification device described above consequently also forms an achievement which is independent of the

achievement of utilizing the coupling coil and the transponder coil to form a transformer.

In a particular embodiment of the transmission module which uses a permeable material rod as core to form an axially aligned magnetic field, the aerial coil serves simultaneously as coupling coil.

To make possible a use of the coil arrangement as transmission module and a simplified application of the coil arrangement on a transponder unit or a substrate of a transponder unit, the coil arrangement is disposed on a carrier film. The term "carrier film" is in this case not to be understood as restrictive in regard to a material choice suitable for the carrier film, that is to say, in contrast to a widespread understanding of the meaning of the term "carrier film", as used here, this term includes not only plastic materials, but also natural materials, such as, for example, cellulose or paper. Here, the term "carrier film" is solely intended to express the fact that a substrate formed as carrier film is essentially determined by its area dimension and has a thickness which is on the negligible side compared with the area dimension.

For certain application cases, for example for producing a chip card provided with such a transmission module, it is advantageous to design the coil arrangement in total as a card inlay.

If the coil arrangement is to be used in coded labels or the like, it proves advantageous if the coil arrangement is formed on an adhesive substrate.

According to Claim 11, the transponder device according to the invention is provided with a transponder unit and a transmission module, wherein the transponder unit comprises a chip having a transponder coil electrically connected to

the chip and the transmission module comprises a coupling element having an aerial coil, wherein the coupling element serves to produce an inductive coupling to the transponder coil, and the aerial coil is electrically connected to the coupling element and serves to produce a contact-free connection to a reading device, wherein, to make possible a matching between the transponder unit and the reading device, the coupling element, designed as coupling coil, and the aerial coil are of different design in regard to at least one of their parameters influencing the coil impedance. The advantages of such a transponder device provided with a transmission module have already been explained in detail at the outset.

Furthermore, according to the invention, a transponder device comprising a transponder unit and a transmission module is proposed according to Claim 12, wherein the transponder unit comprises a chip having a transponder coil electrically connected to the chip and the transmission module comprises a coupling element having an aerial coil, wherein the coupling element serves to produce an inductive coupling to the transponder coil, and the aerial coil is electrically connected to the coupling element and serves to produce a contact-free connection to a reading device, wherein the coupling element is designed as coupling coil and has a comparatively lower number of turns than the transponder coil, in such a way that the coupling coil forms a primary coil and the transponder coil a secondary coil of a transformer.

The advantages of such a transponder device provided with a transmission module in conjunction with a possible increase thereby of the operating voltage of the transponder unit have already been discussed in detail at the outset.

A further transponder device according to the invention is provided, according to Claim 13, with a transponder unit

and a transmission module, wherein the transponder unit comprises a chip having a transponder coil electrically connected to the chip and the transmission module comprises a coupling element having an aerial coil, wherein the coupling element serves to produce an inductive coupling to the transponder coil, and the aerial coil is electrically connected to the coupling element and serves to produce a contact-free connection to a reading device, wherein the coupling element is formed from a permeable material rod, in particular a ferrite core, whose end face serves as coupling surface and the aerial coil is disposed around the material rod.

In a transponder device designed in this way, because of the strongly focused axial alignment of the magnetic field generated by the permeable material rod, a particularly effective and, consequently, low-loss inductive coupling is possible between the transponder coil of the transponder unit and the aerial coil so that, regardless of the possibility described above of impedance matching or step-up transformation of the operating voltage of the transponder unit, this configuration of the transponder device already makes possible an increase in the operating voltage in the transponder unit solely as a result of the particularly low-loss coupling via the material rod.

It proves particularly advantageous that, because of the particularly low-loss inductive coupling between the aerial coil and the transponder coil via the material rod, the configuration described above of the transponder device makes possible the use of a transponder coil which is designed as a chip coil disposed on the surface of the chip. Such chip coils are also known by the term "coil on chip".

In this connection, in a special embodiment of the transponder device, the chip is disposed with its rear side

on the end face of the permeable material rod, and the chip coil disposed on the contact side of the chip opposite the rear side is disposed with its coil surface essentially congruent with the end face of the material rod. This results in an extremely miniaturized transponder device, such as is used, for example, in an injection transponder.

In the method according to the invention of operating a transponder device having a transponder unit comprising a chip and a transponder coil and having a transmission module comprising a coupling coil and an aerial coil electrically connected to the coupling coil, the impedance of the aerial coil matched to a reading device communicating with the transponder unit is converted by means of the transmission module into an impedance of the coupling coil matched to the impedance of the transponder unit.

A further method according to the invention of operating a transponder device having a transponder unit comprising a chip and a transponder coil and having a transmission module comprising a coupling coil and an aerial coil electrically connected to the coupling coil consists in using the coupling coil of the transmission module together with the transponder coil as a transformer which increases the operating voltage in the transponder unit.

Preferred embodiments of the transmission modules according to the invention and also embodiments of transponder devices provided with such transmission modules are explained in greater detail below with respect to the drawings, possible operating modes of such transponder devices being explained.

In the drawings:

Figure 1 shows a diagrammatic view of a data transmission arrangement comprising a transponder device and a reading device;

Figure 2 shows a detail view of the transponder device shown diagrammatically in Figure 1;

Figure 3 shows a sectional view of a chip card constructed in layer technique and provided with a transponder device;

Figure 4 shows a plan view of the transponder device disposed in the chip card shown in Figure 3;

Figure 5 shows a further exemplary embodiment of a transponder device.

Figure 1 shows a data transmission arrangement 10 comprising a transponder device 11 and a reading device 12. The transponder device 11 comprises a transponder unit 13 and a transmission module 14. In the diagrammatic view chosen in Figure 1, the transponder unit 13 comprises a chip 15 and a transponder coil 18 electrically connected to the terminal areas 16, 17 of the chip 15.

The transmission module 14 comprises in the present case a coupling element, designed here as coupling coil 19, and an aerial coil 20 electrically connected to the coupling coil.

The transmission module 14 basically serves to receive the electromagnetic broadcasting power emitted by a broadcasting coil 21 of the reading device 12 via the aerial coil 20 and to transmit it inductively by means of the coupling coil 19 to the transponder coil 18 of the transponder unit 13. In this connection, the coupling coil 19 essentially has the purpose of focusing the electromagnetic field on the transponder coil 18 in order

to achieve as effective an inductive coupling as possible between the coupling coil 19 and the transponder coil 18.

A further function of the transmission module 14 is to effect an increase in the operating voltage of the chip 15 by means of a suitable interaction with the transponder coil 18 in order to make possible an increased transmission distance Δ between the transponder device 11 and the reading device 12.

In addition, the transmission module 14 makes possible a matching of the impedance Z_T of the transponder unit 13 to the impedance Z_L of the reading device 12 as a result of the fact that the coupling coil 19 and the aerial coil 20 are essentially identical in their impedance values to the transponder unit 13 or the reading device 12, respectively, or are matched thereto.

Figure 2 shows, for the purpose of a more detailed explanation of the modes of operation, referred to above, of the transmission module 14, a more detailed view of the transponder device 11 with the transponder unit 13 comprising the chip 15 and the transponder coil 18 and the transmission module 14 comprising the coupling coil 19 and the aerial coil 20.

In the present case, the aerial coil 20 comprises a number of turns n = 8 and the coupling coil 19 comprises a number of turns n = 10. The coupling coil 19 and the aerial coil 20 are connected via electrical conductors 22, 23. Because of the different winding lengths of the coils in conjunction with the number of turns, given otherwise identical coil parameters which influence the coil impedance of the coupling coil 19 and the aerial coil 20, the coupling coil 19 has, in the present case, a lower impedance than the aerial coil 20. Accordingly, the design of the transmission module 14 shown in Figure 2 can be

designed, for example, so that the coupling coil 19 is matched to the relatively low impedance of the transponder unit 13 and the aerial coil 20 is matched to the relatively high impedance of a reading device, which is not shown in greater detail here, so that it becomes possible by means of the transmission module 14 to connect a high-resistance reading device to a low-resistance transponder unit without the transponder unit itself, that is to say the transponder coil 18, having to be matched directly in terms of impedance for this purpose.

In the embodiment of the transmission module 14 shown in Figure 2, in addition, an interaction of the coupling coil 19 provided with a relatively low number of turns n = 10 with the transponder coil 18 comprising a relatively high number of turns n = 20 produces a transformer effect via the inductive coupling indicated here by a diagrammatic field line pattern 24 in such a way that the coupling coil 19 and the transponder coil 18 act as primary coil and secondary coil, respectively, of a transformer 25, with the consequence that a comparatively increased voltage is induced in the transponder coil 18, as a result of which a correspondingly increased operating voltage is available for the chip 15.

Figure 3 shows a transmission module 26 in an embodiment as a card inlay in a chip card 27 formed in layer technique.

In addition to the transmission module 26, the further layers are formed from a chip inlay 28 having a chip 29 accommodated therein, a transponder coil inlay 30 having a transponder coil 31 embedded therein and in contact with the chip 29 and two outer top layers 32 and 33 disposed in each case on the chip inlay 28 or the transmission module 26. The chip inlay 28 and the transponder coil inlay 30 form, in the present case, a transponder device 49.

Figure 4 shows the transmission module 26 in a plan view, with a coupling coil 34 and an aerial coil 35 which are interconnected via conductors 36, 37 and are disposed here on a common carrier layer 38 designed as thin-film substrate, which carrier layer may be composed in the present case of a polyimide film.

Both the transponder coil 31 and the coupling coil 34, and the aerial coil 35 may be formed as wire coils and also as coils produced in another way.

Figure 5 shows a transponder device 39 comprising a transponder unit 40, which is formed from a chip 41 and a transponder coil 43 disposed directly on the contact surface 42 provided with terminal areas. In specialist language, such coil arrangements are also described by the term "coil on chip" and can be produced in an etching or shearing process.

The transponder device 39 comprises a transmission module 44 which is composed of a short-circuited aerial coil 46 disposed around a ferrite core 45. As a departure from the transmission modules 14 and 26 shown in Figures 2 and 4, the electromagnetic field picked up by the aerial coil 46 is focused in the case of the transmission module 44 on the transponder coil 43 not by means of a coupling coil, but by means of the ferrite core 45 which strongly focuses the magnetic field and aligns it axially.

As shown in Figure 5, the transponder device 39 makes possible a construction in which the chip 41 can be positioned by means of its rear side 47 directly on an end face 48 of the ferrite core 45. To achieve as effective an inductive coupling as possible between the ferrite core 45 and the transponder coil 43, the chip 41 is disposed on the end face 48 of the ferrite core 45 in such a way that the end face 48 from which the magnetic field is essentially

emitted and the transponder coil 43 are in a congruent position.

The transponder device shown in Figure 5 is particularly suitable for use as a so-called injection transponder in which the transponder device 39 is disposed in a hermetically sealed manner in an injection container which is formed, for example, from glass and which can be used, for example, when subcutaneously injected as transponder for identifying animals to be slaughtered.

1. Transmission module (14, 26) for the contact-free data transmission between a chip (15, 29) of a transponder unit (49) and a reading device (12) having a coil arrangement which comprises a coupling coil (19, 34) and at least one aerial coil (20, 35) which are electrically interconnected, wherein the coupling coil serves to produce an inductive coupling (24) to a transponder coil (18, 31) electrically connected to the chip and the aerial coil serves to produce a connection to the reading device, and the coupling coil (19, 34) and the aerial coil (20, 35) are of different design in regard to their coil parameters influencing the coil impedance, characterized in that the coupling coil (19, 34) and the aerial coil (20, 35) are disposed on a common carrier layer (38), in such a way that the coil arrangement, together with the carrier layer, forms a unit which can be used independently of the transponder unit.

2. Transmission module according to Claim 1, characterized in that the coil arrangement (34, 35) on the carrier layer (38) forms a card inlay (30) of a chip card constructed in layer technique.

3. Transmission module according to Claim 1 or 2, characterized in that the carrier layer (38) is designed as carrier film.

4. Transmission module according to one or more of the preceding claims, characterized in that the carrier layer is designed as adhesive substrate.

5. Transmission module (44) for the contact-free data transmission between a chip (41) of a transponder unit (40) and a reading device having a coil

arrangement which comprises a coupling element (45) and at least one aerial coil (20, 35, 46), wherein the coupling element serves to produce an inductive coupling to a transponder coil (43) electrically connected to the chip and the aerial coil serves to produce a connection to the reading device, characterized in that the coupling element is designed as a permeable material rod which is surrounded by the aerial coil in such a way that the material rod serves as substrate for the aerial coil and the material rod, together with the aerial coil, forms a unit which can be used independently of the transponder unit.

6. Transponder device (39) comprising a transponder unit (40) and a transmission module (44), wherein the transponder unit comprises a chip (41) with a transponder coil (43) electrically connected to the chip and the transmission module comprises a coupling element (45) having an aerial coil (46), wherein the coupling element serves to produce an inductive coupling to the transponder coil, and the aerial coil serves to produce a contact-free connection to a reading device (12), characterized in that the coupling element is formed from a permeable material rod (45) whose end face (48) serves as coupling surface, and the aerial coil (46) is disposed around the material rod (45).

7. Transponder device according to Claim 6, characterized in that the transponder coil is designed as a "coil-on-chip" chip coil (43) disposed on the surface (42) of the chip (41).

8. Transponder device according to Claim 6 or 7, characterized in that the chip (41) is disposed

with its rear side (47) on the end face (48) of the permeable material rod (45) and the chip coil (43) disposed on the contact surface (42) of the chip (41) opposite the rear side (47) is disposed with its coil surface essentially congruent with the end face (48) of the material rod (45).

FIG 1

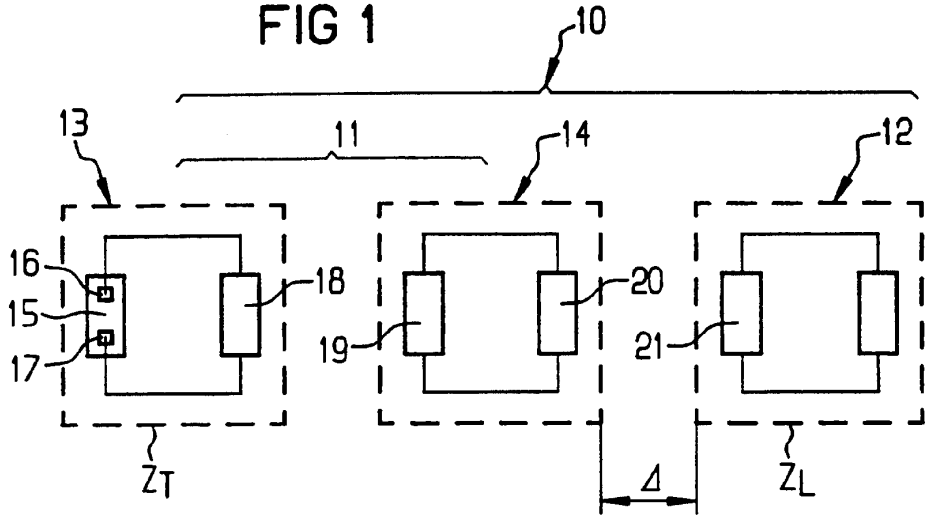

10
11
12
13
14
15
16
17
18
19
20
21
ZT
Δ
ZL

FIG 2

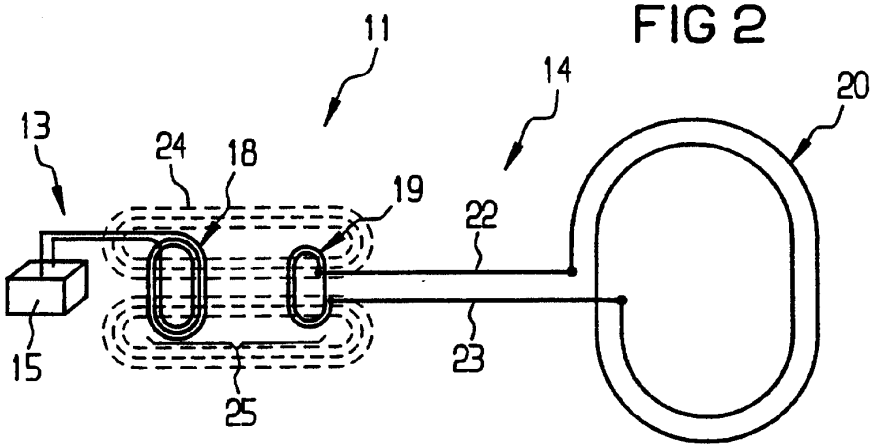

11
13
14
15
18
19
20
22
23
24
25

FIG 3

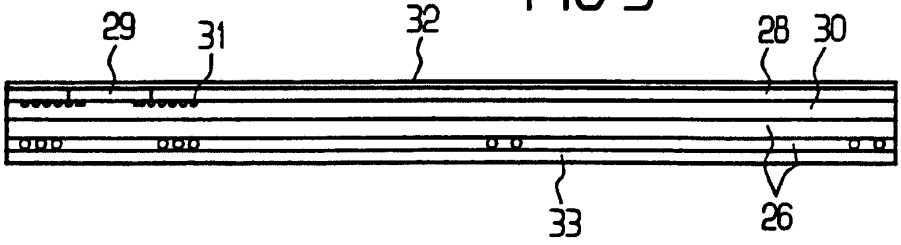


FIG 4

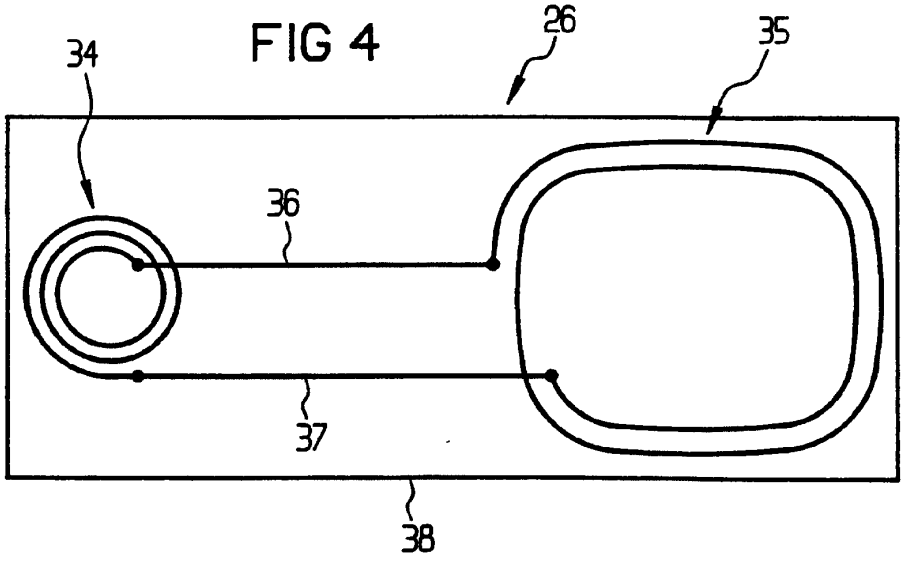
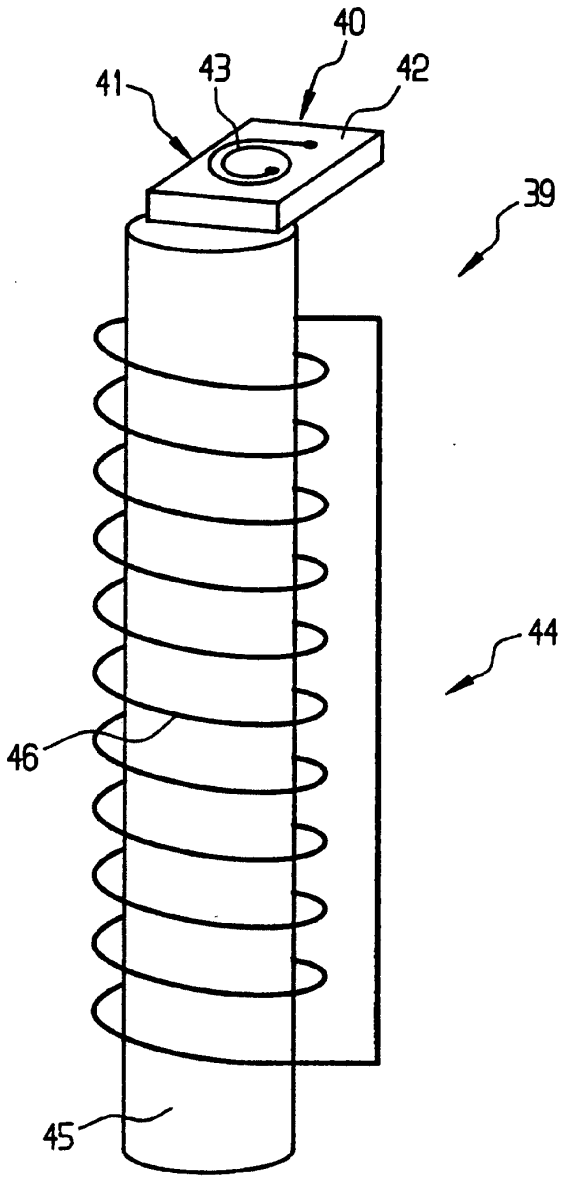


FIG 5



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 101 40 662 C 1**

(51) Int. Cl.[7]: **G 06 K 19/077**

(21) Aktenzeichen: 101 40 662.2-53
(22) Anmeldetag: 24. 8. 2001
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 20. 3. 2003

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
ORGA Kartensysteme GmbH, 33104 Paderborn, DE

(74) Vertreter:
Quermann & Richardt Patentanwälte, 65195 Wiesbaden

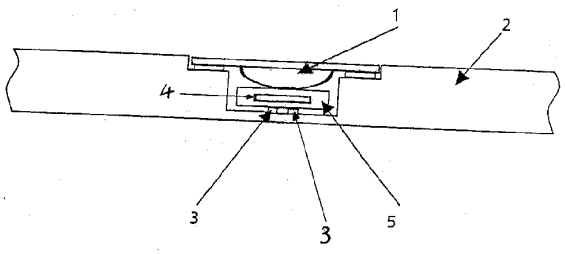
(72) Erfinder:
Osterwald, Frank, Dr.-Ing., 24103 Kiel, DE; Senge, Carsten, Dipl.-Ing., 24105 Kiel, DE; Mentzer, Rüdiger, Dipl.-Ing., 24783 Osterrönfeld, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE	197 00 848 C1
DE	199 35 528 A1
DE	199 14 587 A1
DE	196 45 083 A1
DE	42 05 556 A1
WO	99 16 019 A1

(54) Chipkarte mit integriertem Schalter

(57) Die Erfindung betrifft eine Chipkarte mit integriertem Schalter mit
- einer Kavität,
- einem in der Kavität fixierten Kontaktpaar 3,
- einer in der Kavität angeordneten Kontaktbrücke 4 zum Schließen eines Kontaktes zwischen dem Kontaktpaar 3,
- einem in die Kavität hineinragenden Modul,
so dass bei Ausübung eines äußeren Drucks auf das Modul die Kontaktbrücke 4 gegen das Kontaktpaar 3 gedrückt wird.



DE 101 40 662 C 1

DE 101 40 662 C 1

Beschreibung

[0001] Die Erfindung betrifft eine Chipkarte mit integriertem Schalter sowie ein Verfahren zur Freigabe einer Transaktion mittels einer Chipkarte, insbesondere für die elektronische Bezahlung.

[0002] Aus dem Stand der Technik sind verschiedene Chipkarten mit integrierten Schaltern bekannt: Aus der DE 199 14 587 A1 ist eine Chipkarte mit einer Tastatur mit einzelnen Tastenfeldern bekannt. Mit Hilfe der einzelnen Tastenfelder kann der Benutzer der Chipkarte dem integrierten Halbleiterbaustein Informationen zukommen lassen, die dieser dann verarbeitet und gegebenenfalls über eine Datenübertragungsvorrichtung anderen ergänzenden Einrichtungen zuleitet.

[0003] Aus der WO 99/16019 ist ein tragbarer Datenträger, insbesondere eine Chipkarte, mit Aktivierungsschalter bekannt. Zwischen einer Antenne und einem Halbleiterchip der Chipkarte ist ein durch einen Benutzer betätigbarer Schalter angeordnet, so dass ein Empfang von Daten nur nach einer Betätigung des Schalters möglich ist.

[0004] Aus der DE 197 00 848 C1 ist eine elektrische Schalteinrichtung für eine Smart Card bekannt. Die Schalteinrichtung kann so in die Smart Card integriert werden, dass diese von außen nicht sichtbar ist. Auf der Außenseite des Gehäuses der Smart Card muss dann im Bereich des Schaltelementes eine Markierung angebracht werden, damit der Benutzer weiß, auf welche Stelle er drücken muss, um einen Schaltvorgang durchzuführen.

[0005] Aus der DE 42 05 556 A1 ist eine Chipkarte mit externem Sicherheitsschalter bekannt. Der Schalter ist in die Chipkarte eingebaut, so dass er von außen bedienbar ist und es dem Nutzer der Karte gestattet, in die Funktion der Elektronik einzugreifen. Mit diesem Schalter kann die auf der Karte befindliche Stromquelle (Akku oder Batterie, aber auch Kondensator) ein- und ausgeschaltet werden. Derart bestimmt der Nutzer wahlfrei, wann die Karte ihre Signale abgibt. Dadurch ist eine definierte Sperrung sowie die Aktivierung in Notsituationen möglich. Zwei auf der Oberfläche der Karte erkennbare Ausprägungen des Schalters offenbaren die Schalterstellung für den Benutzer.

[0006] Aus der DE 199 35 528 A1 ist ferner ein Tastschalter für Chipkarten bekannt, der in einem Kontaktbereich eine flexible Schaltmembran mit elektrisch leitender Kontaktfläche beinhaltet. Die Kontaktfläche weist im unbelasteten Zustand der Schaltmembran zu dem Kontaktbereich einen Abstand auf. Die flexible Schaltmembran hat eine Wölbung, beispielsweise einen geprägten Dom, der den Kontaktbereich überspannt.

[0007] Den aus dem Stand der Technik bekannten Chipkarten mit Schaltern ist der Nachteil gemeinsam, dass für den Schalter und das Chipkartenmodul zwei unterschiedliche Kavitäten in der Chipkarte vorhanden sein müssen. Außerdem muss zumindest eine Markierung für die Position des Schalters auf der Oberfläche der Chipkarte angebracht sein, um dem Nutzer die Tastfläche und/oder die Schalterstellung zu signalisieren. Dadurch wird der beispielsweise für den Aufdruck von Werbung auf der Oberfläche der Chipkarte zur Verfügung stehende Bereich eingeschränkt.

[0008] Aus der DE 196 45 083 A1 ist eine kontaktlose Chipkarte mit Transponderspule bekannt. Die Transponderspule ist in dem Kartenkörper angeordnet und weist ein Anschlusskontaktpaar auf. Das Chipmodul der Chipkarte hat ein entsprechendes Paar Anschlussflächen. Zwischen den Anschlussflächen des Chipmoduls und den Anschlusskontakten befindet sich ein Schaltelement aus druckempfindlich leitenden Gummimatten.

[0009] Zur Betätigung des Schalters wird das Chipmodul heruntergedrückt, so dass über das Schaltelement ein Kontakt jeweils zwischen einer Anschlussfläche des Chipmoduls und einem Anschlusskontakt der Spule hergestellt wird. Auf diese Art und Weise wird die Spule an einen Ausgang des Chipmoduls geschaltet, so dass die Spule von dem Chipmodul angesteuert werden kann.

[0010] Nachteilig bei dieser vorbekannten Chipkarte ist insbesondere, dass Kontakte sowohl innerhalb der Kavität als auch an dem Chipmodul angeordnet sein müssen. Dies ist fertigungstechnisch sehr aufwendig und kostspielig. Ein weiterer wesentlicher Nachteil ist, dass für die Aktivierung der Transponderspule der Tastschalter ständig betätigt werden muss. Für den Benutzer ist jedoch nicht erkennbar, welchen Zeitraum das Absenden einer Information von dem Chipmodul über die Transponderspule benötigt, so dass es zu Fehlfunktionen kommen kann. Ferner ist auch die Notwendigkeit, den Tastschalter für eine längere Zeit herunterdrücken zu müssen, für den Benutzer unbequem.

[0011] Der Erfindung liegt daher die Aufgabe zu Grunde, eine verbesserte Chipkarte mit integriertem Schalter sowie ein verbessertes Verfahren zur drahtlosen Übertragung einer Information, beispielsweise für die drahtlose Bezahlung, zu schaffen.

[0012] Die der Erfindung zu Grunde liegende Aufgabe wird mit den Merkmalen der unabhängigen Patentansprüche jeweils gelöst.

[0013] Bevorzugte Ausführungsformen der Erfindung sind in den abhängigen Ansprüchen angegeben.

[0014] Die vorliegende Erfindung erlaubt es, die Funktion eines Schalters, insbesondere eines Tasters, in die Modulkavität einer Chipkarte zu integrieren. Dies hat den Vorteil, dass die gesonderte Montage eines kostenintensiven gesonderten Elements der Karte entfallen kann, in dem die Herstellungsschritte von Modulkavität und Tasterkavität zusammengeführt werden. Ein weiterer Vorteil ist, dass durch den Schalter die zur Aufbringung einer Werbefläche zur Verfügung stehende Kartenoberfläche nicht beschränkt wird.

[0015] Die Erfindung erlaubt es einem Benutzer, durch kurzzeitige Betätigung des Schalters, d. h. durch Ausübung eines äußeren Drucks auf das Modul der Chipkarte, eine Eingabe vorzunehmen, beispielsweise zur Eingabe einer Willensbekundung oder -erklärung. Durch die kurzfristige Betätigung des Schalters zur Eingabe einer Willenserklärung ist es daher möglich, dass der integrierte Schaltkreis des Moduls nach Empfang eines entsprechenden Impulses eine Transaktion frei gibt und entsprechende Daten überträgt.

[0016] Beispielsweise kann es sich hierbei um eine drahtlose Transaktion handeln. Hierfür ist die Ausbildung der erfindungsgemäßen Chipkarte als sogenannte Dual-interface-Karte vorteilhaft.

[0017] Ein bevorzugter Anwendungsfall hierfür ist die drahtlose Bezahlung, beispielsweise für die Entrichtung des Fahrpreises im öffentlichen Nahverkehr. Zunächst wird hierzu die Chipkarte über deren kontaktbehaftetes Interface mit einem Geldguthaben geladen. Die Entrichtung des Fahrpreises erfolgt dann bei Passieren eines entsprechenden drahtlosen Kartenlesegerätes, wenn gleichzeitig der Schalter durch den Benutzer kurzfristig betätigt wird. Dies hat den Vorteil, dass z. B. beim mehrfachen Passieren desselben oder unterschiedlicher Kartenlesegeräte durch den Benutzer der Fahrpreis nicht mehrfach automatisch abgebucht wird, sondern nur nach Bestätigung der Transaktion durch Drükken des Schalters seitens des Benutzers.

[0018] Die Erfindung ist aber keineswegs auf solche drahtlosen Anwendungen beschränkt. Vielmehr erlaubt es die Erfindung auch über den integrierten Schalter in der

Chipkarte andere beliebige Kartenfunktionen zu aktivieren oder zu deaktivieren, beispielsweise Anzeigevorrichtungen, die Stromversorgung, Sensorfunktionen etc.

[0019] Von besonderem Vorteil bei der vorliegenden Erfindung ist, dass lediglich ein Kontaktpaar entweder fest innerhalb der Kavität angeordnet oder an dem Modul selbst für die Realisierung der Schaltfunktion notwendig ist. Dies hat insbesondere große fertigungstechnische Vorteile. Bei der Ausführung des Moduls in Flip-Chip-Technologie ist es besonders vorteilhaft, das Kontaktpaar an der Unterseite des Moduls zu integrieren, in dem es beispielsweise in einer Metallisierungsschicht des Trägers des Chips angeordnet wird. Dies erlaubt eine besonders kostengünstige und flache Ausführung des mit dem Modul integrierten Tasters.

[0020] Im Weiteren wird eine bevorzugte Ausführungsform der Erfindung mit Bezugnahme auf die Zeichnungen beschrieben. Es zeigen:

[0021] **Fig.** 1 Eine erste Ausführungsform der Erfindung, bei der das Kontaktpaar in der Kavität angeordnet ist,

[0022] **Fig.** 2 eine zweite Ausführungsform der Erfindung, bei der das Kontaktpaar an dem Modul angeordnet ist,

[0023] **Fig.** 3 eine bevorzugte Ausführungsform eines erfindungsgemäßen Verfahrens zur Eingabe einer Information in die Chipkarte.

[0024] Die **Fig.** 1 zeigt ein Modul **1** welches in der Kavität eines Kartenkörpers **2** einer Chipkarte angeordnet ist. Dabei können unterschiedlichte Arten von Modulen verwendet werden, beispielsweise sogenannte TAB Module, Chip-on-flex-Module oder Flip-Chip-Module. Solche Module sind an sich aus dem Stand der Technik bekannt, vergleiche hierzu "Handbuch der Chipkarten", Wolfgang Ranke, Wolfgang Effing, Karl-Hanser Verlag **1999**, insbesondere Kapitel 3.2.2, Seite 71 ff.

[0025] Unterhalb des Moduls **1** befindet sich in der Kavität eine Kontaktbrücke. In dem Beispiel der **Fig.** 1 ist die Kontaktbrücke durch einen Metallbügel **4**, der von Silikon **5** umschlossen ist, gebildet. Bei dem Silikon **5** handelt es sich um ein isotrop leitfähiges Silikonformteil.

[0026] Alternativ kann auch ein isotrop leitfähiges Gummiformteil zur Einbettung des Metallbügels **4** verwendet werden. Es ist ferner ebenfalls möglich, auf dem Metallbügel **4** zu verzichten, so dass die Kontaktbrücke nur durch das isotrop leitfähige Silikon- oder Gummimaterial gebildet wird. Ebenso ist es möglich, die Kontaktbrücke lediglich durch einen Metallbügel zu realisieren.

[0027] Auf dem Boden der Kavität des Kartenkörpers **2** befinden sich zwei Kontakte **3**, die ein Kontaktpaar bilden.

[0028] Zur Betätigung des Tastschalters übt der Benutzer auf die Oberfläche des Moduls **1** einen Druck aus, so dass die Kontaktbrücke, d. h. der in das Silikon **5** eingebettete Metallbügel **4**, gegen die Kontakte **3** gedrückt wird. Dadurch wird eine leitfähige Verbindung zwischen den Kontakten **3** hergestellt, d. h. die Kontakte **3** werden kurzgeschlossen.

[0029] Durch den Kurzschluss der Kontakte **3** wird ein Impuls erzeugt, der durch Eingabe in den integrierten elektronischen Schaltkreis des Moduls **1** entsprechende Aktionen auslöst, beispielsweise eine Transaktion freigibt. Die Eingabe des Impulses kann durch eine in der **Fig.** 1 nicht gezeigte Leitungsverbindung von den Kontakten **3** zu dem Modul **1** erfolgen.

[0030] Die **Fig.** 2 zeigt eine alternative Ausführungsform der Erfindung. Elemente der **Fig.** 2, die Elementen der **Fig.** 1 entsprechen, sind mit denselben Bezugszeichen bezeichnet.

[0031] Im Gegensatz zu dem Modul der **Fig.** 1 ist das Modul **1** der **Fig.** 2 in sogenannter Flip-Chip-Technologie realisiert; zur Flip-Chip-Technologie vergleiche "Handbuch der Chipkarten", Wolfgang Ranke, Wolfgang Effing, Carl-Hanser Verlag **1999**, Seiten 572, 573.

[0032] Im Gegensatz zu der Ausführungsform der **Fig.** 1 befinden sich Kontakte **6** an dem Modul **1**. Die Kontakte **6** können beispielsweise in einer Metallisierungsebene des Trägers des Chips des Moduls **1** realisiert werden, oder in einem gesonderten Fertigungsschritt auf die der Kontaktbrücke zugewandten Seite des Chips bzw. des den Chip umhüllenden Materials aufgebracht sein.

[0033] Wenn ein Druck auf das Modul **1** zur Betätigung des Tasters ausgeübt wird, werden die Kontakte **6** gegen die Kontaktbrücke, d. h. gegen den in dem Silikon **5** eingebetteten Metallbügel **4**, gedrückt. Dadurch wird eine leitfähige Verbindung zwischen den Kontakten **6** hergestellt, d. h. diese werden kurzgeschlossen.

[0034] Durch diesen Kurzschluss kann ein Impuls erzeugt werden. Zur Erzeugung des Impulses sind in dem gezeigten Ausführungsbeispiel der **Fig.** 2 die Kontakte **6** über Leiterbahnen auf einer Metallisierungsebene des Trägers mit einem Eingang des Chips verbunden. Der durch das Niederdrücken des Moduls **1** erzeugte Kurzschluss zwischen den Kontakten **6** wird dann als Eingangsimpuls in den integrierten Schaltkreis des Chips des Moduls **1** eingegeben. Beispielsweise hat die Änderung der Eingangsimpedanz in dem integrierten Schaltkreis die Erzeugung eines entsprechenden Impulses zur Folge. Daraufhin kann durch den integrierten Schaltkreis eine programmgesteuerte Aktion ausgelöst werden, beispielsweise für die Freigabe und/oder Durchführung einer Transaktion.

[0035] Von besonderem Vorteil bei der Ausführungsform der **Fig.** 2 ist, dass die Verwendung der Flip-Chip-Technologie einen besonders flachen Aufbau des Moduls und des Schalters erlaubt. Dies erlaubt es auch weitere Formteile für die Tasterfunktion und/oder andere Funktionen in der Kavität unterzubringen.

[0036] Ferner ist vorteilhaft, dass die Flip-Chip-Technologie die Erzeugung der kurzzuschließenden Kontakte **6** mittels Siebdruck auf der Chiprückseite erlaubt.

[0037] Sowohl in der Ausführungsform der **Fig.** 1 als auch der **Fig.** 2 kann die Aktivierung des integrierten Schaltkreises beispielsweise zur Freigabe einer Transaktion sowohl als "active high" oder als "active low" ausgeführt sein. Das heißt, der integrierte Schaltkreis kann je nach Ausführungsform entweder bei gedrücktem Taster (active high) oder bei ungedrücktem Taster (active low) aktiviert werden.

[0038] Die **Fig.** 3 zeigt ein Flußdiagramm zur Eingabe einer Information in eine erfindungsgemäße Chipkarte für eine elektronische Transaktion. In dem Schritt **30** wird zunächst der Schalter durch den Benutzer betätigt, um beispielsweise seinen Willen zur Freigabe einer bestimmten Transaktion, zum Beispiel der Entrichtung eines Fahrpreises, zu bekunden. Hierbei genügt eine kurzfristige Betätigung des Schalters, d. h. es ist nicht erforderlich, den Schalter ständig gedrückt zu halten, bis die Transaktion abgeschlossen ist. Jedoch schadet auch eine längerfristige Betätigung des Schalters nicht, da in jedem Fall nur ein elektrisches Signal, z. B. ein einzelner Impuls, in dem nachfolgenden Schritt **31** erzeugt wird.

[0039] Vorzugsweise erfolgt die Impulserzeugung durch den integrierten Schaltkreis des Moduls selbst, wenn durch die Betätigung des Schalters einer von dessen Eingängen kurzgeschlossen wird. Durch einen solchen Kurzschluß wird eine Information, beispielsweise die besagte Willensbekundung des Benutzers eingegeben, so dass der integrierte Schaltkreis eine entsprechende Transaktion freigibt.

[0040] In dem Schritt **32** wird eine entsprechende Aktion in dem integrierten Schaltkreis zur Durchführung der Transaktion ausgelöst. Zur Durchführung der Transaktion werden beispielsweise in dem Schritt **33** nach Starten eines entspre-

chenden Programmmoduls des integrierten Schaltkreises, der beispielsweise als Mikrocontroller ausgebildet sein kann, entsprechende Daten vorzugsweise drahtlos ausgesendet, um von einem Empfänger, zum Beispiel einem Kartenlesegerät, empfangen und ausgewertet zu werden.

Bezugszeichenliste

1 Modul
2 Kartenkörper
3 Kontakte
4 Metallbügel
5 Silikon
6 Kontakte

Patentansprüche

1. Chipkarte mit integriertem Schalter mit einer Kavität, einem in der Kavität fixierten Kontaktpaar (**3**), einer in der Kavität angeordneten Kontaktbrücke (**4**) zum Schließen eines Kontaktes zwischen dem Kontaktpaar (**3**), einem in die Kavität hineinragenden Modul, so dass bei Ausübung eines äußeren Drucks auf das Modul die Kontaktbrücke (**4**) gegen das Kontaktpaar (**3**) gedrückt wird.

2. Chipkarte mit integriertem Schalter nach Anspruch 1, bei der das Kontaktpaar (**3**) in einem unteren Bereich der Kavität angeordnet ist.

3. Chipkarte mit integriertem Schalter mit einer Kavität, einem in die Kavität hineinragenden Modul, einem an dem Modul fixierten Kontaktpaar (**6**), einer in der Kavität angeordneten Kontaktbrücke zum Schließen eines Kontakts zwischen dem Kontaktpaar, so dass bei Ausübung eines äußeren Drucks auf das Modul (**1**) die Kontaktbrücke (**4**) gegen das Kontaktpaar (**6**) gedrückt wird.

4. Chipkarte mit integriertem Schalter nach Anspruch 3, bei der das Modul (**1**) als Flip-Chip-Modul ausgebildet ist.

5. Chipkarte mit integriertem Schalter nach Anspruch 3 oder 4, bei der das Kontaktpaar (**6**) auf einer Metallisierungsebene eines Trägers des Moduls (**1**) ausgebildet ist.

6. Chipkarte mit integriertem Schalter nach Anspruch 3 oder 4, bei der das Kontaktpaar (**6**) auf der der Kontaktbrücke zugewandten Seite des Chips oder auf dem den Chip umhüllenden Material ausgebildet ist.

7. Chipkarte mit integriertem Schalter nach einem der vorhergehenden Ansprüche 1 bis 6, bei der die Kontaktbrücke (**4**) als Metallbügel ausgebildet ist.

8. Chip arte mit integriertem Schalter nach einem der vorhergehenden Ansprüche 1 bis 6, bei der die Kontaktbrücke (**4**, **5**) als isotrop leitfähiges Silikon- oder Gummiformteil ausgebildet ist.

9. Chip arte mit integriertem Schalter nach einem der vorhergehenden Ansprüche 1 bis 6, bei der die Kontraktbrücke (**4**, **5**) durch einen in ein isotropleitfähiges Silikon- oder Gummiformteil (**5**) eingebetteten Metallbügel (**4**) ausgebildet ist.

10. Chipkarte mit integriertem Schalter nach einem der vorhergehenden Ansprüche 1 bis 9 mit Mitteln zur Erzeugung eines elektrischen Signals, beispielsweise eines Impuls, beim Schließen oder Öffnen des Schalters.

11. Chipkarte mit integriertem Schalter nach Anspruch 10 mit Mitteln zur Eingabe des elektrischen Signals in einen integrierten elektronischen Schaltkreis des Moduls.

12. Chipkarte mit integriertem Schalter nach Anspruch 11, bei der der integrierte elektronische Schaltkreis des Moduls zur automatischen Auslösung einer Aktion nach Eingabe des elektrischen Signals ausgebildet ist.

13. Chipkarte mit integriertem Schalter nach Anspruch 12, bei der der integrierte elektronische Schaltkreis Computerprogrammmittel zur Ausgabe einer Information an einen Empfänger nach Erhalt des elektrischen Signals aufweist.

14. Chipkarte mit integriertem Schalter nach Anspruch 12 oder 13 mit drahtlosen Übertragungsmitteln.

15. Verfahren zur Freigabe einer Transaktion, insbesondere für die drahtlose elektronischen Bezahlung, mit folgenden Schritten:

- Betätigung eines in eine Chipkarte nach einem der vorgehenden Ansprüche 1 bis 14 integrierten Schalters durch einen Benutzer zur Erzeugung eines elektrischen Signals, beispielsweise eines Impulses,
- Eingabe des elektrischen Signals in ein Modul der Chipkarte,
- Ausgabe einer Information für die Abwicklung der Transaktion von der Chipkarte, wobei die Ausgabe der Information vorzugsweise drahtlos an ein Kartenlesegerät erfolgt.

Hierzu 3 Seite(n) Zeichnungen

- Leerseite -

Nummer: **DE 101 40 662 C1**
Int. Cl.[7]: **G 06 K 19/077**
Veröffentlichungstag: 20. März 2003

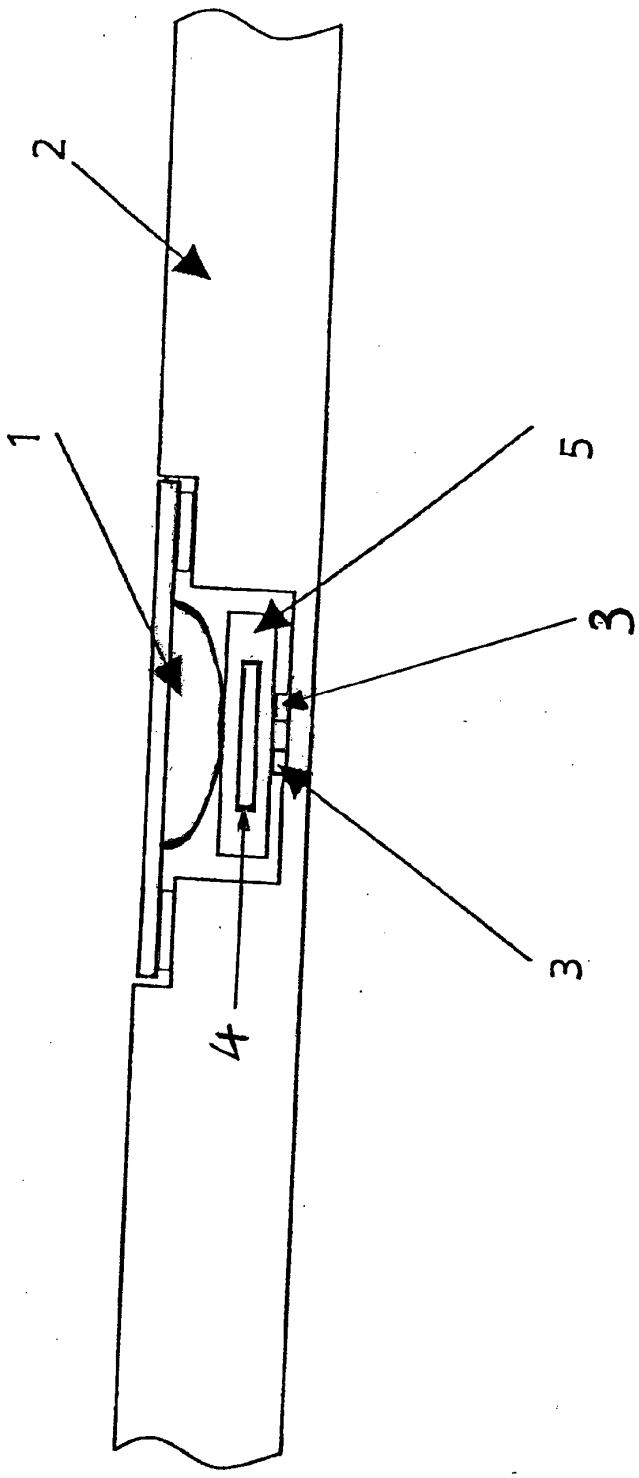


Fig. 1

Nummer: **DE 101 40 662 C1**
Int. Cl.[7]: **G 06 K 19/077**
Veröffentlichungstag: 20. März 2003

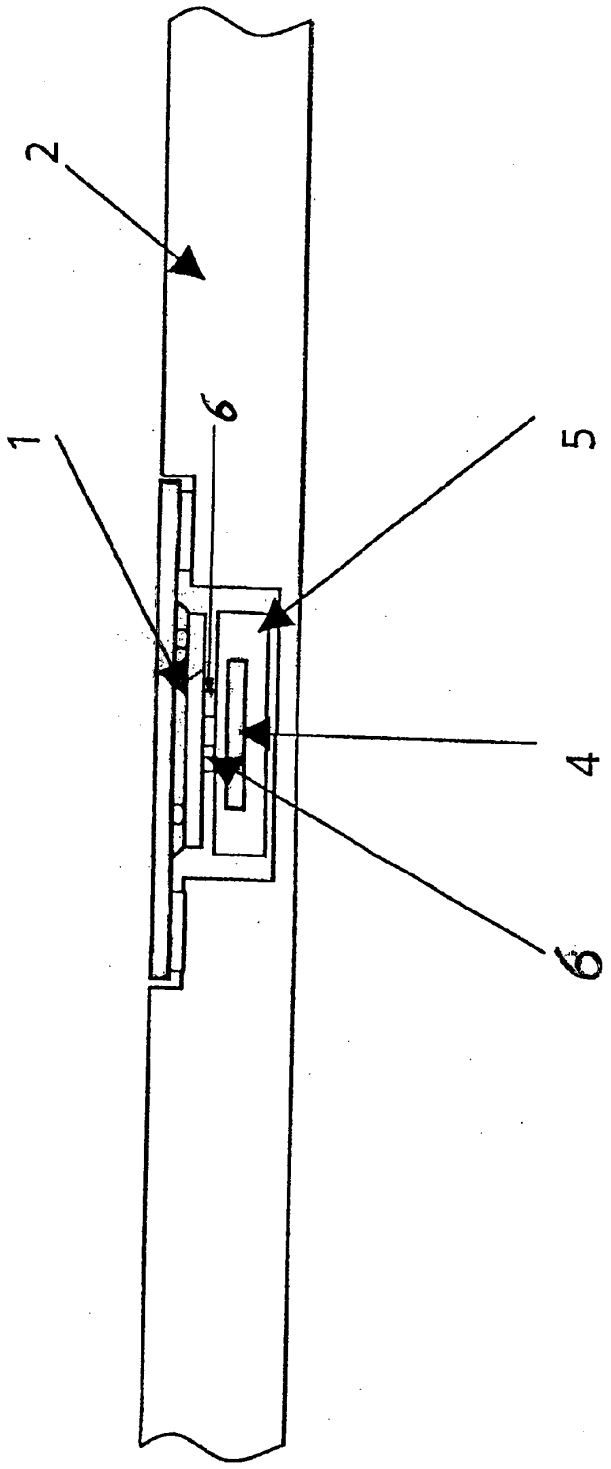


Fig. 2

Nummer: DE 101 40 662 C1
Int. Cl.[7]: G 06 K 19/077
Veröffentlichungstag: 20. März 2003

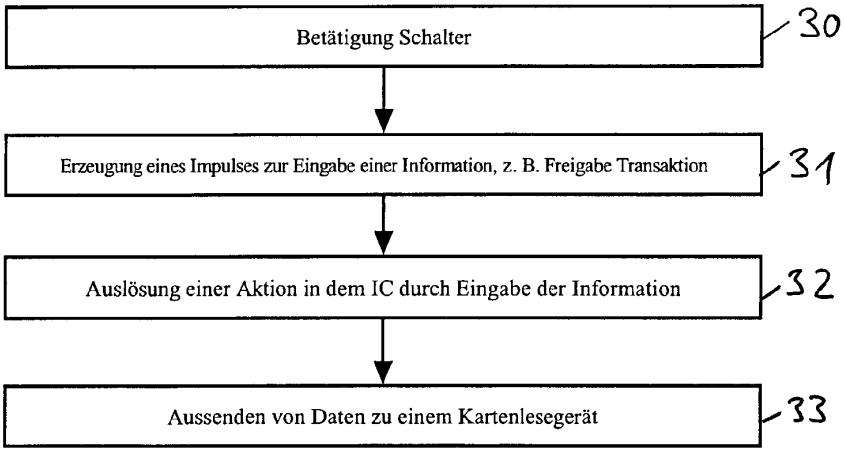


Fig. 3

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 42 900 A 1**

(51) Int. Cl.[6]: **G 06 K 19/07**

(21) Aktenzeichen: 195 42 900.1
(22) Anmeldetag: 17. 11. 95
(43) Offenlegungstag: 22. 5. 97

DE 195 42 900 A 1

(71) Anmelder:
Cubit Electronics GmbH, 99099 Erfurt, DE

(74) Vertreter:
Pöhner,Liedtke & Partner, Dr., 99094 Erfurt

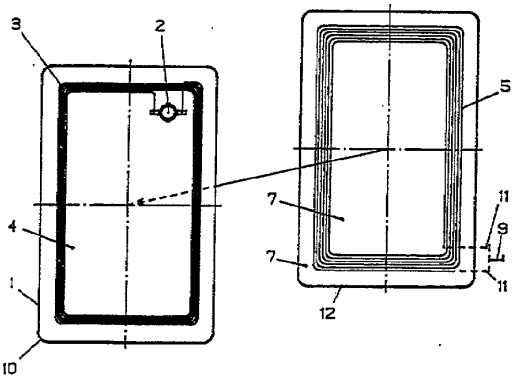
(72) Erfinder:
Michalk, Manfred, Dr., 99096 Erfurt, DE; Michalk, Helga, 99096 Erfurt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 43 02 387 C2
DE 43 28 100 A1
DE 42 33 283 A1
DE 41 05 869 A1

(54) Kontaktloser Datenträger

(57) Der Erfindung liegt die Aufgabe zugrunde, die Schreib- bzw. Lesereichweite des Datenträgers zu verändern, ohne schirmende oder filternde Elemente bewegen zu müssen.
Die Aufgabe wird dadurch gelöst, daß auf dem Datenträger 1 parallel zur Ebene 4 der Antennenspule 3 mindestens eine offene Zusatzspule 5 angeordnet ist.
Die Erfindung betrifft einen kontaktlosen Datenträger mit spulenförmiger Antenne zur elektromagnetischen Daten- und/oder Energieübertragung.



DE 195 42 900 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 03. 97 702 021/231 7/22

Beschreibung

Die Erfindung betrifft einen kontaktlosen Datenträger mit spulenförmiger Antenne zur elektromagnetischen Daten- und/oder Energieübertragung.

Kontaktlose Datenträger werden z. B. in Form von kontaktlosen Chipkarten für vielfältige Einsatzgebiete verwendet. Sie ermöglichen einen berührungslosen Datenaustausch zwischen dem Datenträger und einer Schreib- bzw. Lesestation. Der Datentransfer erfolgt dabei durch Übertragung mittels eines elektromagnetischen Feldes ohne direkten elektrischen Kontakt. Innerhalb des jeweiligen Arbeitsabstandes zwischen Datenträger und Schreib- bzw. Lesestation ist es möglich, den Datenaustausch zu betreiben, ohne daß die Karte in ein Schreib- bzw. Lesegerät eingelegt werden muß.

Dabei besteht die Gefahr des unbeabsichtigten Preisgebens von Daten oder einer ungewollten Änderung der im Datenträger gespeicherten Informationen, da durch verdeckt angebrachte Schreib-Lese-Stationen oder durch unbeabsichtigtes Nähern an Schreib- oder Lesestationen der Datenträger gelesen oder seine Daten verändert werden kann, ohne daß der Benutzer dies bemerkt.

Zum Schutz des Datenträgers vor ungewollten Ablesen bzw. Beschreiben ist es bekannt durch temporäres Abschotten des Datenträgers mit metallischen Folien o. ä. die Reichweite drastisch einzuschränken.

Dies hat jedoch den Nachteil, daß abschirmende Elemente, wie Klappen, Schieber, Blenden o. ä. bei jedem beabsichtigten Gebrauch des Datenträgers in ihrer Lage verändert werden müssen. Weiterhin ist durch das Vorhandensein der schützenden Hülle oder des abschottenden Elementes in der Nähe des Datenträgers in den meisten Fällen eine Verringerung der Lese- bzw. Schreib-Reichweite des Datenträgers nicht zu vermeiden.

Andererseits ist eine Erhöhung der Reichweite wünschenswert, da die maximale Schreib- bzw. Lesereichweite der kontaktlosen Datenträger zur Schreib- und/oder Lesestation durch Toleranzen bei der Herstellung des Datenträgers (z. B. durch Antennen- und Kapazitätstoleranzen) und durch Umgebungseinflüsse, z. B. durch metallische Teile in der Nähe des kontaktlosen Datenträgers, durch den menschlichen Körper, durch die Bekleidung, durch Befestigungs- oder Beförderungsmittel, durch Temperatureinflüsse und dergleichen herabgesetzt wird.

Der Erfindung liegt die Aufgabe zugrunde, die Schreib- bzw. Lesereichweite des Datenträgers zu verändern ohne schirmende oder filternde Elemente bewegen zu müssen.

Die Aufgabe wird erfindungsgemäß durch einen kontaktlosen Datenträger mit den in Anspruch 1 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen sind in den Unteransprüchen angegeben.

Dabei wird unmittelbar am Datenträger oder in einem Abstand zum Datenträger oder je nach Größe des Datenträgers ebenenparallel oder nahezu ebenenparallel zur spulenförmigen Antenne des Datenträgers mindestens eine Zusatzspule mit offenen Enden angeordnet.

Durch diese Zusatzspule wird eine Veränderung des Datenträgerschwingkreises bewirkt, die bei zweckmäßiger Dimensionierung der Datenträgerantenne und der Zusatzantenne sowie der Wahl eines angepaßten Abstandes von Datenträgerantenne und der Zusatzspule zu einer allgemeinen Erhöhung der Schreib- bzw. Lesereichweite des Datenträgers führt.

Durch die Anordnung von je einer Zusatzspule auf jeder Seite der Datenträgerantenne kann eine Verstärkung dieses Effektes erreicht werden.

Werden die Enden mindestens einer Zusatzspule miteinander verbunden oder werden zumindest Teile der Zusatzspule kurzgeschlossen und läßt sich diese Verbindung oder dieser Kurzschluß durch ein schaltendes oder tastbares Element permanent oder zeitweise öffnen, wird dadurch einerseits erreicht, daß die Sende- bzw. Empfangssignale in den Kurzschlußringen nahezu vollständig absorbiert werden, daß also die Sende- bzw. Empfangsreichweite stark verringert wird und daß andererseits bei geöffnetem Zusatzspulenkurzschluß die sonst erreichbare maximale Lese- und/oder Schreibreichweite des Datenträgers wiederhergestellt wird.

Es ergibt sich damit der Vorteil, daß der Datenträger bei beabsichtigter Benutzung eine gegenüber zusatzspulenfreien Datenträgern erhöhte Reichweite und bei Nichtbenutzung der Datenträger keine bzw. nur eine verschwindend kleine Reichweite aufweist. Bei der Benutzung kann z. B. durch Drücken eines öffnenden Tastschalters auf maximale Reichweite geschaltet werden.

Eine weitere Ausgestaltung der erfindungsgemäßen Anordnung ergibt sich dadurch, daß parallel zur Ebene der Datenträgerantenne in bestimmten Abständen eine oder mehrere Zusatzspulen vorzugsweise einseitig zum Antennenträger angeordnet werden und daß zusätzlich in bestimmten Abstand dazu mindestens eine Ferritschichtebene und gegebenenfalls eine weitere Zusatzspule angeordnet wird.

Damit wird eine Vergrößerung der Reichweite erreicht. Dies ist besonders für Anwendungsfälle vorteilhaft, bei denen ein Datenträger direkt auf einem metallischen Gegenstand oder sehr nahe daran angeordnet werden soll. Die Veränderung tritt insbesondere dann ein, wenn der metallische Gegenstand etwa die Flächengröße des Datenträgers einnimmt oder diese überschreitet. Durch die Energieabsorption, die von dem metallischen Gegenstand hervorgerufen wird, wird die Schreib- oder Lesereichweite des Datenträgers deutlich verringert. Die schichtenweise Anordnung von Zusatzantenne und zusätzlich einer Ferritschicht sowie gegebenenfalls einer weiteren Zusatzspule ermöglicht es, daß die Reichweite des Datenträgers nur gering eingeschränkt wird. Insbesondere wenn deren Flächengröße die Flächengröße der Datenträgerantenne überschreitet. Dabei liegen die Zusatzschichten zwischen Datenträgerantenne und Metallfläche bzw. metallischen Gegenstand.

Besonders vorteilhaft ist dabei, daß dieser Mehrschichtenaufbau wesentlich leichter und in seiner Gesamtschichtendicke wesentlich dünner ist, als ein Schichtenaufbau, der nur aus Ferriten besteht. Zudem ergibt die Reichweiteneliminierung durch zeitweises Kurzschließen mindestens einer Zusatzspule einen weiteren Vorteil.

Die Erfindung ermöglicht es einerseits die Schreib- und/oder Lesereichweite kontaktloser Datenträger zu erhöhen oder die Schreib- und/oder Lesereichweite auch bei Eintreten ungünstiger Sende- bzw. Empfangsbedingungen nicht signifikant zu verringern, andererseits kann die Schreib- und/oder Lesereichweite auch drastisch verringert werden, wenn dies erforderlich oder wünschenswert ist.

Für die erfindungsgemäßen Datenträger sind vielfältige Ausführungsformen möglich.

Zur Erzeugung unterschiedlicher Reichweiten können z. B. die Zusatzspulen gleichsinnig oder gegensinnig

zur Antennenspule des Datenträgers gewickelt sein. Ferner ist es möglich, daß die Spule und die Ferritschicht untereinander elektrisch isoliert und/oder daß mehrere Zusatzspulen hintereinander angeordnet sind.

Die Windungen der Zusatzspulen können dabei so gestaltet sein, daß die Zusatzspule eine Windungsganghöhe gleich/größer der der Antennenspule aufweist und/oder daß die Windungsfläche der Zusatzspule gleich/größer der Windungsfläche der Antennenspule ist.

Weiter ist es möglich, daß die Fläche der Zusatzspule gleich oder größer als die Fläche der Antennenspule ist.

Ferner kann die Fläche der Ferritschicht gleich oder größer der Fläche der Antennenspule gestaltet sein.

Zweckmäßig ist es ferner, daß die Fläche der Zusatzspule(n) und gegebenenfalls die Fläche der Ferritschicht(en) größer sind als die Fläche der Antennenspule und/oder daß die Zusatzantenne, Ferritschichten, Kurzschlußschalter als Zusatzpaket bzw. als Reflektorpaket oder als Datenträger angeordnet sind.

Mit diesen Gestaltungsmöglichkeiten läßt sich erreichen, daß einerseits eine Optimierung der Zusatzspulen und Ferritschichten in Bezug auf den Antennenschwingkreis und andererseits eine günstige anwendungstechnische Anordnung von Zusatzspulen, Ferritschichten und Datenträger möglich ist.

Die Erfindung wird im folgenden anhand eines Ausführungsbeispieles näher erläutert.

In der zugehörigen Zeichnung zeigen:

Fig. 1 eine Gestaltungsmöglichkeit für Datenträger und Zusatzspule, wobei die Zusatzspulenenden mit Schalter kurzgeschlossen sind und

Fig. 2 eine Gestaltungsmöglichkeit für die Anordnung eines erfindungsgemäßen Datenträgers auf einem Metallgegenstand im Schnitt.

Fig. 1 erläutert die Gestaltung des Datenträgers **1**, der im beschriebenen Beispiel eine kontaktlose Chipkarte **10** darstellt. Auf bzw. in dieser Chipkarte **10** befindet sich ein Modul **2**, das mit der Datenträgerantenne 3 verbunden ist. Die Datenträgerantenne 3 ist so gewikkelt, daß sie die Antennenebene **4** bildet. Hinter oder vor dieser Ebene **4** ist die Zusatzspule **5** mit den Spulenenden **11** angeordnet, die durch den Schalter **9** kurzgeschlossen sind. Die Zusatzspule **5** weist im dargestellten Beispiel mehr Windungen auf als die Datenträgerantenne 3. Zusatzspule **5** und Schalter **9** befinden sich in elektrisch isolierenden Abstandsschichten **7** und bilden zusammen ein Datenträgerzusatzpaket **12**. Das Datenträgerzusatzpaket **12** liegt deckungsgleich unter der Chipkarte **10**.

Fig. 2 erläutert eine Anordnung, die auf einem Metallgegenstand **8** angebracht ist. Auf diesem Metallgegenstand **8** ist das Reflektorpaket **13** und darüber der Datenträger **1** als Chipkarte **10** angeordnet. Das Reflektorpaket **13** besteht aus mehreren Abstandsschichten **7**, zwischen denen die Ferritschicht **6** und Zusatzspulen **5** angeordnet sind.

Bezugszeichenliste

1 Datenträger
2 Modul
3 Datenträgerantenne
4 Antennenebene
5 Zusatzspule
6 Ferritschicht
7 Abstandsschicht
8 Metallgegenstand
9 Schalter
10 Chipkarte
11 Spulenenden
12 Datenträgerzusatzpaket
13 Reflektorpaket

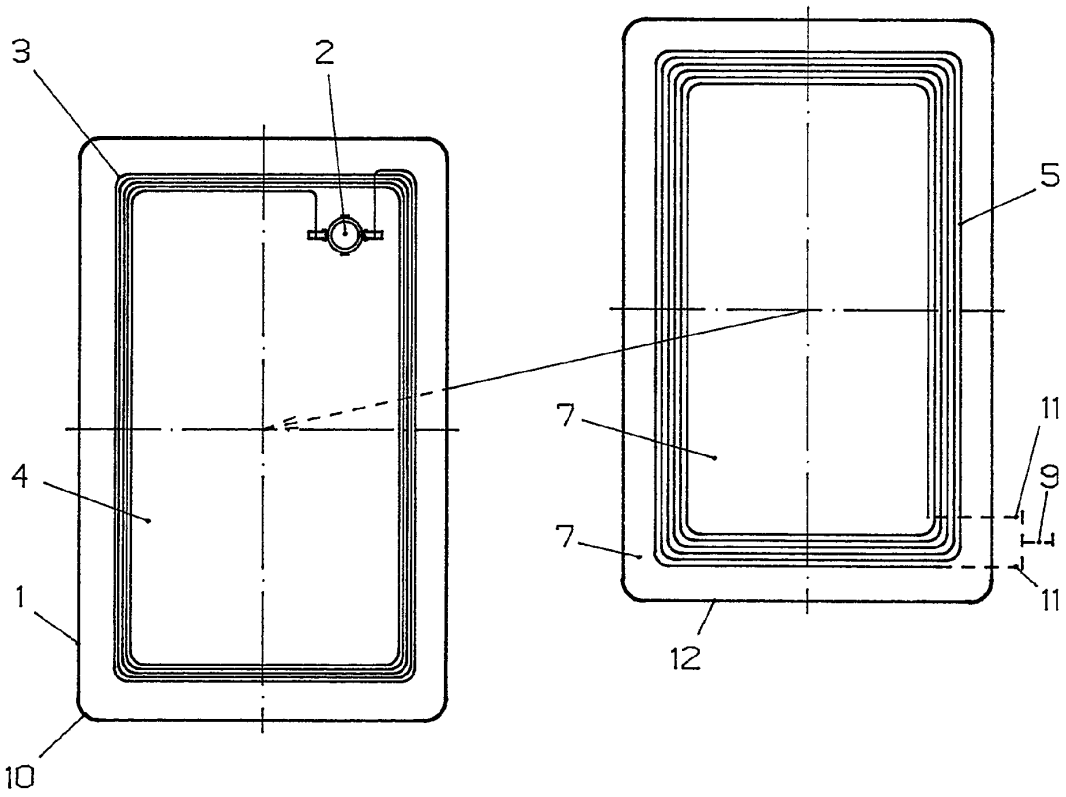
Patentansprüche

1. Kontaktloser Datenträger mit spulenförmiger Antenne zur elektromagnetischen Daten- und/oder Energieübertragung, **dadurch gekennzeichnet,** daß auf dem Datenträger (**1**) parallel zur Ebene (**4**) der Antennenspule (**3**) mindestens eine offene Zusatzspule (**5**) angeordnet ist.
2. Kontaktloser Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß beidseitig zur Antennenspule (3) des Datenträgers (**1**) mindestens je eine offene Zusatzspule (**5**) parallel zur Ebene (**4**) der Antennenspule (3) angeordnet ist.
3. Kontaktloser Datenträger nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß am Datenträger 1 mindestens ein Schalter (**9**) angeordnet ist, mit dem mindestens eine Zusatzspule (**5**) ganz oder teilweise kurzgeschlossen werden kann.
4. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß mindestens eine Zusatzspule (**5**) gegensinnig zur Antennenspule (3) des Datenträgers (**1**) gewickelt ist.
5. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß parallel zur Ebene (**4**) der Antennenspule (3) des Datenträgers (**1**) eine Zusatzspule (**5**) und nachfolgend eine Ferritschicht (**6**) angeordnet sind.
6. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Antennenspule (3), die Zusatzspulen (**5**) und die Ferritschicht (**6**) untereinander durch elektrisch isolierende Abstandsschichten (**7**) getrennt sind.
7. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Ferritschicht (**6**) nur einseitig zum Datenträger (**1**) und auf der senderabgewandten Seite angeordnet ist.
8. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß auf der senderabgewandten Seite des Datenträgers (**1**) mehrere Zusatzspulen (**5**) und mindestens eine Ferritschichtenebene (**6**) angeordnet sind.
9. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß die Ferritschichtenebenen (**6**) durch Zusatzspulen (**5**) getrennt sind.
10. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß Zusatzspule (**5**) und Kurzschlußschalter (**9**) und/oder weitere Zusatzspulen (**5**) und/oder Ferritschichten (**6**) Elemente eines Datenträgerhalters sind.
11. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß der Datenträgerhalter eine Chipkartenschutzhülle ist.
12. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß Datenträger (**1**), Zusatzspule (**5**) und/oder Kurzschlußschalter (**9**) und/oder weitere Zusatzspulen (**5**) und/oder Ferritschicht(en) (**6**) zu einem einteiligen Kompaktdatenträger verbunden sind.
13. Kontaktloser Datenträger nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, daß Zu-

satzspule (5) und Kurzschlußschalter (9) und/oder weitere zusatzspulen (5) und/oder Ferritschicht(en) (6) Elemente eines datenträgerflächengleichen Datenträgerzusatzpaketes (12) sind.

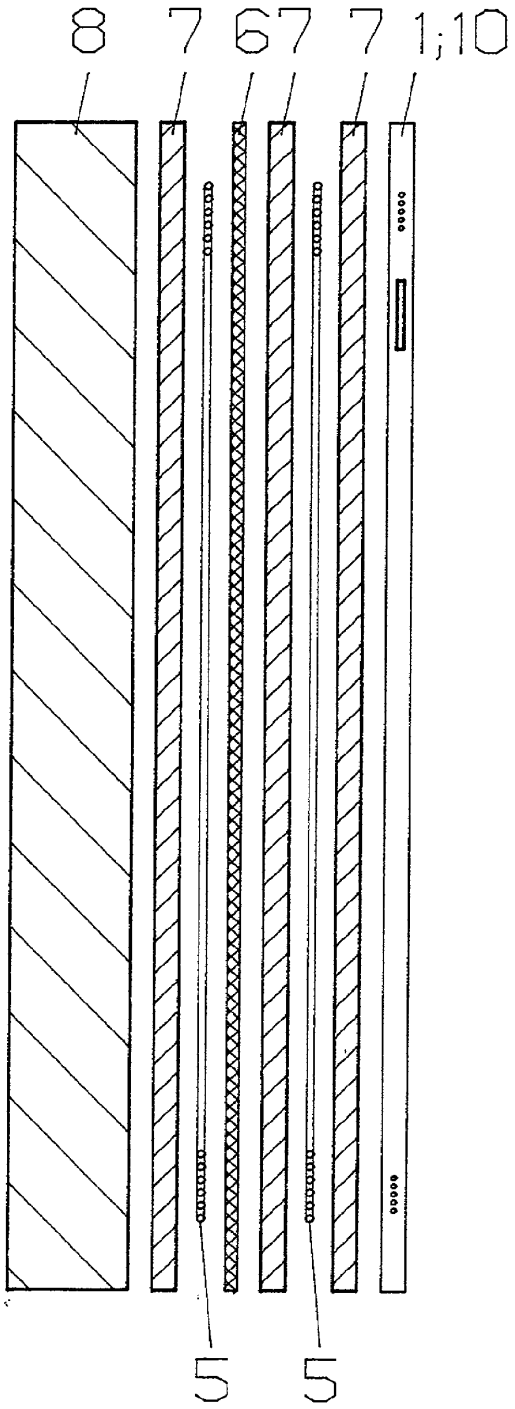
Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 195 42 900 A1
Int. Cl.[6]: G 06 K 19/07
Offenlegungstag: 22. Mai 1997



Figur 1

Nummer: DE 195 42 900 A1
Int. Cl.[6]: G 06 K 19/07
Offenlegungstag: 22. Mai 1997



Figur 2

702 021/231

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 197 42 126 A 1**

(51) Int. Cl.[6]: **G 06 K 19/073**

(21) Aktenzeichen: 197 42 126.1
(22) Anmeldetag: 24. 9. 97
(43) Offenlegungstag: 25. 3. 99

DE 197 42 126 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Hoedeau, Detlef, 84085 Langquaid, DE; Heinemann, Erik, 93049 Regensburg, DE; Püschner, Frank, 93309 Kelheim, DE

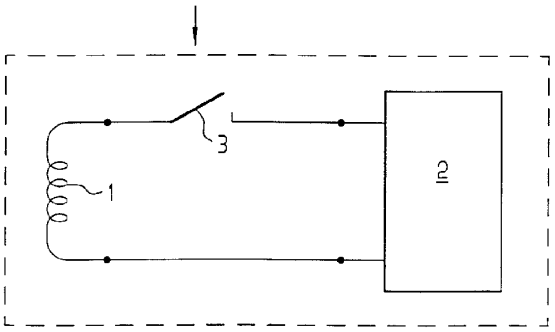
(56) Entgegenhaltungen:
DE 1 95 42 900 A1
DE 42 05 827 A1
DE 42 05 556 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Tragbarer Datenträger mit Aktivierungsschalter

(57) Bei einem tragbaren Datenträger, insbesondere einer Chipkarte, mit einer Antenne (1) und einem damit verbundenen Halbleiterchip (2), ist zwischen der Antenne (1) und dem Halbleiterchip (2) ein durch den Benutzer des Datenträgers betätigbares Schaltmittel (3) angeordnet, so daß ein Empfang von Daten nur nach einer Betätigung des Schaltmittels (3) möglich ist.



DE 197 42 126 A 1

Beschreibung

Die Erfindung betrifft einen tragbaren Datenträger, insbesondere eine Chipkarte, mit einer Antenne und einem damit verbundenen Halbleiterchip.

Solche sogenannten kontaktlosen Datenträger, insbesondere Chipkarten, werden schon seit einiger Zeit beispielsweise in Zutrittskontrollsystemen eingesetzt. Es gab jedoch auch schon Feldversuche, kontaktlose Datenträger in Form von Armbanduhren bei Skiliften zu verwenden.

Die US 4,701,601 beschreibt eine Chipkarte mit Kontaktfeldern für den kontaktbehafteten Betrieb in Chipkartenterminals und einer Sendespule zur Emulation eines Magnetstreifens für den Betrieb in herkömmlichen Magnetstreifenterminals. Um die eingebaute Batterie nicht zu sehr zu belasten ist ein Sendeknopf vorgesehen, der das Senden von Daten über die Emulationsspule auf einen kleinen Zeitraum begrenzt.

Eine sich seit einiger Zeit im Gespräch befindende Einsatzmöglichkeit von kartenförmigen, kontaktlosen Datenträgern ist die Verwendung als abbuchbares Zahlungsmittel im öffentlichen Nahverkehr. Diese Chipkarten sind hinsichtlich ihres Wertes wiederaufladbar, was bedeutet, daß ein einen Geldwert repräsentierender Zählerstand auch erhöht werden kann. Sie weisen zu diesem Zweck zusätzlich zur Antenne Kontaktfelder auf, über die sie mittels eines Lese/Schreibterminals durch ohmsche Kontaktierung wieder aufgeladen werden können.

Allen heute gebräuchlichen kontaktlosen und auch sowohl Kontaktelemente als auch eine Antenne aufweisenden Chipkarten oder allgemein Datenträgern ist gemeinsam, daß sie über die kontaktlose Schnittstelle mit Energie versorgt werden können und daß darüber auch die bidirektionale Datenübertragung stattfindet.

Bei Datenträgern, deren Wert bei Benutzung verringert wird, also beispielsweise bei Verwendung als Zahlungsmittel im Nahverkehr, besteht die Gefahr, daß ein zufälliger Aufenthalt des Benutzers in der Nähe eines Abbuchungsautomaten zu einer Wertverringerung führt, ohne daß die entsprechende Dienstleistung in Anspruch genommen wird. Auch könnte es zu Mehrfachabbuchungen führen, wenn der Aufenthalt auch bei gewünschter Inanspruchnahme der Dienstleistung zu lange ist.

Das der Erfindung zugrunde liegende Problem ist es somit, einen tragbaren Datenträger anzugeben, der diesen Nachteil nicht aufweist.

Das Problem wird bei einem gattungsgemäßen Datenträger dadurch gelöst, daß zwischen der Antenne und dem Halbleiterchip ein durch den Benutzer des Datenträgers betätigbares Schaltmittel angeordnet ist, so daß ein Empfang von Daten nur nach einer Betätigung des Schaltmittels möglich ist.

Durch diese erfindungsgemäße Maßnahme hat es der Benutzer selbst in der Hand, den]Datenträger zu aktivieren, so daß ein Datenempfang nur erfolgen kann, wenn dies der Benutzer wünscht.

In Weiterbildung der Erfindung ist das Schaltmittel verrastbar ausgebildet, so daß eine ständige Verbindung zwischen der Antenne, die in vorteilhafter Weise als Spule ausgebildet sein kann, und dem Halbleiterchip, der zumindest einen Speicher und Logikschaltungen enthält, eingestellt werden kann, falls der Benutzer dies wünscht, wobei er dann allerdings wieder dem Risiko ausgesetzt ist, daß Fehlabbuchungen vorkommen können.

Das durch den Benutzer betätigbare Schaltmittel, das als einfacher Druckschalter ausgeführt sein kann, kann als separates Bauteil in eine Aussparung der Karte, beispielsweise in einer Ecke der Karte eingesetzt sein oder auf einem den Halbleiterchip tragenden Trägerelement angeordnet sein.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe von Figuren näher erläutert. Dabei zeigen:

Fig. 1 eine Prinzipdarstellung eines erfindungsgemäßen Datenträgers und

Fig. 2 eine schematische Querschnittsdarstellung eines erfindungsgemäßen Datenträgers.

Gemäß **Fig.** 1 weist der mit einer strichlierten Linie angedeutete Datenträger eine Antennenspule **1** sowie einen Halbleiterchip **2** auf. Der Halbleiterchip **2** weist in bekannter Weise Speichereinheiten wie beispielsweise ein EEPROM sowie Logikschaltungen wie einen Mikroprozessor auf. Die Antennenspule **1** ist zur Energieübertragung zum und zur bidirektionalen Datenübertragung von und zum Halbleiterchip **2** mit diesem über ein Schaltmittel **3** verbunden. Das Schaltmittel **3** ist, wie durch einen Pfeil angedeutet ist, von außerhalb des Datenträgers durch den Benutzer betätigbar. Eine Energie- und Datenübertragung von der Antennenspule **1** zum Halbleiterchip **2** kann also nur stattfinden, wenn der Benutzer zuvor das Schaltmittel **3** betätigt hat.

Fig. 2 zeigt einen Querschnitt durch einen erfindungsgemäßen Datenträger in Form einer Plastikkarte **6**. Die Antennenspule **1** ist in einigen Windungen entlang der äußeren Abmessung der Plastikkarte geführt. Der Halbleiterchip **2** ist auf einem Trägerelement **7** angeordnet und mittels diesem in bekannter Weise mit der Plastikkarte **6** beispielsweise durch Kleben verbunden. Zwei Enden **4**a, **4**b der Antennenspule **1** sind mit dem Trägerelement **7** und über dieses mit dem Halbleiterchip **2** verbunden.

Fig. 2 zeigt außerdem das Schaltmittel **3**, dessen Oberfläche mit der Oberfläche der Karte **6** fluchtet, und das zwischen zwei Unterbrechungen **5**a, **5**b der Antennenspule **1** geschaltet ist.

In der Darstellung gemäß **Fig.** 2 ist das Schaltmittel **3** als separates Bauelement ausgeführt und in einer Ausnehmung der Plastikkarte **6** angeordnet. Es wäre jedoch ebenso denkbar, das Schaltmittel **3** als Bestandteil des Trägerelements **7** zu gestalten.

Patentansprüche

1. Tragbarer Datenträger, insbesondere Chipkarte, mit einer Antenne (**1**) und einem damit verbundenen Halbleiterchip (**2**), **dadurch gekennzeichnet**, daß zwischen der Antenne (**1**) und dem Halbleiterchip (**2**) ein durch den Benutzer des Datenträgers betätigbares Schaltmittel (**3**) angeordnet ist, so daß ein Empfang von Daten nur nach einer Betätigung des Schaltmittels (**3**) möglich ist.
2. Tragbarer Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß das Schaltmittel (**3**) verrastbar ausgebildet ist.
3. Tragbarer Datenträger nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Antenne (**1**) als Spule ausgebildet ist.
4. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Schaltmittel (**3**) als separates Bauteil in einer Ausnehmung des Datenträgers angeordnet ist.
5. Tragbarer Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Oberfläche des Schaltmittels (**3**) mit der Oberfläche des Datenträgers fluchtet.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: **DE 197 42 126 A1**
Int. Cl.[6]: **G 06 K 19/073**
Offenlegungstag: 25. März 1999

FIG 1

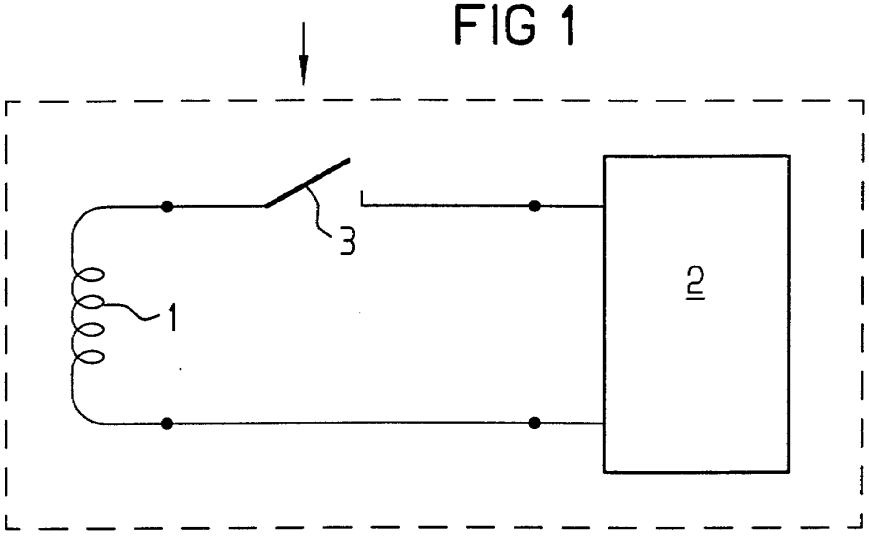
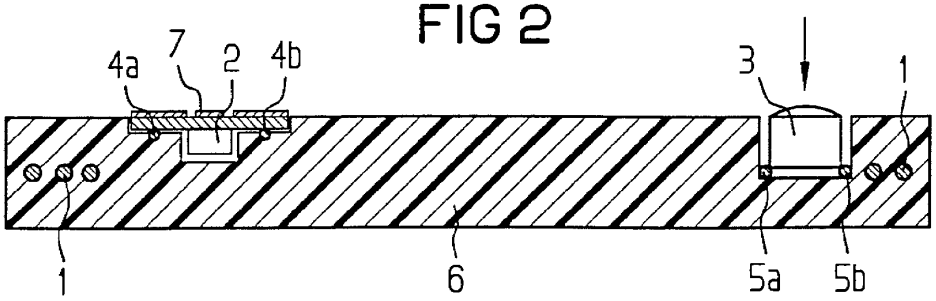


FIG 2



(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 728 710**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 15570**

(51) Int Cl⁶ : G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 23.12.94.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 28.06.96 Bulletin 96/26.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :** CERTIFICAT D'UTILITÉ RÉSULTANT DE LA TRANSFORMATION VOLONTAIRE DE LA DEMANDE DE BREVET DÉPOSÉE LE 27/12/94

(71) **Demandeur(s) :** *SOLAIC SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** LARCHEVESQUE ALAIN et GAUMET MICHEL.

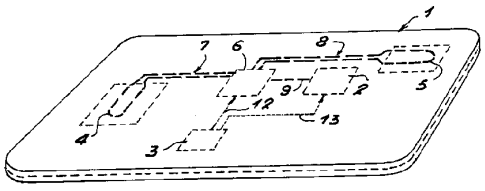
(73) **Titulaire(s) :**

(74) **Mandataire :**

(54) CARTE ELECTRONIQUE COMPORTANT UN ELEMENT FONCTIONNEL ACTIVABLE MANUELLEMENT.

(57) La carte électronique selon l'invention comprend un corps en matière plastique (1) renfermant un élément fonctionnel (2) alimenté par une source d'énergie (3), et est caractérisée en ce que la source d'énergie est reliée à un élément sensible (4) dans lequel une grandeur physique varie lorsqu'il est soumis à une action manuelle volontaire, et à un circuit électronique (6) apte à fournir un signal de commande à l'élément fonctionnel (2) en réponse à un signal émis par l'élément sensible (4) et correspondant à une valeur de la grandeur physique, située dans une plage de valeurs prédéterminée.

Afin d'éviter une activation intempestive de l'élément fonctionnel, il est souhaitable que le circuit électronique ne délivre le signal de commande que lorsque la valeur de la grandeur physique varie à une vitesse située dans une plage de vitesses prédéterminée.



FR 2 728 710 - A1

"Carte électronique comportant un élément fonctionnel activable manuellement"

La présente invention concerne une carte électronique comprenant un corps en matière plastique renfermant un élément fonctionnel alimenté par une source d'énergie.

Les cartes électroniques de ce type ne sont pas pourvues actuellement de moyens d'actionnement permettant d'activer et ou de désactiver volontairement leur élément fonctionnel. L'épaisseur du corps de ces cartes est en effet trop faible pour que l'on puisse installer sur celles-ci un interrupteur ou un bouton-poussoir destiné à commander l'activation de l'élément fonctionnel.

La présente invention se propose de remédier à cette lacune et, pour ce faire, elle a pour objet une carte électronique du type indiqué ci-dessus, qui se caractérise en ce que la source d'énergie est reliée à un élément sensible dans lequel une grandeur physique varie lorsqu'il est soumis à une action manuelle volontaire, et à un circuit électronique apte à fournir un signal de commande à l'élément fonctionnel en réponse à un signal émis par l'élément sensible et correspondant à une valeur de la grandeur physique, située dans une plage de valeurs prédéterminée.

L'élément sensible utilisé peut être réalisé avec de faibles dimensions, ce qui permet de l'installer dans le corps des cartes électroniques, ou même sur l'une des faces de celles-ci, sans qu'il fasse saillie à l'extérieur.

Comme l'élément fonctionnel n'est activé que lorsque cela est nécessaire, les pertes d'énergie qui étaient relativement importantes jusqu'ici sont évitées. La source d'énergie peut par conséquent être utilisée beaucoup plus longtemps que les sources actuelles.

On notera par ailleurs qu'une activation intempestive de l'élément fonctionnel n'est pas possible puisque le circuit électronique ne peut commander ce dernier lorsque la grandeur physique reste inférieure à la valeur minimale de la plage d'activation ni lorsque cette grandeur devient supérieure à la valeur maximale de ladite plage.

Afin de limiter encore les risques d'une activation intempestive de l'élément fonctionnel, il est préférable que le circuit électronique ne délivre le signal de commande que lorsque la valeur de la grandeur physique varie à une vitesse située dans une plage de vitesses prédéterminée.

L'élément fonctionnel ne sera donc pas activé si la valeur de la grandeur physique varie à une vitesse inférieure à la vitesse minimale de la plage de vitesses ou supérieure

à la vitesse maximale de cette plage.

Selon un premier mode de réalisation de l'invention, l'élément sensible est une jauge de contrainte disposée dans le corps en matière plastique tandis que la grandeur physique est un courant électrique dont l'intensité varie lorsque le corps en matière plastique est soumis à une flexion manuelle dans une zone adjacente à la jauge de contrainte.

Pour éviter qu'une flexion involontaire du corps de la carte déclenche une activation intempestive de l'élément fonctionnel, une seconde jauge de contrainte reliée au circuit électronique est avantageusement disposée dans le corps en matière plastique, le circuit électronique fournissant le signal de commande à l'élément fonctionnel lorsque la différence des valeurs instantanées des courants électriques traversant les jauges de contrainte est située dans une plage de valeurs déterminée.

Selon un second mode de réalisation, l'élément sensible est une résistance thermique tandis que la grandeur physique est la résistance électrique de la résistance thermique, qui varie lorsque celle-ci est chauffée par un doigt appliqué volontairement contre elle.

Afin d'éviter qu'un échauffement de la résistance thermique par une source externe déclenche l'activation de l'élément fonctionnel, une seconde résistance thermique est reliée au circuit électronique, celui-ci fournissant le signal de commande à l'élément fonctionnel lorsque la différence des valeurs instantanées des résistances électriques des deux résistances thermiques est située dans une plage de valeurs déterminée.

Selon un troisième mode de réalisation, l'élément sensible est un thermocouple tandis que la grandeur physique est une force électromotrice dont la grandeur varie lorsque le thermocouple est chauffé par un doigt appliqué volontairement contre lui.

Comme un échauffement involontaire du thermocouple pourrait déclencher l'activation de l'élément fonctionnel, il est souhaitable qu'un second thermocouple soit relié au circuit électronique, celui-ci fournissant le signal de commande à l'élément fonctionnel lorsque la différence des valeurs instantanées des forces électromotrices créées dans les deux thermocouples est située dans une plage de valeurs déterminée.

On précisera ici que les éléments sensibles utilisés dans les trois modes de réalisation ci-dessus sont encastrés dans le corps des cartes électroniques, mais

pourraient être dans le plan de l'une des grandes faces du corps de ces dernières.

Selon un quatrième mode de réalisation, l'élément sensible est constitué par deux électrodes adjacentes disposées sur le corps en matière plastique tandis que la grandeur physique est l'impédance établie entre les deux électrodes et variant lorsqu'un doigt est appliqué volontairement contre lesdites électrodes.

Pour éviter qu'un organe externe provoque une variation intempestive de l'impédance et déclenche l'activation de l'élément fonctionnel, deux autres électrodes adjacentes reliées au circuit électronique sont disposées sur le corps en matière plastique, le circuit électronique fournissant le signal de commande à l'élément fonctionnel lorsque les impédances respectivement établies entre les électrodes appariées sont les mêmes et varient à la même vitesse.

Plusieurs modes d'exécution de la présente invention sont décrits ci-après à titre d'exemples nullement limitatifs en référence aux dessins annexés dans lesquels :

- la figure 1 est une vue en perspective schématique d'une carte électronique conforme à l'invention ;

- la figure 2 est un schéma d'un circuit électronique susceptible d'être inséré dans le corps de la carte visible sur la figure 1 ; et

- les figures 3 à 5 sont des vues schématiques d'autres cartes électroniques conformes à l'invention.

La carte électronique que l'on peut voir sur la figure 1 comprend un corps plat 1 en matière plastique, ayant deux grandes faces opposées rectangulaires et dont l'épaisseur est inférieure à 1 mm.

Son corps 1 renferme un élément fonctionnel 2 constitué par exemple par un microcircuit ou une puce, une source d'énergie 3 telle qu'une pile électrique, deux jauges de contrainte 4,5 situées en deux emplacements éloignés l'un de l'autre, et un circuit électronique 6.

Des liaisons conductrices 7,8,9 sont prévues pour relier électriquement le circuit électronique 6 aux jauges de contrainte 4 et 5 et à l'élément fonctionnel 2. D'autres liaisons conductrices 12,13 sont quant à elles prévues pour relier électriquement la source d'énergie 3 au circuit électronique 6 et à l'élément fonctionnel 2.

Le circuit électronique 6 est réalisé de façon à permettre la circulation de courants

électriques dans les jauges de contrainte 4 et 5 lorsque les parties du corps 1 qui sont adjacentes à ces dernières sont soumises à une flexion manuelle, et à fournir à l'élément fonctionnel 2 un signal de commande lorsque la différence des valeurs instantanées des courants électriques dans les jauges est située dans une plage de valeurs prédéterminée.

Ainsi, lorsque les parties du corps 1 qui sont adjacentes aux jauges de contraintes sont soumises à des flexions du même ordre de grandeur, et que la valeur de la différence précitée reste inférieure à la valeur minimale de la plage prédéterminée, l'élément fonctionnel 2 ne sera pas activé par le circuit électronique 6.

On peut rencontrer une telle situation, par exemple quand une carte électronique conservée dans une poche de vêtement d'un utilisateur est soumise involontairement à des flexions locales faibles sur toute sa surface.

De même, si les parties du corps 1 qui sont adjacentes aux jauges de contrainte sont soumises à des flexions différentes au point que la valeur de la différence précitée devienne supérieure à la valeur maximale de la plage prédéterminée, l'élément fonctionnel 2 ne sera toujours pas activé par le circuit électronique.

Une telle situation peut par exemple se rencontrer lorsque le corps de la carte électronique est soumis accidentellement à une forte flexion au voisinage d'une seule jauge de contrainte.

Dans le mode de réalisation qui vient d'être décrit, le corps de la carte comporte deux jauges de contrainte. Il va de soi que l'on ne sortirait pas du cadre de la présente invention s'il n'en comptait qu'une seule.

Dans ce cas, le circuit électronique 6 pourrait être réalisé de telle sorte que l'élément fonctionnel 2 ne soit activé que si le courant électrique circulant dans la jauge a une intensité située dans une plage de valeurs prédéterminée, et qu'une activation intempestive de l'élément fonctionnel soit évitée.

Afin de réduire encore les risques d'une activation involontaire, le circuit électronique 6 pourrait également être réalisé de telle sorte que l'élément fonctionnel ne soit activé que si la valeur de l'intensité du courant circulant dans la jauge de contrainte varie à une vitesse située dans une plage de vitesses prédéterminée.

Un exemple de réalisation du circuit électronique 6 ainsi conçu est représenté schématiquement sur la figure 2.

Comme on peut le voir sur cette figure, le circuit 6 comporte un Pont de Wheatstone P dont une branche est constituée par la jauge de contrainte (4 ou 5) et dont deux sommets opposés sont reliés aux bornes positive et négative de la source d'énergie, un circuit amplificateur analogique différentiel 14 relié aux deux autres sommets opposés du Pont de Wheatstone et alimenté par la source d'énergie, et deux circuits 15,16 montés en parallèle entre le circuit amplificateur 14 et l'élément fonctionnel 2, le circuit 15 permettant de mesurer la variation de l'intensité du courant circulant dans la jauge tandis que le circuit 16 permet de mesurer la vitesse à laquelle varie l'intensité de ce courant.

La carte électronique représentée sur la figure 3 diffère légèrement de celle qui a été décrit en référence à la figure 1. Au lieu de comporter deux jauges de contrainte, elle comporte en effet deux résistances thermiques 4a,5a dont les résistances électriques varient lorsqu'elles sont chauffées.

Par ailleurs, son circuit électronique 6a est conçu de façon à activer l'élément fonctionnel 2 lorsque la différence des valeurs instantanées des résistances électriques des résistances thermiques 4a,5a est située dans une plage de valeurs prédéterminée.

Ainsi, lorsque l'utilisateur applique un doigt sur la partie du corps 1 qui est adjacente à une résistance thermique, celle-ci s'échauffe tandis que l'autre demeure à la température ambiante.

La résistance électrique de la résistance thermique qui est chauffée varie par rapport à celle de l'autre résistance thermique, de telle sorte que la différence entre les valeurs instantanées des résistances électriques prend une valeur pour laquelle le circuit électrique 6a active l'élément fonctionnel 2.

Par contre, si l'utilisateur place une carte dans une atmosphère homogène froide ou chaude, la différence entre les valeurs instantanées des résistances électriques sera pratiquement nulle et l'élément fonctionnel 1 ne sera pas activé.

Si maintenant la température de l'une des parties du corps 1 qui est adjacente à une résistance thermique subit une variation importante, et si la différence entre les valeurs instantanées des résistances électriques des deux résistances thermiques est supérieure à la valeur maximale de la plage de valeurs prédéterminée, l'élément fonctionnel 2 ne sera toujours pas activé.

La carte électronique représentée sur la figure 3 pourrait ne comporter qu'une seule

résistance thermique.

Dans ce cas, le circuit électronique 6a pourrait être réalisé de telle sorte que l'élément fonctionnel 2 ne soit activé que si l'utilisateur, en appliquant un doigt sur la partie du corps 1 qui est adjacente à la résistance thermique, amène la résistance électrique de celle-ci à prendre une valeur située dans une plage de valeurs prédéterminée.

Afin de réduire encore les risques d'une activation intempestive de l'élément fonctionnel 2, le circuit électronique 6a pourrait également être conçu de façon à ce que ce dernier ne soit activé que si la valeur de la résistance thermique varie à une vitesse située dans une plage de vitesses prédéterminée.

La carte électronique représentée sur la figure 4 diffère des cartes décrites précédemment en ce que les jauges de contrainte et les résistances thermiques ont été remplacées par deux thermocouples 4b,5b.

Son circuit électronique 6b est quant à lui conçu de façon à activer l'élément fonctionnel 2 lorsque la différence des valeurs instantanées des forces électromotrices créées dans les deux thermocouples est située dans une plage de valeurs prédéterminée.

Lorsque l'utilisateur applique un doigt sur la partie du corps 1 qui est adjacente à un thermocouple, celui-ci s'échauffe tandis que l'autre thermocouple demeure à la température ambiante.

La force électromotrice du thermocouple qui est chauffée varie par rapport à celle de l'autre thermocouple de telle sorte que la différence entre les valeurs instantanées des forces électromotrices prend une valeur pour laquelle le circuit électronique 6b active l'élément fonctionnel 2.

Par contre, si l'utilisateur place une carte dans une atmosphère homogène froide ou chaude, la différence entre les valeurs instantanées des forces électromotrices sera pratiquement nulle et l'élément fonctionnel 2 ne sera pas activé.

Si maintenant la température de l'une des parties du corps 1 qui est adjacente à un thermocouple subit une variation importante, et si la différence entre les valeurs instantanées des forces électromotrices des deux thermocouples est supérieure à la valeur maximale de la plage de valeurs prédéterminée, l'élément fonctionnel 2 ne sera toujours pas activé.

La carte électronique représentée sur la figure 4 pourrait ne comporter qu'un seul thermocouple.

Dans ce cas, le circuit électronique 6b pourrait être réalisé de telle sorte que l'élément fonctionnel 2 ne soit activé que si l'utilisateur, en appliquant un doigt sur la partie du corps 1 qui est adjacente au thermocouple, fait prendre à la force électromotrice de celui-ci, une valeur située dans une plage de valeurs prédéterminée.

Afin de réduire encore les risques d'une activation involontaire de l'élément fonctionnel 2, le circuit électronique 6b pourrait également être conçu de façon à n'activer ce dernier que si la valeur de la force électromotrice varie à une vitesse située dans une plage de vitesses prédéterminée.

Dans les trois modes de réalisation qui ont été décrit ci-dessus, les jauges de contrainte, les résistances thermiques et les thermocouples sont encastrés dans le corps des cartes électroniques. Il va de soi cependant qu'ils pourraient être situés dans le plan de l'une des grandes faces desdites cartes.

La carte électronique représentée sur la figure 5 diffère des cartes décrites ci-dessus en ce qu'elle comporte deux électrodes adjacentes 4c,5c sur chacune de ses grandes faces, les deux paires d'électrodes remplaçant les jauges de contrainte ainsi que les résistances thermiques et les thermocouples.

Son circuit électronique 6c est quant à lui conçu de façon à activer l'élément fonctionnel 2 lorsque l'utilisateur, en appliquant un doigt sur chaque paire d'électrodes, permet l'établissement d'impédances de même valeur et variant à la même vitesse.

Cette solution a en effet été adoptée afin d'éviter qu'un phénomène involontaire d'électrostriction fasse apparaître de l'électricité statique et provoque une activation intempestive de l'élément fonctionnel.

On remarquera que les électrodes situées sur l'une des grandes faces de la carte sont en face des électrodes situées sur l'autre face de cette dernière pour d'évidentes raisons d'ergonomie.

La carte électronique représentée sur la figure 5 pourrait ne comporter qu'une seule paire d'électrodes sur l'une de ses grandes faces.

Dans ce cas, le circuit électronique pourrait être réalisé de telle sorte que l'élément fonctionnel 2 ne soit activé que si l'utilisateur, en appliquant un doigt sur les deux

électrodes, fait varier l'impédance à une vitesse située dans une plage de vitesses prédéterminée.

On notera par ailleurs qu'il est souhaitable de blinder le circuit électronique 6c et les autres circuits qui lui sont associés afin d'éviter la formation de décharges électrostatiques.

Pour être complet, on précisera que les cartes électroniques conformes à l'invention comportent un corps réalisé à partir de deux plaques de matière plastique fixées l'une contre l'autre par collage ou toute autre technique équivalente, l'élément fonctionnel 2, la source d'énergie 3, et le circuit électronique 6 étant situés entre ces deux plaques tout comme les jauges de contrainte 4,5, les résistances thermiques 4a,5a ou les thermocouples 4b,5b.

Enfin, on notera que la présente invention couvre également une carte électronique dont le corps serait pourvu d'une combinaison d'au moins deux éléments sensibles différents pris parmi ceux décrits ci-dessus.

REVENDICATIONS

1. Carte électronique comprenant un corps en matière plastique (1) renfermant un élément fonctionnel (2) alimenté par une source d'énergie (3), caractérisée en ce que la source d'énergie est reliée à un élément sensible (4,4a,4b,4c) dans lequel une grandeur physique varie lorsqu'il est soumis à une action manuelle volontaire, et à un circuit électronique (6,6a,6b,6c) apte à fournir un signal de commande à l'élément fonctionnel en réponse à un signal émis par l'élément sensible et correspondant à une valeur de la grandeur physique, située dans une plage de valeurs prédéterminée.

2. Carte électronique selon la revendication 1, caractérisée en ce que le circuit électronique (6,6a,6b,6c) ne délivre le signal de commande que lorsque la valeur de la grandeur physique varie à une vitesse située dans une plage de vitesses prédéterminée.

3. Carte électronique selon la revendication 1 ou 2, caractérisée en ce que l'élément sensible est une jauge de contrainte (4) disposée dans le corps en matière plastique (1) tandis que la grandeur physique est un courant électrique dont l'intensité varie lorsque le corps en matière plastique est soumis à une flexion manuelle dans une zone adjacente à la jauge de contrainte.

4. Carte électronique selon la revendication 3, caractérisée en ce qu'une seconde jauge de contrainte (5) reliée au circuit électronique est disposée dans le corps en matière plastique (1), le circuit électronique (6) fournissant le signal de commande à l'élément fonctionnel (2) lorsque la différence des valeurs instantanées des courants électriques traversant les jauges de contrainte (4,5) est située dans une plage de valeurs prédéterminée.

5. Carte électronique selon la revendication 1 ou 2, caractérisée en ce que l'élément sensible est une résistance thermique (4a) tandis que la grandeur physique est la résistance électrique de la résistance thermique, qui varie lorsque celle-ci est chauffée par un doigt appliqué volontairement contre elle.

6. Carte électronique selon la revendication 5, caractérisée en ce qu'une seconde résistance thermique (5a) est reliée au circuit électronique (6a), celui-ci fournissant le signal de commande à l'élément fonctionnel (2) lorsque la différence des valeurs instantanées des résistances électriques des deux résistances thermiques est située dans une plage de valeurs déterminée.

7. Carte électronique selon la revendication 1 ou 2, caractérisée en ce que l'élément sensible est un thermocouple (4b) tandis que la grandeur physique est une force électromotrice dont la grandeur varie lorsque le thermocouple est chauffé par un doigt appliqué volontairement contre lui.

8. Carte électronique selon la revendication 7, caractérisée en ce qu'un second thermocouple (5b) est relié au circuit électronique (6b), celui-ci fournissant le signal de commande à l'élément fonctionnel (2) lorsque la différence des valeurs instantanées des forces électromotrices créées dans les deux thermocouples (4a,5b) est située dans une plage de valeurs prédéterminée.

9. Carte électronique selon la revendication 1 ou 2, caractérisée en ce que l'élément sensible est constitué par deux électrodes adjacentes (4c) disposées sur le corps en matière plastique (1) tandis que la grandeur physique est l'impédance établie entre les deux électrodes et variant lorsqu'un doigt est appliqué volontairement contre lesdites électrodes.

10. Carte électronique selon la revendication 9, caractérisée en ce que deux autres électrodes adjacentes (5c) reliées au circuit électronique (6c) sont disposées sur le corps en matière plastique (1), le circuit électronique fournissant le signal de commande à l'élément fonctionnel (2) lorsque les impédances respectivement établies entre les électrodes appariées (4c,5c) sont les mêmes et varient à la même vitesse.

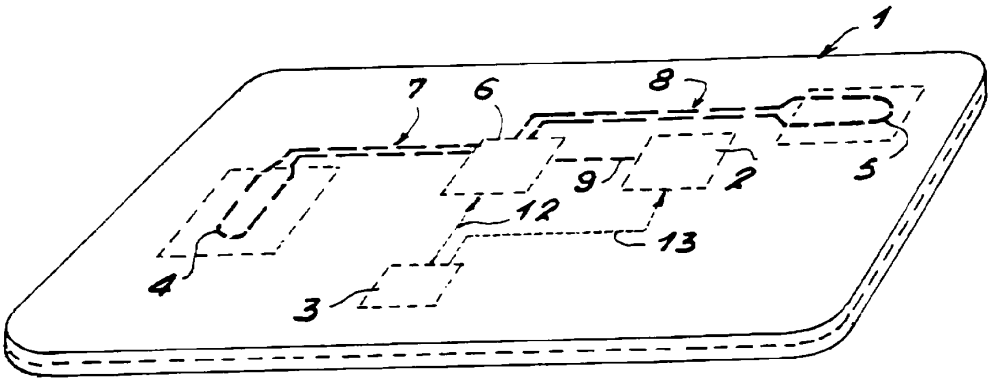


FIG. 1

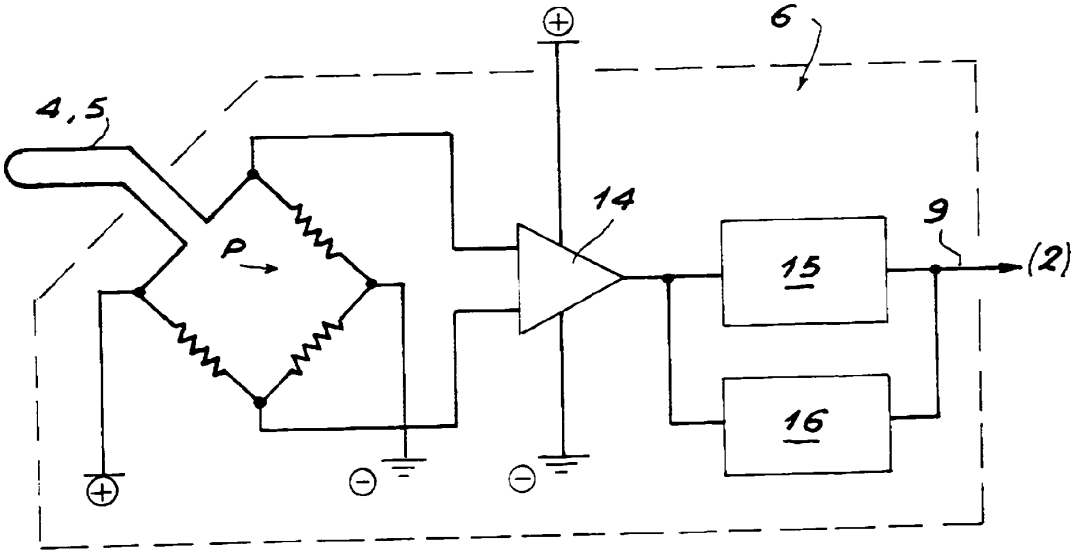


FIG. 2

FIG. 3

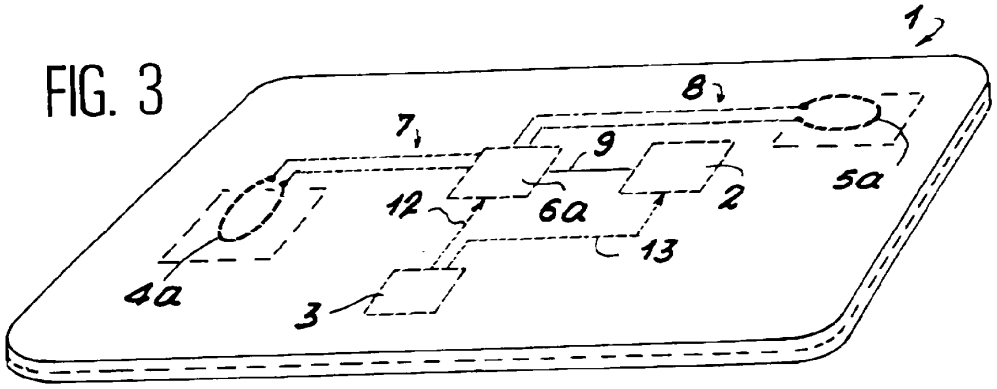


FIG. 4

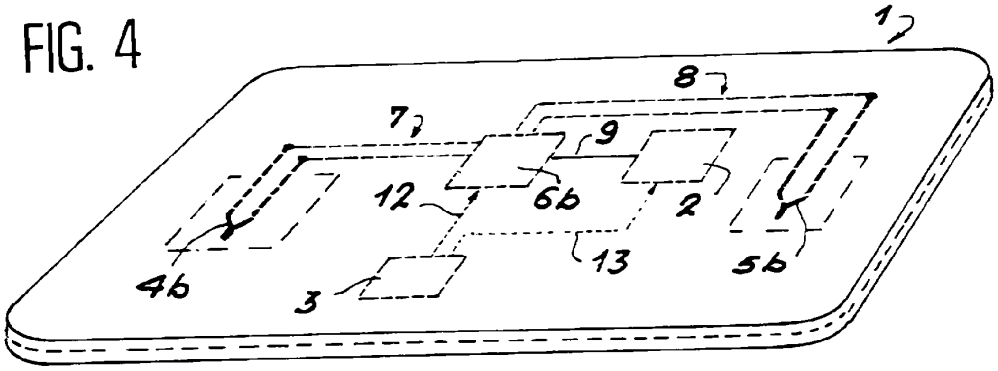
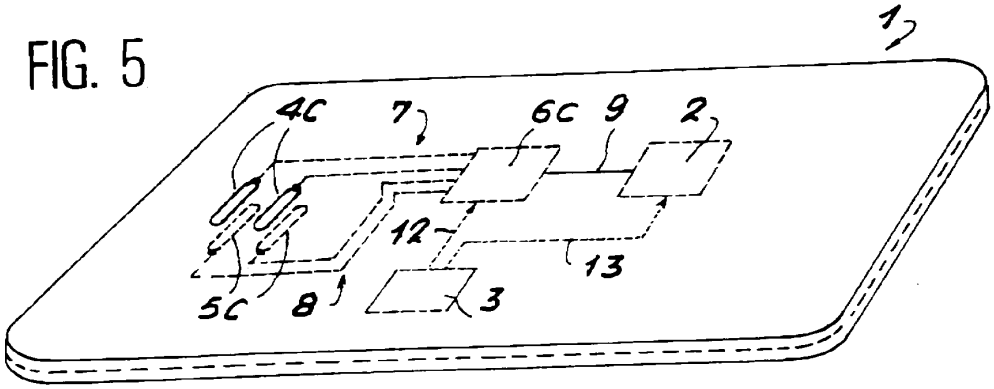


FIG. 5



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2728710
N° d'enregistrement national

FA 508980
FR 9415570

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	EP-A-0 408 456 (GEMPLUS CARD INT) 16 Janvier 1991 * le document en entier * ---	1,3,4,9, 10
X	PATENT ABSTRACTS OF JAPAN vol. 012 no. 123 (P-690) ,16 Avril 1988 & JP-A-62 248085 (NEC CORP) 29 Octobre 1987, * abrégé * ---	1
X	PATENT ABSTRACTS OF JAPAN vol. 015 no. 139 (E-1053) ,9 Avril 1991 & JP-A-03 019380 (CANON INC) 28 Janvier 1991, * abrégé * ---	1
X	EP-A-0 509 567 (PHILIPS NV) 21 Octobre 1992 * le document en entier * -----	1,2

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
G06K

1

Date d'achèvement de la recherche	Examinateur
29 Septembre 1995	Gysen, L

EPO FORM 1503 03.82 (P04C13)

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : **G06K 19/077**	**A1**	**(11) Internationale Veröffentlichungsnummer: WO 98/20450** **(43) Internationales Veröffentlichungsdatum:** 14. Mai 1998 (14.05.98)

(21) Internationales Aktenzeichen: PCT/EP97/05996

(22) Internationales Anmeldedatum: 30. Oktober 1997 (30.10.97)

(30) Prioritätsdaten:
196 45 083.7 1. November 1996 (01.11.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: AUSTRIA CARD GMBH [AT/AT]; Lamezanstrasse 4–8, A–1232 Wien (AT).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: PRANCZ, Markus [AT/AT]; Treustrasse 3/12, A–1200 Wien (AT).

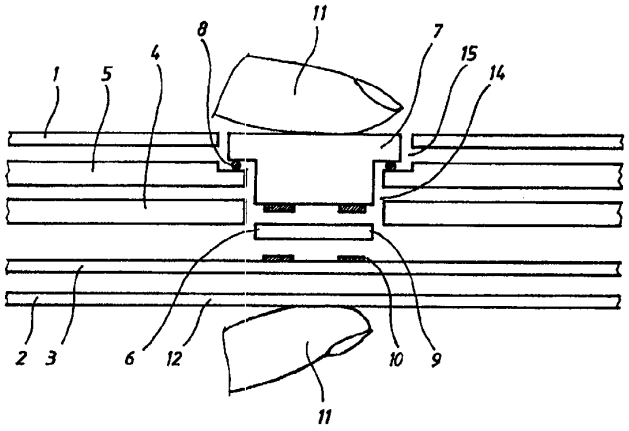
(74) Anwalt: RIEBLING, Peter; Postfach 3160, D–88113 Lindau (DE).

(81) Bestimmungsstaaten: CZ, HU, JP, PL, RU, SI, SK, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: CONTACTLESS SMART CARD WITH A TRANSPONDER COIL

(54) Bezeichnung: KONTAKTLOSE CHIPKARTE MIT TRANSPONDERSPULE



(57) Abstract

The invention relates to an ID card with a transaction coil and a method for the production thereof. The transaction coil is configured as a screen–printed silver or conductive paste which is built into a plastic card body corresponding to usual ISO standards. A milling process enables the ends of said coil to be laid bare in order to implant a special chip module or the contact ends are already bare if a lamination or injection moulding process is used. Contacting of said coil can only occur when pressure is consciously applied. The coil is automatically deactivated when pressure ceases.

(57) **Zusammenfassung**

Die Erfindung betrifft eine Identifikationskarte mit Transaktionsspule und ein Verfahren zu deren Herstellung. Die Transaktionsspule ist in Form einer Silber- bzw. allg. Leitpasten-Siebdruckausführung ausgebildet, die in eine den üblichen ISO Normen entsprechenden Kunststoff-Kartenkörper eingebracht werden und deren Enden anschließend mittels Fräsprozeß für die Implantation eines speziellen Chipmoduls freigelegt werden oder deren Kontaktenden bereits im Laminier- oder Spritzgußvorgang freigehalten worden sind und dessen Kontaktierung nur durch eine bewußte Druckaufbringung erfolgen kann und automatisch nach Beendigung dieses Druckaufbringens inaktiv wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Repnblik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Kontaktlose Chipkarte mit Transponderspule

Die Erfindung betrifft eine kontaktlose Chipkarte mit Transponderspule und ein Verfahren zu deren Herstellung.

Gegenstand der vorliegenden Erfindung ist eine Identifikationskarte mit Transponderspule und eingebautem Chipmodul, wobei die auf dem Chipmodul gespeicherten Daten ausgelesen und mit Hilfe der Transponderspule kontaktlos auf einen Empfänger übertragen werden können.

Identifikationskarten zur kontaktlosen Transaktion werden entsprechend den ISO/IEC DIS 10536 Normen für die unterschiedlichsten Anwendungen einer Standardisierung unterworfen. Zielsetzung aller dieser Normen ist die Erhöhung der Sicherheit und der Geschwindigkeit von Identifikations- und Transaktionsvorgängen bei gleichzeitiger Reduktion der integralen Kosten und einer weltweiten Anwendung und gewissen Kompatibilität.

Identifikationsvorgänge mittels sogenannter handgehaltener berührungsloser Identifikationskarten werden in immer stärkerem Ausmaß im öffentlichen Personen und Nahverkehr bzw. ganz allgemein zur komfortablen und raschen Identifikation bzw. Zutrittskontrolle und oftmals der vollautomatischen Abbuchung entsprechender Werteinheiten oder Geldbeträge verwendet.
Im überwiegenden Maße wird diese rasche und unbemerkte Identifikation sinnvoll und vom Besitzer voll akzeptiert stattfinden.

Bei mißbräuchlichem Einsatz ist der Benutzer ziemlich machtlos und kann erst rückwirkend diesen Mißbrauch feststellen. Aus diesem Grund werden reine Geldtransaktionen

bevorzugt mittels kontaktbehafteter Chipkarten durchgeführt und der Transaktionsvorgang bewußt und oftmals nur nach Eingabe einer persönlichen Identifikationsnummer (PIN) durchgeführt.

Bei allen Arten von Identifikationskarten Applikationen mittels berührungsloser Transponder-Chipkarten müssen die Aspekte der länderweit durchaus sehr unterschiedlichen Datenschutzgesetze und Verordnungen bzw. ganz allgemein der guten Sitten berücksichtigt werden.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, eine Chipkarte der eingangs erwähnten Art so weiterzubilden, daß mittels eines möglichst kostengünstigen Prozesses ein möglichst einfach anwendbares Produkt dem Benutzer einer derartigen berührungslos funktionierenden Chipkarte die Möglichkeit gibt, den Vorgang der Identifikation und Transaktion bewußt herbeizuführen und weiters damit jegliche Kollision oder Konfrontation mit dem Datenschutzgesetz zu vermeiden.

Die Lösung dieser Aufgabe ist durch die technischen Merkmale des Anspruchs 1 gegeben.

Ein Herstellungsverfahren der erfindungsgemäßen Chipkarte ist Gegenstand des unabhängigen Anspruchs 11.

Wesentlich bei der vorliegenden Erfindung ist demnach die bewusste Schaltung einer Transponderspule, wobei bevorzugt die Kontaktflächen der Transponderspule mit zugeordneten Kontaktflächen eines Chipmoduls durch die willkürliche Schaltung miteinander verbunden werden.

In einer ersten, bevorzugten Ausführungsform erfolgt diese Durchschaltung der Kontaktflächen der Transponderspule zu den Kontaktflächen des Chipmoduls über ein ohmsches

Kontaktelement, welches z.B. aus einem drucksensitiv-leitenden Silikongummi besteht, welches als Kontaktmaterial im Zwischenraum zwischen den beiden einander gegenüberliegenden Kontaktflächen liegt und - sobald der Luftzwischenraum zwischen den Kontaktflächen komprimiert wird, kommt dieses Kontaktelement sowohl in direkten ohmschen Kontakt mit den Kontaktflächen der Transponderspule als auch mit den gegenüberliegenden Kontaktflächen des Chipmoduls.

Der vorliegenden Erfindung liegt nun die Erkenntnis zugrunde, daß die Implantation eines Chipmoduls mit Kontaktflächen in der Karte und der Kontakt mit den beiden Enden der Spule prozeßtechnisch sehr einfach mittels sogenannter druckempfindlicher leitfähiger Silikon-Gummi-Matten mit Silberkügelchen herbeigeführt werden kann, und in einer weiteren Ausführungsform, durch die Ausbildung des Kartenkörpers und des zu implantierenden Chipmoduls eine Art mechanischer Schalter derart hergestellt werden kann, daß im Ruhezustand ein entsprechender Luftspalt zwischen den Kontaktpartnern gegeben ist, der nur durch mechanischen Druck, beispielsweise durch Fingerdruck, im Bereich des Chipmoduls überbrückt werden kann und dadurch zum Kontakt zwischen Chipmodul und Transponderspule und damit zur Aktivierung der Transponder-Chip Einheit führt.

In einer weiteren typischen Ausführungsform kann das Chipmodul ein sogenanntes Hybridmodul sein, das entweder zwei Chips beinhaltet, wobei ein Chip für die berührungslose Transaktion und ein zweiter Chip für die standardmäßige kontaktbehaftete Transaktion zuständig ist, oder aber einen Kombinationschip enthalten, der beide Funktionen in einem Chip vereint. In beiden Fällen müssen die Kontakte für die Transponderspule an der Unterseite bzw. Innenseite des Chipmoduls liegen, respektive auf der Seite, die den

Kontaktflächen des kontaktbehafteten Chipmoduls gegenüberliegt.

In einer Weiterbildung der vorliegenden Erfindung ist es vorgesehen, daß die Schaltung der Transponderspule nicht durch willkürliche Schaltung eines Kontaktelements erfolgt, sondern daß die Schaltung durch ein externes Signal ausgelöst wird. Diese weiterführende technische Lehre hat den Vorteil, daß die Chipkarte nach der Erfindung gleichzeitig auch diebstahlgesichert ist. Ein externes Signal zum Schalten der Transponderspule wird beispielsweise von einem Personenerkennungssystem ausgelöst, welches z.B. visuell oder akustisch die Berechtigung des Benutzers zum Eintritt in einen bestimmten Bereich erkennt. Sobald dieses System den berechtigten Benutzer erkannt hat, wird ein derartiges externes Signal ausgelöst, welches dann die Transponderspule schaltet. Die Transponderspule liest dann die in dem Chipmodul gespeicherten Daten, wie z.B. Identifizierung, Zeitpunkt und andere Personendaten aus, wodurch sichergestellt ist, daß auch nur der berechtigte Benutzer dieser Chipkarte durch den geschützten Eingangsbereich gelangt.

Transaktions-Chipkarten sind durch den erforderlichen Aufbau und aufgrund der noch nicht in Großserien gefertigten Chiptypen bzw. Chipmodule üblicherweise teurer in der Herstellung und in Verbindung mit einer typischen Identifikationsanwendung häufiger und meist auch länger im Einsatz als herkömmliche kontaktbehaftete Chipkarten. An die Lebensdauer und Verwendungshäufigkeit derartiger handgehaltener Karten werden große Anforderungen gestellt und diesbezüglich stellt die Biegebeanspruchung ein wesentliches Kriterium dar. Eine Schwachstelle dabei sind die Kontakte und die Dimension der Chipfläche. In der vorliegenden Erfindung wird der feste mechanische Verbund zwischen Kartenkörper und Chipkontakten vermieden und damit

wesentlich geringere Anforderungen an die Spannungsrißfestigkeit der Kontaktelemente und die Gleichmäßigkeit der Wärmeausdehnungskoeffizienten der verschiedenen Verbundpartner gestellt.

Die Herstellung der Kartengrundkörper erfolgt in bekannter Weise einer typischen Ausführungsform dadurch, daß dünne Druckbögen mit typisch 80 bis 350 Mikrometer Dicke und Formaten für Mehrfachnutzen, typischerweise 24 bzw. 48 Karten pro Druckbogen mit Abmessungen von beispielsweise 30 x 50 cm oder 50 x 70 cm mit den in der Kreditkartenproduktion üblichen Offsetdrucken und Siebdrucken kundenspezifisch gestaltet werden und falls notwendig mit entsprechenden thermisch aktivierbaren Klebebeschichtungen, bevorzugt im Siebdruck, versehen werden.

Im folgenden wird eine Ausführungsform der Erfindung anhand von Zeichnungen näher erläutert. Hierbei gehen aus den Zeichnungen und ihrer Beschreibung weitere erfindungswesentliche Merkmale und Vorteile der Erfindung hervor.

Figur 1: zeigt den Schnitt durch den Chipmodulbereich einer Chipkarte nach der Erfindung,

Figur 2: die Draufsicht auf die Folie mit Darstellung der Transponderspule,

Figur 3: die Draufsicht auf die Oberseite der Chipkarte bei noch nicht eingesetztem Chipmodul und noch nicht eingesetztem Schaltelement,

Figur 4: eine Abwandlung gegenüber Figur 3.

Wie in Figur 1 gezeigt, werden beispielsweise je zwei typisch 80 my dicke, transparente Deckfolien 1 und 2 als sogenannte Overlayfolien verwendet. Diese transparenten Overlayfolien können nun wahlweise auf den Innenseiten mit thermisch aktivierbaren Schmelzklebern mittels Siebdruck oder direkt beim Folienzulieferanten beschichtet werden, wobei je nach geforderter Qualität als Material z.B. PVC-h, ABS, PET oder Polycarbonat (PC) eingesetzt werden kann und im weiteren dabei gegebenenfalls auf die Verwendbarkeit für Laserbeschriftungen und/oder Hochprägungen und/oder den Einbau eines Magnetstreifens geachtet werden muß.

Als nächste Schichten sind Folien 3 und 5 vorgesehen, wobei deren nach außen gerichtete Flächen grafisch mittels Offsetdruck und Siebdruck bzw. auch mittels der verschiedenen digitalen Druckverfahren kundenspezifisch gestaltet werden können. Üblicherweise werden diese Folien in neutralem Farbton und in Dicken von 80 my bis 350 my verwendet. Die innerste Schicht der Chipkarte bildet eine Kernfolie 4, die z.B. aus ABS- oder PC-Material besteht und eine Dicke von z.B. 300 my aufweist.

Im vorliegenden Beispiel wird die Folie 5 in einer Dicke von etwa 300 my eingesetzt und kann in Kombination mit einer PC-Deckfolie 1 z.B. aus ABS sein. In der Ausführung ABS wird entsprechend dem im Vergleich zu PC niedrigerem Schmelzpunkt eine bessere Fließeigenschaft erreicht, was unter Umständen einen homogeneren Laminataufbau bewirken kann.

Folie 3 wird in möglichst dünner Ausführung, typisch 80 my verwendet und wird bevorzugt aus PC-Material sein, um die Trocknungsvorgänge der aufgebrachten Silberpastendrucke auf der Innenseite ohne wesentliche Schrumpfung bestehen zu können. D.h. auf dieser 80 my PC-weiß Folie, die außen grafisch gestaltet ist, wird auf der Innenseite mittels Siebdruck, bevorzugt Zylindersiebdruck, eine sogenannte Transponderspule 13 gedruckt. Dabei werden handelsübliche

Silberpasten, bevorzugt mit guter elektrischer Leitfähigkeit und geeignet für den Kunststoff-Foliendruck eingesetzt. Derartige Silberpasten werden bei der Herstellung flexibler Leiterplatten aus Polyester- und Polyamidfolien verwendet und können bei etwa 120°C getrocknet werden, ohne daß eine maßliche Beeinträchtigung dieser PC-Folien stattfindet, was natürlich für diesen Mehrfachnutzenaufbau sehr wesentlich ist.

Die Geometrie der Transponderspule wird je nach Anforderung an die Eigenschaften der Spule 13, d.h. die Anforderung an den Sende- und Empfangsvorgang und die Höhe der erzeugten Induktionsspannung in der Spule - zwecks Stromversorgung des Halbleiterbausteins - gewählt werden.

Dabei können die Anzahl der Windungen, die Leiterbahnbreite und der Leiterbahnabstand, die Formen der Anschlußkontakte 10 und natürlich die Dicke des Leitpastenaufbaues bzw. die Art der verwendeten Leitpaste variiert werden. Typischerweise werden einige 3 bis 5 Windungen mit Leiterbahnbreiten im Bereich 100 my bis 1 mm gewählt werden. Um den ohmschen Widerstand möglich niedrig zu halten, werden u.U. mehrere übereinanderliegende Drucke durchgeführt. In einer kostengünstigeren Variante können die Silberpasten auch durch Karbonpasten, Kupferpasten oder Mischen aus den verschiedenen Leitpastentypen erfolgen.

Ein sehr wesentliches Detail stellt die Art der Anschlußkontakte 10, d.h. die Ausbildung der Enden der Spule 13 dar, da diese zur Kontaktierung des Chipmoduls 7 benötigt werden.

In der vorliegenden Erfindung ist nun sehr wesentlich, daß die Anschlußflächen 9 des Chipmoduls 7 auf der Unterseite, d.h. der Seite, die in Kontakt zu den Spulen-Anschlußkontakten 10 treten sollen, liegen und einen entsprechend weiten Abstand haben, so daß die Bahnen der Spule 13 dazwischen durchgeführt werden können und die Enden der Spule 13 relativ großflächig ausgeführt werden können.

Übliche Leitpastendrucke in Einfach- und Mehrfachdruckausführung weisen eine Dicke von 10 bis 30 my auf, typisch 15 bis 20 my im getrockneten Zustand. Die Freifräsung der Ausnehmungen 14 und 15 im Anschluß an die Lamination des gesamten aus den Folienlagen 1-5 bestehenden Paketes muß nun sehr exakt auf die erforderliche Tiefe eingestellt werden, um einerseits die Leitpaste der Transponderspule 13 elektrisch freizulegen, jedoch andererseits keine zu starke Reduktion der Leitpastendicke und damit Reduktion des Leitungsquerschnittes der Spule 13 herbeizuführen.

Übliche Fräsanlagen für die Vertiefungen von Chipmodulen arbeiten mit Toleranzen bis zu +/-10 my. Im vorliegenden Fall ist jedoch eine Toleranz von vorzugsweise +/-3 my anzustreben. Dabei spielt noch die Dicken-Toleranz der Folienlagen 2 und 3 eine sehr wesentliche Rolle, da diese in die Toleranzrechnung mit einbezogen werden müssen.

Diese sehr genaue mechanische Freilegung der Kontakte 10 der Spule 13 ist in der vorliegenden Erfindung gegenüber dem Stand der Technik insofern von Bedeutung, als üblicherweise derart freigelegte Kontakte 10 mittels Leitkleber oder Leitpaste kontaktiert werden und damit den Flächenleitwert verbessern.

In der vorliegenden Erfindung werden jedoch diese Anschlußflächen 10 der Spule 13 nur mittels eines Schaltelements 6 kontaktiert. Dieses Schaltelement 6 kann beispielsweise aus sogenannten druckempfindlich-leitenden Gummimatten in Materialstärken von z.B. 0,2 bis 0,3 mm bestehen bzw. aus einzelnen Kontaktelementen pro Anschluß 10a bzw. 10b.

Derartige Gummimatten werden üblicherweise mit Nickelkügelchen oder Silberkügelchen in Form einer Matrix hergestellt und werden erst bei Druck leitend. Gemäß dem Stand der Technik werden derartige Drucksensitiv-leitende Gummimatten z.B. zur Kontaktierung von Glassubstraten, typisch LCD's und Bildschirmen als auch flexiblen Substraten

verwendet und dabei wird mittels entsprechender Klammern Druck über entsprechenden Anschlußflächen hergestellt.

Im vorliegenden Fall können mittels derartiger drucksensitiv-leitender Gummimatten sehr einfache und effiziente Schalter hergestellt werden, die auf extrem geringen Raum einen funktionellen Kontakt ohne starke Deformationsvorgänge in den einzelnen Lagen der Identifikationskarte herstellen können.

In einer weiteren Ausführungsform ist vorgesehen, die Dicken der einzelnen Folienlagen 1-5 der ID-Karte derart abzustimmen, daß die Lagen 2 und 3 als Membrane verwendet werden können und zwischen sich einen Luftspalt einschließen, der durch Druckaufbringung überbrückt und somit ein Kontakt zwischen Chipmodul 7 und Transponderspule 13 hergestellt werden kann. Dabei werden die Leitpastenkontaktflächen 10 der Spule 13 mit den Kontaktflächen 9 des Chipmoduls 7 zusammengepreßt und dadurch die Funktion der Transponder-Chipkarte aktiviert. Das System ist ebenfalls ohne bewußte Druckaufbringung nicht aktiv und es kann daher keinerlei unbewußte Identifikation oder Transaktion stattfinden.

In Erweiterung dieser genannten Ausführungsform können nach deren Freilegung auf die Anschlußflächen 10 der Leitpastenkontaktflächen leitfähige elastomere Kontaktelemente mittels Dispenser oder Tampondruck aufgebracht werden, so daß im Falle des Druckaufbringens ein elastisches leitendes Element zwischen den Kontakten 9 und 10 vorhanden ist und damit zu einer optimalen Kontaktsicherheit führt.

Die Ausführung des Chipmoduls 7 wird geometrisch gemäß dem Stand der Technik ausgeführt, allerdings mit nach innen zur Transponderspule gerichteten Kontaktflächen 9, bevorzugt in vergoldeter bzw. auch verzinnter oder vernickelter

Oberflächenausführung. Wahlweise kann das Chipmodul noch mit oberseitigen Kontakten für die Kontaktierung eines kontaktbehafteten Chipsystems ausgeführt werden, wobei je nach Kundenwunsch ein oder zwei Halbleiterelemente zum Einsatz gelangen. Die mechanische Fixierung des Chipelements 7 erfolgt in einer formangepassten Ausfräsung 14, 15 der Folienschichten 1, 5 und 4 mittels einer Klebebefestigung 8. Dadurch werden optimale Festigkeitswerte hinsichtlich der Biegewechselfestigkeit erreicht, als auch eine optimale Abdichtung des Innenraums (Kontaktraumes) gegen etwaige Silbermigration der Silberleitpaste. Weiters kann mittels dieses dem Stand der Technik entsprechenden Prozesses eine exakte Planheit der Oberflächen erreicht werden.

Die Figuren 3 und 4 zeigen eine Draufsicht auf die Oberseite (Deckfolienlage 1) der Chipkarte bei noch nicht eingesetztem Chipmodul und noch nicht eingesetztem Schaltelement. Man erkennt im Bereich der Ausfräsung einen Ausschnitt der Folienlage 3 mit aufgebrachter Transponderspule und deren Kontaktanschlüssen 10. Die Kontaktanschlüsse 10 können z.B. punktförmig 10a oder zur Vergrößerung der Kontaktfläche oval 10b ausgebildet sein. Die Ausfräsung vergrößert sich hin zur Kartenoberfläche (vgl. Figur 1) und man erkennt einen Teil der Folienlage 5, mit welcher später das Chipmodul 7 verklebt oder verschweißt wird.

Zeichnungslegende

1	Deckfolie
2	Deckfolie
3	Folie
4	Kernfolie
5	Folie
6	Schaltelement
7	Chipmodul
8	Kleber
9	Kontaktfläche
10	Kontaktfläche (10a, 10b)
11	Finger
12	Kunststofflage
13	Transponderspule
14	Ausnehmung
15	Ausnehmung

Patentansprüche

1. Kontaktlose Chipkarte mit Transponderspule und eingebautem Chipmodul, wobei die auf dem Chipmodul gespeicherten Daten ausgelesen und mit Hilfe der Transponderspule kontaktlos auf einen Empfänger übertragen werden können, dadurch gekennzeichnet, daß die Transponderspule (13) zur bewussten Aktivierung und damit Auslösung einer Identifikation oder Transaktion der Chipkarte schaltbar ausgebildet ist.

2. Kontaktlose Chipkarte nach Anspruch 1, dadurch gekennzeichnet, daß die Schaltung der Transponderspule (13) willkürlich, z.B. durch Fingerdruck erfolgt.

3. Kontaktlose Chipkarte nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die willkürliche Schaltung der Transponderspule (13) durch einen ohmschen Kontaktschluss zwischen Kontaktflächen (10) der Transponderspule (13) und entsprechenden Kontaktflächen (9) des Chipmoduls (7) erfolgt.

4. Kontaktlose Chipkarte nach Anspruch 1, dadurch gekennzeichnet, daß die Schaltung der Transponderspule (13) durch ein externes Signal verursacht wird.

5. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 4, dadurch gekennzeichnet, daß die Chipkarte aus mehreren Folienschichten besteht und zumindest zwei Deckschichten (1,2) und eine oder mehrere Zwischenschichten (3-5) aufweist.

6. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 5, dadurch gekennzeichnet, daß die Chipkarte eine Ausnehmung (14,15) aufweist, die sich vorzugsweise über die

Folienschichten (1,4,5) erstreckt, wobei das Chipmodul (7) in der Ausnehmung (14,15) angeordnet ist.

7. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 6, dadurch gekennzeichnet, daß das Chipmodul (7) in Richtung zur Transponderspule (13) gerichtete Kontaktflächen (9) aufweist.

8. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 7, dadurch gekennzeichnet, daß die Transponderspule (13) auf einer der Zwischenschichten (3-5) aufgebracht ist und im Bereich der Ausnehmung (14,15) angeordnete Kontaktflächen (10) aufweist.

9. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 8, dadurch gekennzeichnet, daß zwischen den Kontaktflächen (9) des Chipmoduls und den Kontaktflächen (10) der Transponderspule (13) eine drucksensitiv-leitende Gummimatte (6) angeordnet ist, die ohne Druckbeaufschlagung isolierend wirkt und nur bei hinreichendem Druck leitend wird und dadurch einen Kontakt zwischen den Kontaktflächen (9, 10) herstellt.

10. Kontaktlose Chipkarte nach Anspruch 9, dadurch gekennzeichnet, daß die Gummimatte (6) aus einer Silikongummimatte mit matrixförmig angeordneten Silber- bzw. Nickelkügelchen besteht.

11. Verfahren zur Herstellung einer kontaktlosen Chipkarte gemäß einem der Ansprüche 1 bis 10, dadurch gekennzeichnet,

daß mehrere übereinanderliegende Folienschichten miteinander zu einer Chipkarte verbunden werden,

daß zuvor eine der inneren Folienschichten mit einer elektrisch leitenden Transponderspule bedruckt wird, wobei an den Enden der Transponderspule Kontaktflächen vorgesehen werden,

daß durch einen Fräsvorgang an der Chipkarte, im Bereich der Kontaktflächen, eine Ausnehmung zur Aufnahme des Chipmoduls geschaffen wird, wobei die Ausfräsung bis zur mit der Transponderspule bedruckten Folienschicht reicht,

daß das Chipmodul derart in die Ausnehmung eingesetzt wird, daß dessen Kontaktflächen in einem Abstand zu den Kontaktflächen der Transponderspule zu liegen kommen, so daß sich die Kontaktflächen nicht berühren.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß zwischen die Kontaktflächen der Chipmoduls und die zugeordneten Kontaktflächen der Transponderspule ein drucksensitiv-leitendes Schaltelement eingelegt wird.

13. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß auf die Kontaktflächen der Transponderspule nach deren mechanischem Freilegen mittels eines Fräsprozesses mittels Dispenser oder Tampondruck elastische leitende Kontaktpunkte aufgebracht werden, welche bevorzugt aus Silber-, Karbon-, Kupfer- oder Nickel- gefüllten Elastomerpasten bestehen.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die Elastomerpasten aus Silikongummi mit typisch 1-10 mOhm*cm Volumenwiderstand bestehen und im Falle des Zusammendrückens einen guten und elastischen und damit sicheren elektrischen Kontakt ermöglichen.

15. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß durch den Freifräsprozeß der Ausnehmung für das Chipmodul nicht die gesamte Fläche bis zu der Oberfläche der Transponderspule freigelegt wird, sondern lediglich selektiv im Bereich der beiden Kontaktflächen mittels spezieller Stirnfräser und entsprechend erhöhter z-Achsen Genauigkeit und anschließend in diese Vertiefungen entsprechende Elastomerkontaktelemente eingebracht werden, die mittels

Druckbeaufschlagung zu einer Aktivierung des Transponder-Chip-Systems führen.

1/1

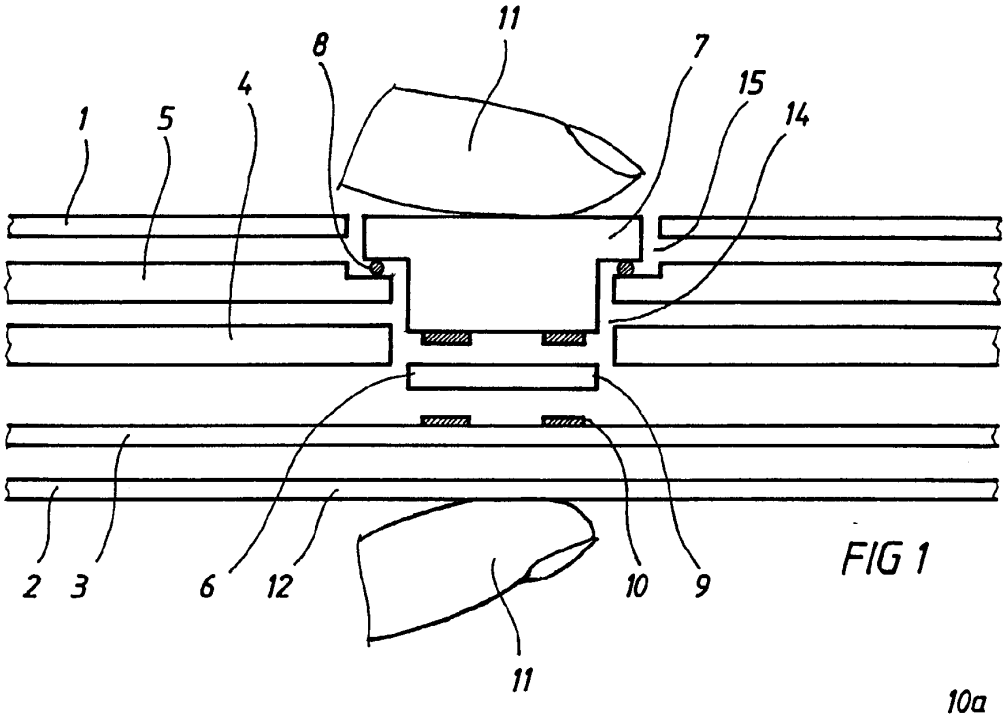


FIG 1

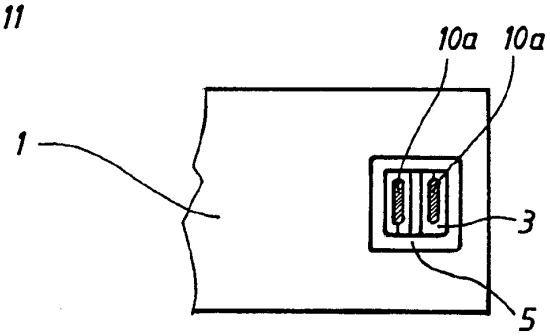


FIG 3

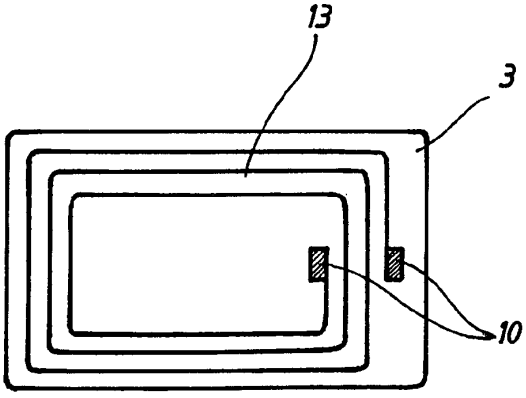


FIG 2

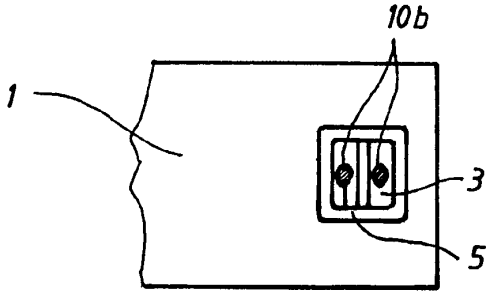


FIG 4

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/EP 97/05996

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K19/077

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 44 03 753 C (ANGEWANDTE DIGITAL ELEKTRONIK) 20 July 1995 see claim 1	1,2.5-8
X	DE 42 05 827 A (ANGEWANDTE DIGITAL ELEKTRONIK) 2 September 1993 see claim 1	1,2
X	EP 0 557 934 A (ANGEWANDTE DIGITAL ELEKTRONIK) 1 September 1993 see claim 1	1,2
A	DE 39 35 364 C (ANGEWANDTE DIGITAL ELEKTRONIK) 23 August 1990 see column 1, line 62 - line 65	4

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
3 April 1998	09/04/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Herskovic, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/EP 97/05996

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 682 321 A (GIESECKE & DEVRIENT GMBH) 15 November 1995 see the whole document -----	11

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/EP 97/05996

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4403753 C	20-07-95	AU 1574395 A	29-08-95
		CN 1140502 A	15-01-97
		WO 9522121 A	17-08-95
		EP 0744061 A	27-11-96
		EP 0751478 A	02-01-97
		JP 9507931 T	12-08-97
DE 4205827 A	02-09-93	DE 4305571 A	25-08-94
		EP 0562292 A	29-09-93
		JP 6004723 A	14-01-94
		US 5376778 A	27-12-94
		DE 4205556 A	26-08-93
		FR 2702065 A	02-09-94
		GB 2275554 A,B	31-08-94
EP 0557934 A	01-09-93	DE 4205556 A	26-08-93
		DE 4305571 A	25-08-94
DE 3935364 C	23-08-90	EP 0424726 A	02-05-91
		JP 3209592 A	12-09-91
		US 5206495 A	27-04-93
EP 0682321 A	15-11-95	DE 4416697 A	16-11-95
		JP 8044840 A	16-02-96

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 97/05996

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06K19/077

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 44 03 753 C (ANGEWANDTE DIGITAL ELEKTRONIK) 20.Juli 1995 siehe Anspruch 1	1,2,5-8
X	DE 42 05 827 A (ANGEWANDTE DIGITAL ELEKTRONIK) 2.September 1993 siehe Anspruch 1	1,2
X	EP 0 557 934 A (ANGEWANDTE DIGITAL ELEKTRONIK) 1.September 1993 siehe Anspruch 1	1,2
A	DE 39 35 364 C (ANGEWANDTE DIGITAL ELEKTRONIK) 23.August 1990 siehe Spalte 1, Zeile 62 - Zeile 65	4

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

1

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
3.April 1998	09/04/1998
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	**Bevollmächtigter Bediensteter** Herskovic, M

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Inte .ionales Aktenzeichen
PCT/EP 97/05996

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 682 321 A (GIESECKE & DEVRIENT GMBH) 15.November 1995 siehe das ganze Dokument	11

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 97/05996

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4403753 C	20-07-95	AU 1574395 A	29-08-95
		CN 1140502 A	15-01-97
		WO 9522121 A	17-08-95
		EP 0744061 A	27-11-96
		EP 0751478 A	02-01-97
		JP 9507931 T	12-08-97
DE 4205827 A	02-09-93	DE 4305571 A	25-08-94
		EP 0562292 A	29-09-93
		JP 6004723 A	14-01-94
		US 5376778 A	27-12-94
		DE 4205556 A	26-08-93
		FR 2702065 A	02-09-94
		GB 2275554 A,B	31-08-94
EP 0557934 A	01-09-93	DE 4205556 A	26-08-93
		DE 4305571 A	25-08-94
DE 3935364 C	23-08-90	EP 0424726 A	02-05-91
		JP 3209592 A	12-09-91
		US 5206495 A	27-04-93
EP 0682321 A	15-11-95	DE 4416697 A	16-11-95
		JP 8044840 A	16-02-96

Electronic Acknowledgement Receipt

EFS ID:	3869339
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	01-SEP-2008
Filing Date:	18-JUL-2007
Time Stamp:	12:15:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	F31_CA2279176A1.pdf	793154 355a4a6244a8b139e0ce5c118ad19a06837f5cbc	no	21

Warnings:	
Information:	

2	Foreign Reference	F32_DE10140662C1.pdf	403828 f6e5237b8fdc5c0454f2837569f1eb12c7a49e0d	no	8
Warnings:					
Information:					
3	Foreign Reference	F33_DE19542900A1.pdf	363672 59077e984a64ed0509ccf738c0dbf3206b376440	no	6
Warnings:					
Information:					
4	Foreign Reference	F34_DE19742126A1.pdf	162820 3de91caa15007a5e9f0d09c6b6fa3d88f16d889b	no	4
Warnings:					
Information:					
5	Foreign Reference	F35_FR2728710A1.pdf	532919 e29bf3b97961b305613903c5990efb5578bdcb83	no	14
Warnings:					
Information:					
6	Foreign Reference	F36_WO1998020450A1.pdf	890364 9384f418494fa47e67c7fb0bd7d1f7e413bfc603	no	24
Warnings:					
Information:					
		Total Files Size (in bytes):	3146757		

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Note: this is not an EFS form

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11779299** conf 1938
	Filing Date	**07/18/2007**
	First Named Inventor	**Finn**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Art Unit	
	Examiner Name	
Sheet 1 OF 2	Practitioner Docket No.	**C18**

U.S. PATENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY -or- MM/YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	4014602	03-29-1977	Ruell	
	2	4897644	01-30-1990	Hirano	
	3	5034648	07-23-1991	Gastgeb	
	4	5084699	01-28-1992	DeMichele	
	5	5376778	12-27-1994	Kreft	
	6	5399847	03-21-1995	Droz	
	7	5696363	12-9-1997	Larchevesque	
	8	5741392	04-12-1998	Droz	
	9	6111288	08-29-2000	Watanabe, et al.	
	10	6343744	02-05-2002	Shibata, et al.	
	11	6424029	07-23-2002	Giesler	
	12	6522308	02-18-2003	Mathieu	
	13	6575374	06-10-2003	Boyadjian , et al.	
	14	6879424	04-12-2005	Vincent, et al.	
	15	7054050	05-30-2006	Vincent, et al.	
	16	7093499	08-22-2006	Baudendistel	
	17	7145432	12-05-2006	Lussey , et al.	

U.S. PATENT APPLICATION PUBLICATIONS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY -or- MM/YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	A1	20030132301	07-17-2003	Selker	
	A2	20060255903	11-16-2006	Lussey et al.	
	A3	20070290051	12-20-2007	Bielmann et al.	

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	F1	CA 2279176	07-30-1998	Rietzler Manfred See also WO98/33142	
	F2	DE 10140662	03-20-2003	Osterwald et al.	
	F3	DE 19542900	05-22-1997	Michalk et al	
	F4	DE 19742126	03-25-1999	Hoedeau et al	
	F5	FR 2728710	06-28-1996	Larchevesque et al	
	F6	WO98/20450	05-14-1998	Austria Card GmbH	

Note: this is not an EFS form

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11779299** conf 1938
	Filing Date	**07/18/2007**
	First Named Inventor	**Finn**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Art Unit	
	Examiner Name	
Sheet 2 OF 2	Practitioner Docket No.	**C18**

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	N1	-none cited at this time-	T

_____ _____

Examiner Signature Date Considered

OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

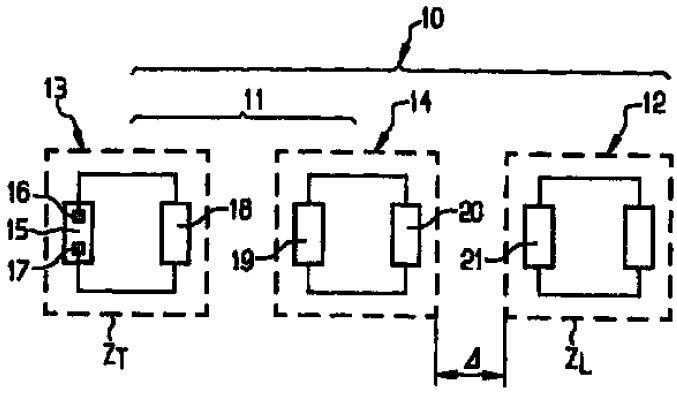
(21) (A1) **2,279,176**
(86) 1998/01/27
(87) 1998/07/30

(72) RIETZLER, MANFRED, DE
(72) WILM, ROBERT, DE
(71) AMATECH ADVANCED MICROMECHANIC & AUTOMATION TECHNOLOGY GMBH & CO. KG, DE
(71) PAV CARD GMBH, DE

(51) Int.Cl.[6] G06K 19/07
(30) 1997/01/28 (197 03 029.7) DE

(54) **MODULE DE TRANSMISSION POUR DISPOSITIF TRANSPONDEUR, ET DISPOSITIF TRANSPONDEUR ET PROCEDE PERMETTANT DE FAIRE FONCTIONNER UN DISPOSITIF TRANSPONDEUR**

(54) **TRANSMISSION MODULE FOR A TRANSPONDER DEVICE, TRANSPONDER DEVICE AND METHOD FOR OPERATING SAID DEVICE**



(57) L'invention concerne un module de transmission (14) pour la transmission de données sans contact entre une puce (15) et un dispositif de lecture (12) comprenant un montage à bobines qui comporte un élément de couplage (19) et au moins une bobine d'antenne (20) qui sont reliés électriquement l'un avec l'autre, l'élément de couplage servant à la réalisation d'un couplage inductif avec une bobine de transpondeur (18) reliée électriquement à la puce, et la bobine d'antenne servant à la réalisation d'une liaison avec le dispositif de lecture. L'élément de couplage, qui se présente sous la forme d'une bobine de couplage (19), et la bobine d'antenne (20) sont conçus différemment en ce qui concerne leurs paramètres de bobine influant sur l'impédance de bobine.

(57) The invention relates to a transmission module (14) for contactless transmission of data between a chip (15) and a reading device (12) with a coil arrangement comprising a coupling element (19) and at least one antenna coil (20) that are electrically interconnected, wherein said coupling element is used to produce inductive coupling with a transponder coil (18) which is electrically connected to the chip, and the antenna coil is used to enable connection to the reading device. The coupling element embodied as a coupling coil (19) and the antenna coil (20) are configured differently with respect to the coil parameters affecting coil impedance.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 101 40 662 C 1**

(51) Int. Cl.[7]: **G 06 K 19/077**

(21) Aktenzeichen: 101 40 662.2-53
(22) Anmeldetag: 24. 8. 2001
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 20. 3. 2003

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
ORGA Kartensysteme GmbH, 33104 Paderborn, DE

(74) Vertreter:
Quermann & Richardt Patentanwälte, 65195 Wiesbaden

(72) Erfinder:
Osterwald, Frank, Dr.-Ing., 24103 Kiel, DE; Senge, Carsten, Dipl.-Ing., 24105 Kiel, DE; Mentzer, Rüdiger, Dipl.-Ing., 24783 Osterrönfeld, DE

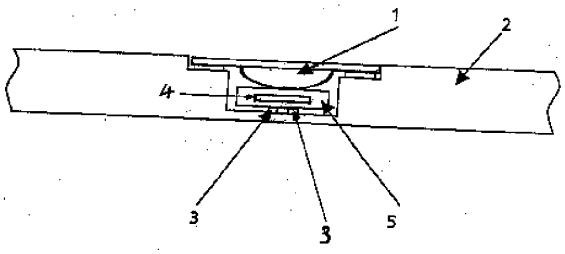
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE	197 00 848 C1
DE	199 35 528 A1
DE	199 14 587 A1
DE	196 45 083 A1
DE	42 05 556 A1
WO	99 16 019 A1

(54) **Chipkarte mit integriertem Schalter**

(57) Die Erfindung betrifft eine Chipkarte mit integriertem Schalter mit
- einer Kavität,
- einem in der Kavität fixierten Kontaktpaar 3,
- einer in der Kavität angeordneten Kontaktbrücke 4 zum Schließen eines Kontaktes zwischen dem Kontaktpaar 3,
- einem in die Kavität hineinragenden Modul,

so dass bei Ausübung eines äußeren Drucks auf das Modul die Kontaktbrücke 4 gegen das Kontaktpaar 3 gedrückt wird.



DE 101 40 662 C 1

DE 101 40 662 C 1

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 42 900 A 1**

(51) Int. Cl.[6]: G 06 K 19/07

(21) Aktenzeichen: 195 42 900.1
(22) Anmeldetag: 17. 11. 95
(43) Offenlegungstag: 22. 5. 97

DE 195 42 900 A 1

(71) Anmelder:
Cubit Electronics GmbH, 99099 Erfurt, DE

(74) Vertreter:
Pöhner,Liedtke & Partner, Dr., 99094 Erfurt

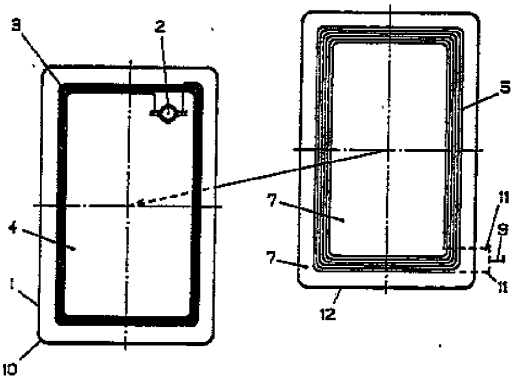
(72) Erfinder:
Michalk, Manfred, Dr., 99096 Erfurt, DE; Michalk, Helga, 99096 Erfurt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 43 02 387 C2
DE 43 28 100 A1
DE 42 33 283 A1
DE 41 05 869 A1

(54) Kontaktloser Datenträger

(57) Der Erfindung liegt die Aufgabe zugrunde, die Schreib- bzw. Lesereichweite des Datenträgers zu verändern, ohne schirmende oder filternde Elemente bewegen zu müssen.
Die Aufgabe wird dadurch gelöst, daß auf dem Datenträger 1 parallel zur Ebene 4 der Antennenspule 3 mindestens eine offene Zusatzspule 5 angeordnet ist.
Die Erfindung betrifft einen kontaktlosen Datenträger mit spulenförmiger Antenne zur elektromagnetischen Daten- und/oder Energieübertragung.



DE 195 42 900 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 03. 97 702 021/231 7/22

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 197 42 126 A 1**

(51) Int. Cl.[6]: **G 06 K 19/073**

(21) Aktenzeichen: 197 42 126.1
(22) Anmeldetag: 24. 9. 97
(43) Offenlegungstag: 25. 3. 99

DE 197 42 126 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Hoedeau, Detlef, 84085 Langquaid, DE; Heinemann, Erik, 93049 Regensburg, DE; Püschner, Frank, 93309 Kelheim, DE

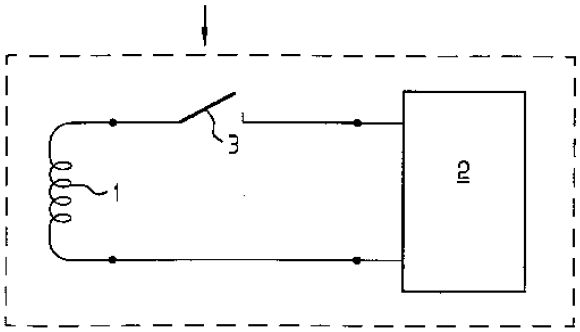
(56) Entgegenhaltungen:
DE 1 95 42 900 A1
DE 42 05 827 A1
DE 42 05 556 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Tragbarer Datenträger mit Aktivierungsschalter

(57) Bei einem tragbaren Datenträger, insbesondere einer Chipkarte, mit einer Antenne (1) und einem damit verbundenen Halbleiterchip (2), ist zwischen der Antenne (1) und dem Halbleiterchip (2) ein durch den Benutzer des Datenträgers betätigbares Schaltmittel (3) angeordnet, so daß ein Empfang von Daten nur nach einer Betätigung des Schaltmittels (3) möglich ist.



DE 197 42 126 A 1

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 728 710**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 15570**

(51) Int Cl⁶ : G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 23.12.94.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : 28.06.96 Bulletin 96/26.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule.*

(60) Références à d'autres documents nationaux apparentés : CERTIFICAT D'UTILITÉ RÉSULTANT DE LA TRANSFORMATION VOLONTAIRE DE LA DEMANDE DE BREVET DÉPOSÉE LE 27/12/94

(71) Demandeur(s) : *SOLAIC SOCIETE ANONYME* — FR.

(72) Inventeur(s) : LARCHEVESQUE ALAIN et GAUMET MICHEL.

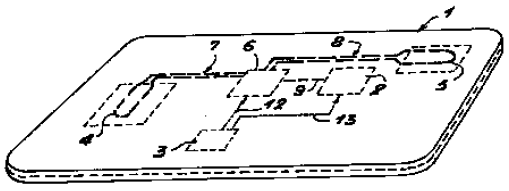
(73) Titulaire(s) :

(74) Mandataire :

(54) CARTE ELECTRONIQUE COMPORTANT UN ELEMENT FONCTIONNEL ACTIVABLE MANUELLEMENT.

(57) La carte électronique selon l'invention comprend un corps en matière plastique (1) renfermant un élément fonctionnel (2) alimenté par une source d'énergie (3), et est caractérisée en ce que la source d'énergie est reliée à un élément sensible (4) dans lequel une grandeur physique varie lorsqu'il est soumis à une action manuelle volontaire, et à un circuit électronique (6) apte à fournir un signal de commande à l'élément fonctionnel (2) en réponse à un signal émis par l'élément sensible (4) et correspondant à une valeur de la grandeur physique, située dans une plage de valeurs prédéterminée.

Afin d'éviter une activation intempestive de l'élément fonctionnel, il est souhaitable que le circuit électronique ne délivre le signal de commande que lorsque la valeur de la grandeur physique varie à une vitesse située dans une plage de vitesses prédéterminée.



FR 2 728 710 - A1

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G06K 19/077

A1

(11) Internationale Veröffentlichungsnummer: **WO 98/20450**

(43) Internationales Veröffentlichungsdatum: 14. Mai 1998 (14.05.98)

(21) Internationales Aktenzeichen: PCT/EP97/05996

(22) Internationales Anmeldedatum: 30. Oktober 1997 (30.10.97)

(30) Prioritätsdaten:
196 45 083.7 1. November 1996 (01.11.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: AUSTRIA CARD GMBH [AT/AT]; Lamezanstrasse 4–8, A–1232 Wien (AT).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: PRANCZ, Markus [AT/AT]; Treustrasse 3/12, A–1200 Wien (AT).

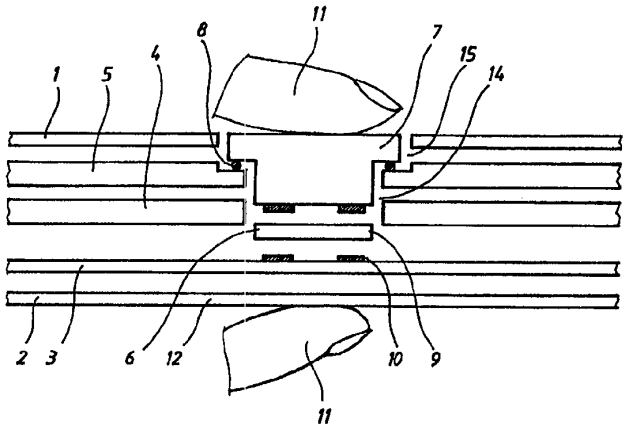
(74) Anwalt: RIEBLING, Peter; Postfach 3160, D–88113 Lindau (DE).

(81) Bestimmungsstaaten: CZ, HU, JP, PL, RU, SI, SK, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: CONTACTLESS SMART CARD WITH A TRANSPONDER COIL

(54) Bezeichnung: KONTAKTLOSE CHIPKARTE MIT TRANSPONDERSPULE



(57) Abstract

The invention relates to an ID card with a transaction coil and a method for the production thereof. The transaction coil is configured as a screen–printed silver or conductive paste which is built into a plastic card body corresponding to usual ISO standards. A milling process enables the ends of said coil to be laid bare in order to implant a special chip module or the contact ends are already bare if a lamination or injection moulding process is used. Contacting of said coil can only occur when pressure is consciously applied. The coil is automatically deactivated when pressure ceases.

(57) Zusammenfassung

Die Erfindung betrifft eine Identifikationskarte mit Transaktionsspule und ein Verfahren zu deren Herstellung. Die Transaktionsspule ist in Form einer Silber– bzw. allg. Leitpasten–Siebdruckausführung ausgebildet, die in eine den üblichen ISO Normen entsprechenden Kunststoff–Kartenkörper eingebracht werden und deren Enden anschließend mittels Fräsprozeß für die Implantation eines speziellen Chipmoduls freigelegt werden oder deren Kontaktenden bereits im Laminier– oder Spritzgußvorgang freigehalten worden sind und dessen Kontaktierung nur durch eine bewußte Druckaufbringung erfolgen kann und automatisch nach Beendigung dieses Druckaufbringens inaktiv wird.

Kontaktlose Chipkarte mit Transponderspule

Die Erfindung betrifft eine kontaktlose Chipkarte mit Transponderspule und ein Verfahren zu deren Herstellung.

Gegenstand der vorliegenden Erfindung ist eine Identifikationskarte mit Transponderspule und eingebautem Chipmodul, wobei die auf dem Chipmodul gespeicherten Daten ausgelesen und mit Hilfe der Transponderspule kontaktlos auf einen Empfänger übertragen werden können.

Identifikationskarten zur kontaktlosen Transaktion werden entsprechend den ISO/IEC DIS 10536 Normen für die unterschiedlichsten Anwendungen einer Standardisierung unterworfen. Zielsetzung aller dieser Normen ist die Erhöhung der Sicherheit und der Geschwindigkeit von Identifikations- und Transaktionsvorgängen bei gleichzeitiger Reduktion der integralen Kosten und einer weltweiten Anwendung und gewissen Kompatibilität.

Identifikationsvorgänge mittels sogenannter handgehaltener berührungsloser Identifikationskarten werden in immer stärkerem Ausmaß im öffentlichen Personen und Nahverkehr bzw. ganz allgemein zur komfortablen und raschen Identifikation bzw. Zutrittskontrolle und oftmals der vollautomatischen Abbuchung entsprechender Werteinheiten oder Geldbeträge verwendet.
Im überwiegenden Maße wird diese rasche und unbemerkte Identifikation sinnvoll und vom Besitzer voll akzeptiert stattfinden.

Bei mißbräuchlichem Einsatz ist der Benutzer ziemlich machtlos und kann erst rückwirkend diesen Mißbrauch feststellen. Aus diesem Grund werden reine Geldtransaktionen

bevorzugt mittels kontaktbehafteter Chipkarten durchgeführt und der Transaktionsvorgang bewußt und oftmals nur nach Eingabe einer persönlichen Identifikationsnummer (PIN) durchgeführt.

Bei allen Arten von Identifikationskarten Applikationen mittels berührungsloser Transponder-Chipkarten müssen die Aspekte der länderweit durchaus sehr unterschiedlichen Datenschutzgesetze und Verordnungen bzw. ganz allgemein der guten Sitten berücksichtigt werden.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, eine Chipkarte der eingangs erwähnten Art so weiterzubilden, daß mittels eines möglichst kostengünstigen Prozesses ein möglichst einfach anwendbares Produkt dem Benutzer einer derartigen berührungslos funktionierenden Chipkarte die Möglichkeit gibt, den Vorgang der Identifikation und Transaktion bewußt herbeizuführen und weiters damit jegliche Kollision oder Konfrontation mit dem Datenschutzgesetz zu vermeiden.

Die Lösung dieser Aufgabe ist durch die technischen Merkmale des Anspruchs 1 gegeben.

Ein Herstellungsverfahren der erfindungsgemäßen Chipkarte ist Gegenstand des unabhängigen Anspruchs 11.

Wesentlich bei der vorliegenden Erfindung ist demnach die bewusste Schaltung einer Transponderspule, wobei bevorzugt die Kontaktflächen der Transponderspule mit zugeordneten Kontaktflächen eines Chipmoduls durch die willkürliche Schaltung miteinander verbunden werden.

In einer ersten, bevorzugten Ausführungsform erfolgt diese Durchschaltung der Kontaktflächen der Transponderspule zu den Kontaktflächen des Chipmoduls über ein ohmsches

Kontaktelement, welches z.B. aus einem drucksensitiv-leitenden Silikongummi besteht, welches als Kontaktmaterial im Zwischenraum zwischen den beiden einander gegenüberliegenden Kontaktflächen liegt und - sobald der Luftzwischenraum zwischen den Kontaktflächen komprimiert wird, kommt dieses Kontaktelement sowohl in direkten ohmschen Kontakt mit den Kontaktflächen der Transponderspule als auch mit den gegenüberliegenden Kontaktflächen des Chipmoduls.

Der vorliegenden Erfindung liegt nun die Erkenntnis zugrunde, daß die Implantation eines Chipmoduls mit Kontaktflächen in der Karte und der Kontakt mit den beiden Enden der Spule prozeßtechnisch sehr einfach mittels sogenannter druckempfindlicher leitfähiger Silikon-Gummi-Matten mit Silberkügelchen herbeigeführt werden kann, und in einer weiteren Ausführungsform, durch die Ausbildung des Kartenkörpers und des zu implantierenden Chipmoduls eine Art mechanischer Schalter derart hergestellt werden kann, daß im Ruhezustand ein entsprechender Luftspalt zwischen den Kontaktpartnern gegeben ist, der nur durch mechanischen Druck, beispielsweise durch Fingerdruck, im Bereich des Chipmoduls überbrückt werden kann und dadurch zum Kontakt zwischen Chipmodul und Transponderspule und damit zur Aktivierung der Transponder-Chip Einheit führt.

In einer weiteren typischen Ausführungsform kann das Chipmodul ein sogenanntes Hybridmodul sein, das entweder zwei Chips beinhaltet, wobei ein Chip für die berührungslose Transaktion und ein zweiter Chip für die standardmäßige kontaktbehaftete Transaktion zuständig ist, oder aber einen Kombinationschip enthalten, der beide Funktionen in einem Chip vereint. In beiden Fällen müssen die Kontakte für die Transponderspule an der Unterseite bzw. Innenseite des Chipmoduls liegen, respektive auf der Seite, die den

Kontaktflächen des kontaktbehafteten Chipmoduls gegenüberliegt.

In einer Weiterbildung der vorliegenden Erfindung ist es vorgesehen, daß die Schaltung der Transponderspule nicht durch willkürliche Schaltung eines Kontaktelements erfolgt, sondern daß die Schaltung durch ein externes Signal ausgelöst wird. Diese weiterführende technische Lehre hat den Vorteil, daß die Chipkarte nach der Erfindung gleichzeitig auch diebstahlgesichert ist. Ein externes Signal zum Schalten der Transponderspule wird beispielsweise von einem Personenerkennungssystem ausgelöst, welches z.B. visuell oder akustisch die Berechtigung des Benutzers zum Eintritt in einen bestimmten Bereich erkennt. Sobald dieses System den berechtigten Benutzer erkannt hat, wird ein derartiges externes Signal ausgelöst, welches dann die Transponderspule schaltet. Die Transponderspule liest dann die in dem Chipmodul gespeicherten Daten, wie z.B. Identifizierung, Zeitpunkt und andere Personendaten aus, wodurch sichergestellt ist, daß auch nur der berechtigte Benutzer dieser Chipkarte durch den geschützten Eingangsbereich gelangt.

Transaktions-Chipkarten sind durch den erforderlichen Aufbau und aufgrund der noch nicht in Großserien gefertigten Chiptypen bzw. Chipmodule üblicherweise teurer in der Herstellung und in Verbindung mit einer typischen Identifikationsanwendung häufiger und meist auch länger im Einsatz als herkömmliche kontaktbehaftete Chipkarten. An die Lebensdauer und Verwendungshäufigkeit derartiger handgehaltener Karten werden große Anforderungen gestellt und diesbezüglich stellt die Biegebeanspruchung ein wesentliches Kriterium dar. Eine Schwachstelle dabei sind die Kontakte und die Dimension der Chipfläche. In der vorliegenden Erfindung wird der feste mechanische Verbund zwischen Kartenkörper und Chipkontakten vermieden und damit

wesentlich geringere Anforderungen an die Spannungsrißfestigkeit der Kontaktelemente und die Gleichmäßigkeit der Wärmeausdehnungskoeffizienten der verschiedenen Verbundpartner gestellt.

Die Herstellung der Kartengrundkörper erfolgt in bekannter Weise einer typischen Ausführungsform dadurch, daß dünne Druckbögen mit typisch 80 bis 350 Mikrometer Dicke und Formaten für Mehrfachnutzen, typischerweise 24 bzw. 48 Karten pro Druckbogen mit Abmessungen von beispielsweise 30 x 50 cm oder 50 x 70 cm mit den in der Kreditkartenproduktion üblichen Offsetdrucken und Siebdrucken kundenspezifisch gestaltet werden und falls notwendig mit entsprechenden thermisch aktivierbaren Klebebeschichtungen, bevorzugt im Siebdruck, versehen werden.

Im folgenden wird eine Ausführungsform der Erfindung anhand von Zeichnungen näher erläutert. Hierbei gehen aus den Zeichnungen und ihrer Beschreibung weitere erfindungswesentliche Merkmale und Vorteile der Erfindung hervor.

Figur 1: zeigt den Schnitt durch den Chipmodulbereich einer Chipkarte nach der Erfindung,

Figur 2: die Draufsicht auf die Folie mit Darstellung der Transponderspule,

Figur 3: die Draufsicht auf die Oberseite der Chipkarte bei noch nicht eingesetztem Chipmodul und noch nicht eingesetztem Schaltelement,

Figur 4: eine Abwandlung gegenüber Figur 3.

Wie in Figur 1 gezeigt, werden beispielsweise je zwei typisch 80 my dicke, transparente Deckfolien 1 und 2 als sogenannte Overlayfolien verwendet. Diese transparenten Overlayfolien können nun wahlweise auf den Innenseiten mit thermisch aktivierbaren Schmelzklebern mittels Siebdruck oder direkt beim Folienzulieferanten beschichtet werden, wobei je nach geforderter Qualität als Material z.B. PVC-h, ABS, PET oder Polycarbonat (PC) eingesetzt werden kann und im weiteren dabei gegebenenfalls auf die Verwendbarkeit für Laserbeschriftungen und/oder Hochprägungen und/oder den Einbau eines Magnetstreifens geachtet werden muß.

Als nächste Schichten sind Folien 3 und 5 vorgesehen, wobei deren nach außen gerichtete Flächen grafisch mittels Offsetdruck und Siebdruck bzw. auch mittels der verschiedenen digitalen Druckverfahren kundenspezifisch gestaltet werden können. Üblicherweise werden diese Folien in neutralem Farbton und in Dicken von 80 my bis 350 my verwendet. Die innerste Schicht der Chipkarte bildet eine Kernfolie 4, die z.B. aus ABS- oder PC-Material besteht und eine Dicke von z.B. 300 my aufweist.

Im vorliegenden Beispiel wird die Folie 5 in einer Dicke von etwa 300 my eingesetzt und kann in Kombination mit einer PC-Deckfolie 1 z.B. aus ABS sein. In der Ausführung ABS wird entsprechend dem im Vergleich zu PC niedrigerem Schmelzpunkt eine bessere Fließeigenschaft erreicht, was unter Umständen einen homogeneren Laminataufbau bewirken kann.

Folie 3 wird in möglichst dünner Ausführung, typisch 80 my verwendet und wird bevorzugt aus PC-Material sein, um die Trocknungsvorgänge der aufgebrachten Silberpastendrucke auf der Innenseite ohne wesentliche Schrumpfung bestehen zu können. D.h. auf dieser 80 my PC-weiß Folie, die außen grafisch gestaltet ist, wird auf der Innenseite mittels Siebdruck, bevorzugt Zylindersiebdruck, eine sogenannte Transponderspule 13 gedruckt. Dabei werden handelsübliche

Silberpasten, bevorzugt mit guter elektrischer Leitfähigkeit und geeignet für den Kunststoff-Foliendruck eingesetzt. Derartige Silberpasten werden bei der Herstellung flexibler Leiterplatten aus Polyester- und Polyamidfolien verwendet und können bei etwa 120°C getrocknet werden, ohne daß eine maßliche Beeinträchtigung dieser PC-Folien stattfindet, was natürlich für diesen Mehrfachnutzenaufbau sehr wesentlich ist.

Die Geometrie der Transponderspule wird je nach Anforderung an die Eigenschaften der Spule 13, d.h. die Anforderung an den Sende- und Empfangsvorgang und die Höhe der erzeugten Induktionsspannung in der Spule - zwecks Stromversorgung des Halbleiterbausteins - gewählt werden.

Dabei können die Anzahl der Windungen, die Leiterbahnbreite und der Leiterbahnabstand, die Formen der Anschlußkontakte 10 und natürlich die Dicke des Leitpastenaufbaues bzw. die Art der verwendeten Leitpaste variiert werden. Typischerweise werden einige 3 bis 5 Windungen mit Leiterbahnbreiten im Bereich 100 my bis 1 mm gewählt werden. Um den ohmschen Widerstand möglich niedrig zu halten, werden u.U. mehrere übereinanderliegende Drucke durchgeführt. In einer kostengünstigeren Variante können die Silberpasten auch durch Karbonpasten, Kupferpasten oder Mischen aus den verschiedenen Leitpastentypen erfolgen.

Ein sehr wesentliches Detail stellt die Art der Anschlußkontakte 10, d.h. die Ausbildung der Enden der Spule 13 dar, da diese zur Kontaktierung des Chipmoduls 7 benötigt werden.

In der vorliegenden Erfindung ist nun sehr wesentlich, daß die Anschlußflächen 9 des Chipmoduls 7 auf der Unterseite, d.h. der Seite, die in Kontakt zu den Spulen-Anschlußkontakten 10 treten sollen, liegen und einen entsprechend weiten Abstand haben, so daß die Bahnen der Spule 13 dazwischen durchgeführt werden können und die Enden der Spule 13 relativ großflächig ausgeführt werden können.

Übliche Leitpastendrucke in Einfach- und Mehrfachdruckausführung weisen eine Dicke von 10 bis 30 my auf, typisch 15 bis 20 my im getrockneten Zustand.
Die Freifräsung der Ausnehmungen 14 und 15 im Anschluß an die Lamination des gesamten aus den Folienlagen 1-5 bestehenden Paketes muß nun sehr exakt auf die erforderliche Tiefe eingestellt werden, um einerseits die Leitpaste der Transponderspule 13 elektrisch freizulegen, jedoch andererseits keine zu starke Reduktion der Leitpastendicke und damit Reduktion des Leitungsquerschnittes der Spule 13 herbeizuführen.

Übliche Fräsanlagen für die Vertiefungen von Chipmodulen arbeiten mit Toleranzen bis zu +/-10 my. Im vorliegenden Fall ist jedoch eine Toleranz von vorzugsweise +/-3 my anzustreben. Dabei spielt noch die Dicken-Toleranz der Folienlagen 2 und 3 eine sehr wesentliche Rolle, da diese in die Toleranzrechnung mit einbezogen werden müssen.

Diese sehr genaue mechanische Freilegung der Kontakte 10 der Spule 13 ist in der vorliegenden Erfindung gegenüber dem Stand der Technik insofern von Bedeutung, als üblicherweise derart freigelegte Kontakte 10 mittels Leitkleber oder Leitpaste kontaktiert werden und damit den Flächenleitwert verbessern.

In der vorliegenden Erfindung werden jedoch diese Anschlußflächen 10 der Spule 13 nur mittels eines Schaltelements 6 kontaktiert. Dieses Schaltelement 6 kann beispielsweise aus sogenannten druckempfindlich-leitenden Gummimatten in Materialstärken von z.B. 0,2 bis 0,3 mm bestehen bzw. aus einzelnen Kontaktelementen pro Anschluß 10a bzw. 10b.

Derartige Gummimatten werden üblicherweise mit Nickelkügelchen oder Silberkügelchen in Form einer Matrix hergestellt und werden erst bei Druck leitend. Gemäß dem Stand der Technik werden derartige Drucksensitiv-leitende Gummimatten z.B. zur Kontaktierung von Glassubstraten, typisch LCD's und Bildschirmen als auch flexiblen Substraten

verwendet und dabei wird mittels entsprechender Klammern Druck über entsprechenden Anschlußflächen hergestellt.

Im vorliegenden Fall können mittels derartiger drucksensitiv-leitender Gummimatten sehr einfache und effiziente Schalter hergestellt werden, die auf extrem geringen Raum einen funktionellen Kontakt ohne starke Deformationsvorgänge in den einzelnen Lagen der Identifikationskarte herstellen können.

In einer weiteren Ausführungsform ist vorgesehen, die Dicken der einzelnen Folienlagen 1-5 der ID-Karte derart abzustimmen, daß die Lagen 2 und 3 als Membrane verwendet werden können und zwischen sich einen Luftspalt einschließen, der durch Druckaufbringung überbrückt und somit ein Kontakt zwischen Chipmodul 7 und Transponderspule 13 hergestellt werden kann. Dabei werden die Leitpastenkontaktflächen 10 der Spule 13 mit den Kontaktflächen 9 des Chipmoduls 7 zusammengepreßt und dadurch die Funktion der Transponder-Chipkarte aktiviert. Das System ist ebenfalls ohne bewußte Druckaufbringung nicht aktiv und es kann daher keinerlei unbewußte Identifikation oder Transaktion stattfinden.

In Erweiterung dieser genannten Ausführungsform können nach deren Freilegung auf die Anschlußflächen 10 der Leitpastenkontaktflächen leitfähige elastomere Kontaktelemente mittels Dispenser oder Tampondruck aufgebracht werden, so daß im Falle des Druckaufbringens ein elastisches leitendes Element zwischen den Kontakten 9 und 10 vorhanden ist und damit zu einer optimalen Kontaktsicherheit führt.

Die Ausführung des Chipmoduls 7 wird geometrisch gemäß dem Stand der Technik ausgeführt, allerdings mit nach innen zur Transponderspule gerichteten Kontaktflächen 9, bevorzugt in vergoldeter bzw. auch verzinnter oder vernickelter

Oberflächenausführung. Wahlweise kann das Chipmodul noch mit oberseitigen Kontakten für die Kontaktierung eines kontaktbehafteten Chipsystems ausgeführt werden, wobei je nach Kundenwunsch ein oder zwei Halbleiterelemente zum Einsatz gelangen. Die mechanische Fixierung des Chipelements 7 erfolgt in einer formangepassten Ausfräsung 14, 15 der Folienschichten 1, 5 und 4 mittels einer Klebebefestigung 8. Dadurch werden optimale Festigkeitswerte hinsichtlich der Biegewechselfestigkeit erreicht, als auch eine optimale Abdichtung des Innenraums (Kontaktraumes) gegen etwaige Silbermigration der Silberleitpaste. Weiters kann mittels dieses dem Stand der Technik entsprechenden Prozesses eine exakte Planheit der Oberflächen erreicht werden.

Die Figuren 3 und 4 zeigen eine Draufsicht auf die Oberseite (Deckfolienlage 1) der Chipkarte bei noch nicht eingesetztem Chipmodul und noch nicht eingesetztem Schaltelement. Man erkennt im Bereich der Ausfräsung einen Ausschnitt der Folienlage 3 mit aufgebrachter Transponderspule und deren Kontaktanschlüssen 10. Die Kontaktanschlüsse 10 können z.B. punktförmig 10a oder zur Vergrößerung der Kontaktfläche oval 10b ausgebildet sein. Die Ausfräsung vergrößert sich hin zur Kartenoberfläche (vgl. Figur 1) und man erkennt einen Teil der Folienlage 5, mit welcher später das Chipmodul 7 verklebt oder verschweißt wird.

Zeichnungslegende

1	Deckfolie
2	Deckfolie
3	Folie
4	Kernfolie
5	Folie
6	Schaltelement
7	Chipmodul
8	Kleber
9	Kontaktfläche
10	Kontaktfläche (10a, 10b)
11	Finger
12	Kunststofflage
13	Transponderspule
14	Ausnehmung
15	Ausnehmung

Patentansprüche

1. Kontaktlose Chipkarte mit Transponderspule und eingebautem Chipmodul, wobei die auf dem Chipmodul gespeicherten Daten ausgelesen und mit Hilfe der Transponderspule kontaktlos auf einen Empfänger übertragen werden können, dadurch gekennzeichnet, daß die Transponderspule (13) zur bewussten Aktivierung und damit Auslösung einer Identifikation oder Transaktion der Chipkarte schaltbar ausgebildet ist.

2. Kontaktlose Chipkarte nach Anspruch 1, dadurch gekennzeichnet, daß die Schaltung der Transponderspule (13) willkürlich, z.B. durch Fingerdruck erfolgt.

3. Kontaktlose Chipkarte nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die willkürliche Schaltung der Transponderspule (13) durch einen ohmschen Kontaktschluss zwischen Kontaktflächen (10) der Transponderspule (13) und entsprechenden Kontaktflächen (9) des Chipmoduls (7) erfolgt.

4. Kontaktlose Chipkarte nach Anspruch 1, dadurch gekennzeichnet, daß die Schaltung der Transponderspule (13) durch ein externes Signal verursacht wird.

5. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 4, dadurch gekennzeichnet, daß die Chipkarte aus mehreren Folienschichten besteht und zumindest zwei Deckschichten (1,2) und eine oder mehrere Zwischenschichten (3-5) aufweist.

6. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 5, dadurch gekennzeichnet, daß die Chipkarte eine Ausnehmung (14,15) aufweist, die sich vorzugsweise über die

Folienschichten (1,4,5) erstreckt, wobei das Chipmodul (7) in der Ausnehmung (14,15) angeordnet ist.

7. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 6, dadurch gekennzeichnet, daß das Chipmodul (7) in Richtung zur Transponderspule (13) gerichtete Kontaktflächen (9) aufweist.

8. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 7, dadurch gekennzeichnet, daß die Transponderspule (13) auf einer der Zwischenschichten (3-5) aufgebracht ist und im Bereich der Ausnehmung (14,15) angeordnete Kontaktflächen (10) aufweist.

9. Kontaktlose Chipkarte nach einem der Ansprüche 1 - 8, dadurch gekennzeichnet, daß zwischen den Kontaktflächen (9) des Chipmoduls und den Kontaktflächen (10) der Transponderspule (13) eine drucksensitiv-leitende Gummimatte (6) angeordnet ist, die ohne Druckbeaufschlagung isolierend wirkt und nur bei hinreichendem Druck leitend wird und dadurch einen Kontakt zwischen den Kontaktflächen (9, 10) herstellt.

10. Kontaktlose Chipkarte nach Anspruch 9, dadurch gekennzeichnet, daß die Gummimatte (6) aus einer Silikongummimatte mit matrixförmig angeordneten Silber- bzw. Nickelkügelchen besteht.

11. Verfahren zur Herstellung einer kontaktlosen Chipkarte gemäß einem der Ansprüche 1 bis 10, dadurch gekennzeichnet,

daß mehrere übereinanderliegende Folienschichten miteinander zu einer Chipkarte verbunden werden,

daß zuvor eine der inneren Folienschichten mit einer elektrisch leitenden Transponderspule bedruckt wird, wobei an den Enden der Transponderspule Kontaktflächen vorgesehen werden,

daß durch einen Fräsvorgang an der Chipkarte, im Bereich der Kontaktflächen, eine Ausnehmung zur Aufnahme des Chipmoduls geschaffen wird, wobei die Ausfräsung bis zur mit der Transponderspule bedruckten Folienschicht reicht,

daß das Chipmodul derart in die Ausnehmung eingesetzt wird, daß dessen Kontaktflächen in einem Abstand zu den Kontaktflächen der Transponderspule zu liegen kommen, so daß sich die Kontaktflächen nicht berühren.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß zwischen die Kontaktflächen der Chipmoduls und die zugeordneten Kontaktflächen der Transponderspule ein drucksensitiv-leitendes Schaltelement eingelegt wird.

13. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß auf die Kontaktflächen der Transponderspule nach deren mechanischem Freilegen mittels eines Fräsprozesses mittels Dispenser oder Tampondruck elastische leitende Kontaktpunkte aufgebracht werden, welche bevorzugt aus Silber-, Karbon-, Kupfer- oder Nickel- gefüllten Elastomerpasten bestehen.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die Elastomerpasten aus Silikongummi mit typisch 1-10 mOhm*cm Volumenwiderstand bestehen und im Falle des Zusammendrückens einen guten und elastischen und damit sicheren elektrischen Kontakt ermöglichen.

15. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß durch den Freifräsprozeß der Ausnehmung für das Chipmodul nicht die gesamte Fläche bis zu der Oberfläche der Transponderspule freigelegt wird, sondern lediglich selektiv im Bereich der beiden Kontaktflächen mittels spezieller Stirnfräser und entsprechend erhöhter z-Achsen Genauigkeit und anschließend in diese Vertiefungen entsprechende Elastomerkontaktelemente eingebracht werden, die mittels

Druckbeaufschlagung zu einer Aktivierung des Transponder-Chip-Systems führen.

1/1

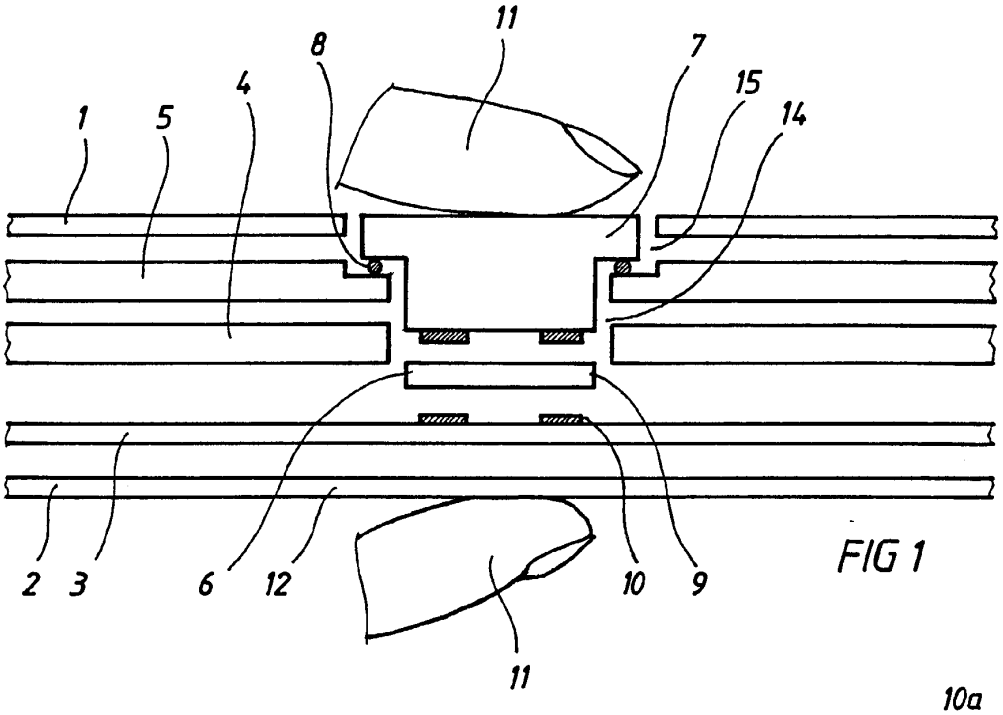


FIG 1

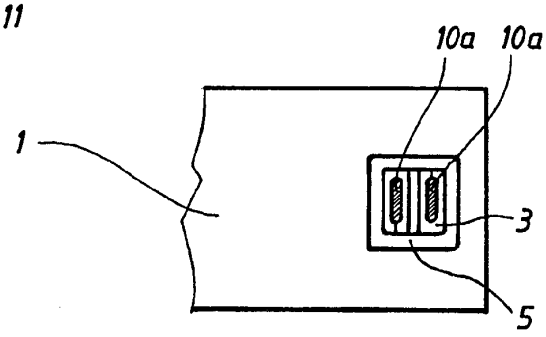


FIG 3

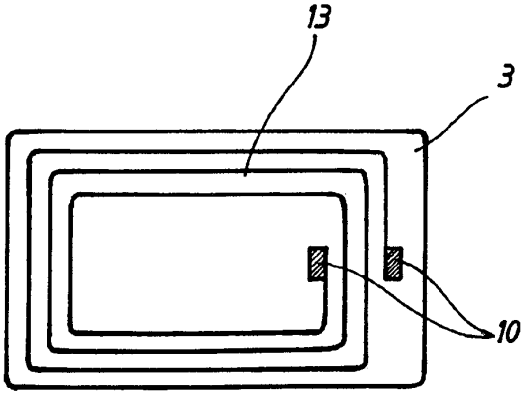


FIG 2

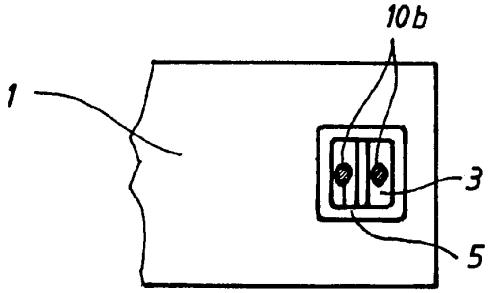


FIG 4

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/EP 97/05996

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K19/077

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 44 03 753 C (ANGEWANDTE DIGITAL ELEKTRONIK) 20 July 1995 see claim 1 ---	1,2.5-8
X	DE 42 05 827 A (ANGEWANDTE DIGITAL ELEKTRONIK) 2 September 1993 see claim 1 ---	1,2
X	EP 0 557 934 A (ANGEWANDTE DIGITAL ELEKTRONIK) 1 September 1993 see claim 1 ---	1,2
A	DE 39 35 364 C (ANGEWANDTE DIGITAL ELEKTRONIK) 23 August 1990 see column 1, line 62 - line 65 ---	4
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of ... international search report
3 April 1998	09/04/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Herskovic, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/EP 97/05996

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 682 321 A (GIESECKE & DEVRIENT GMBH) 15 November 1995 see the whole document -----	11

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/EP 97/05996

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4403753 C	20-07-95	AU 1574395 A	29-08-95
		CN 1140502 A	15-01-97
		WO 9522121 A	17-08-95
		EP 0744061 A	27-11-96
		EP 0751478 A	02-01-97
		JP 9507931 T	12-08-97
DE 4205827 A	02-09-93	DE 4305571 A	25-08-94
		EP 0562292 A	29-09-93
		JP 6004723 A	14-01-94
		US 5376778 A	27-12-94
		DE 4205556 A	26-08-93
		FR 2702065 A	02-09-94
		GB 2275554 A,B	31-08-94
EP 0557934 A	01-09-93	DE 4205556 A	26-08-93
		DE 4305571 A	25-08-94
DE 3935364 C	23-08-90	EP 0424726 A	02-05-91
		JP 3209592 A	12-09-91
		US 5206495 A	27-04-93
EP 0682321 A	15-11-95	DE 4416697 A	16-11-95
		JP 8044840 A	16-02-96

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Int. ionales Aktenzeichen
PCT/EP 97/05996

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06K19/077

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 44 03 753 C (ANGEWANDTE DIGITAL ELEKTRONIK) 20.Juli 1995 siehe Anspruch 1	1,2,5-8
X	DE 42 05 827 A (ANGEWANDTE DIGITAL ELEKTRONIK) 2.September 1993 siehe Anspruch 1	1,2
X	EP 0 557 934 A (ANGEWANDTE DIGITAL ELEKTRONIK) 1.September 1993 siehe Anspruch 1	1,2
A	DE 39 35 364 C (ANGEWANDTE DIGITAL ELEKTRONIK) 23.August 1990 siehe Spalte 1, Zeile 62 - Zeile 65	4

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

1

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
3.April 1998	09/04/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Herskovic, M

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Inte .ionales Aktenzeichen
PCT/EP 97/05996

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 682 321 A (GIESECKE & DEVRIENT GMBH) 15.November 1995 siehe das ganze Dokument -----	11

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 97/05996

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4403753 C	20-07-95	AU 1574395 A	29-08-95
		CN 1140502 A	15-01-97
		WO 9522121 A	17-08-95
		EP 0744061 A	27-11-96
		EP 0751478 A	02-01-97
		JP 9507931 T	12-08-97
DE 4205827 A	02-09-93	DE 4305571 A	25-08-94
		EP 0562292 A	29-09-93
		JP 6004723 A	14-01-94
		US 5376778 A	27-12-94
		DE 4205556 A	26-08-93
		FR 2702065 A	02-09-94
		GB 2275554 A,B	31-08-94
EP 0557934 A	01-09-93	DE 4205556 A	26-08-93
		DE 4305571 A	25-08-94
DE 3935364 C	23-08-90	EP 0424726 A	02-05-91
		JP 3209592 A	12-09-91
		US 5206495 A	27-04-93
EP 0682321 A	15-11-95	DE 4416697 A	16-11-95
		JP 8044840 A	16-02-96

Electronic Acknowledgement Receipt

EFS ID:	3852370
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	27-AUG-2008
Filing Date:	18-JUL-2007
Time Stamp:	23:01:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Information_Disclosure_c18_abx.pdf	26353 0ba8dc4a31cfe3dac528e46cf0fb5f8725782603	no	2

Warnings:	
Information:	

2	Foreign Reference	F1_abx_CA2279176A1.pdf	28644 ca459f7f6aee1b266b1e025e761f0c64496010d1	no	1
Warnings:					
Information:					
3	Foreign Reference	F2_abx_DE10140662C1.pdf	17777 bca9a1541e02de8a1cb685ca3457117a90857ec5	no	1
Warnings:					
Information:					
4	Foreign Reference	F3_abx_DE19542900A1.pdf	19657 891ded7bb242a944fc11a5bee36bf6febceacc20	no	1
Warnings:					
Information:					
5	Foreign Reference	F4_abx_DE19742126A1.pdf	14656 d0a954f5f7d081ae78d2a0aa3592df7d0f645fd8	no	1
Warnings:					
Information:					
6	Foreign Reference	F5_abx_FR2728710A1.pdf	20470 57059538267610 39a8d7a403f276b5cd5d40ff6f	no	1
Warnings:					
Information:					
7	Foreign Reference	F6_abx_wo98020450.pdf	890332 9e64729479f73041e45fee21c0dd9772d635ab2b	no	24
Warnings:					
Information:					
		Total Files Size (in bytes):	1017889		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/779,299	07/18/2007	David Finn	Finn-C18

CONFIRMATION NO. 1938

63397
GERALD E. LINDEN
12925 LAROCHELLE CR.
PALM BEACH GARDENS, FL33410

Title: Portable Identity Card Reader System For Physical and Logical Access

Publication No. US-2008-0014867-A1
Publication Date: 01/17/2008

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Pre-Grant Publication Division, 703-605-4283

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/779,299	07/18/2007	David Finn	Finn-C18

CONFIRMATION NO. 1938

63397
GERALD E. LINDEN
12925 LAROCHELLE CR.
PALM BEACH GARDENS, FL33410

Date Mailed. 11/15/2007

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 01/17/2008. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Patent Publication at 1-888-786-0101.

PART 1 - ATTORNEY/APPLICANT COPY

Note: this is not an EFS form

Filename: C18_substitute_IDS_Usonly_August

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**July 18, 2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

U.S. PATENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	6070240	05-30-2000	Xydis	
	2	6172430	01-09-2001	Schmitz et al.	
	3	6181024	01-30-2001	Geil et al.	
	4	6307471	10-23-2001	Xydis	
	5	6341727	01-29-2002	Canard et al.	
	6	6456958	09-24-2002	Xydis	
	7	6560711	05-06-2003	Given et al.	
	8	6745042	06-01-2004	Xydis	
	9	6763315	07-13-2004	Xydis	
	10	6913196	07-05-2005	Morrow et al.	
	11	6963794	11-08-2005	Geber et al.	
	12	6992562	01-31-2006	Fuks et al.	
	13	7034238	04-25-2006	Uleski et al.	
	14	7042332	05-09-2006	Takamura et al.	
	15	7150397	12-19-2006	Morrow et al.	

U.S. PATENT APPLICATION PUBLICATIONS

Exam. Initials	Cite No.	Publication Number.	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
	A1	US 20020065625	05-30-2002	Xydis	
	A2	US 20020069030	06-06-2002	Xydis	
	A3	US 20020104012	08-01-2002	Xydis	
	A4	US 20050044424	02-24-2005	Xydis	
	A5	US 20050269402	12-08-2005	Spitzer et al.	
	A6	US 20060186209	08-24-2006	Narend	
	A7	US 20060213982	09-28-2006	Cannon et al.	
	A8	US 20060226217	10-12-2006	Narend et al.	
	A9	US 20060230437	10-12-2006	Boyer et at.	
	A10	US 20060273176	12-07-2006	Audebert et al.	
	A11	US 20010054148	12-20-2001	Hoonaert et al.	

Examiner Signature _____ Date Considered _____

Electronic Acknowledgement Receipt

EFS ID:	2043773
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	03-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	05:58:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	c18_substitute_IDS_USonly-August.pdf	23121 f4910c759e652139ba4ba0e71ab18efec9fac874	no	1
Warnings:					

Information:	
This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	23121

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Note: this is not an EFS form

Filename: C18_substitute_IDS_USonly

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

U.S. PATENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	US 4,367,965	01-11-1983	Speitel et al.	
	2	US 5,761,648	06-02-1998	Golden et al.	
	3	US 6,067,235	05-23-2000	Finn et al.	
	4	US 6,085,320	07-04-2000	Kaliski, Jr.	
	5	US 6,148,354	11-14-2000	Ban et al.	
	6	US 6,168,077	01-02-2001	Gray et al.	
	7	US 6,189,098	02-13-2001	Kaliski, Jr.	
	8	US 6,240,184	05-29-2001	Huynh et al.	
	9	US 6,283,658	09-04-2001	Estevez et al.	
	10	US 6,342,839	01-29-2002	Curkendall et al.	
	11	US 6,370,603	04-09-2002	Silverman et al.	
	12	US 6,385,677	05-07-2002	Yao	
	13	US 6,505,773	01-14-2003	Palmer et al.	
	14	US 6,543,690	04-08-2003	Leydier et al.	
	15	US 6,567,273	05-20-2003	Liu et al.	
	16	US 6,658,516	12-02-2003	Yao	
	17	US 6,694,399	02-17-2004	Leydier et al.	
	18	US 6,724,680	04-20-2004	Ng et al.	
	19	US 6,744,634	06-01-2004	Yen	
	20	US 6,748,541	06-08-2004	Margalit et al.	
	21	US 6,752,321	06-22-2004	Leaming	
	22	US 6,763,399	07-13-2004	Margalit et al.	
	23	US 6,772,956	08-10-2004	Leaming	
	24	US 6,798,169	09-28-2004	Stratmann et al.	
	25	US 6,801,956	10-05-2004	Feuser et al.	
	26	US 6,813,164	11-02-2004	Yen	
	27	US 6,848,045	01-25-2005	Long et al.	
	28	US 6,876,420	04-05-2005	Hong et al.	
	29	US 6,879,597	04-12-2005	Tordera et al.	
	30	US 6,983,888	01-10-2006	Weng	

Examiner Signature _____ Date Considered _____

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINNN, David**
	Art Unit	
	Examiner Name	
Sheet 2 OF 2	Practitioner Docket No.	**FINN-C18**

U.S. PATENT APPLICATION PUBLICATIONS

Exam. Initials	Cite No.	Publication Number.	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
	A1	US 2001 0043702	11-22-2001	Elteto et al.	
	A2	US 2001 0054148	12-20-2001	Hoornaert	
	A3	US 2002 0011516	01-31-2002	Lee	
	A4	US 2003 0000267	01-02-2003	Jacob et al.	
	A5	US 2003 0028797	02-06-2003	Long et al.	
	A6	US 2003 0087601	05-08-2003	Agam et al.	
	A7	US 2003 0102380	06-05-2003	Spencer	
	A8	US 2003 0236821	12-25-2003	Jiau	
	A9	US 2005 0274803	12-15-2005	Lee	(HK 04104126.5)
	A10	US 2005 0109841	05-26-2005	FINN	a related application (c4)

Examiner Signature _____ Date Considered _____

Electronic Acknowledgement Receipt

EFS ID:	2038678
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	02-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	08:22:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	C18_substitute_IDS_USonly.pdf	27511 bfc1265e42003770e799a1822c24de4e9415749b	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	27511

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Note: this is not an EFS form
Filename: C18_substitute_IDS_Foreign_rev

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	
Sheet 1 OF 1	Practitioner Docket No.	**FINN-C18**

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines (if not otherwise noted, "entire document")
	1	DE19631050	02-05-1998	Bergler et al.	Drawings
	2	HK 1063994			
	3	HK 1063995			
	4	JP2004246720	09-02-2004	Sazawa et al.	Drawings
	5	WO99 052051	10-14-1999	International Business Machines	
	6	WO99 038062	07-29-1999	Kobil Computer GMBH	Abs.(Engl), Dwg.
	7	WO00 036252	06-22-2000	Jacob	Abs.(Engl), Dwg.
	8	WO00 042491	07-20-2000	Rainbow Technologies, Inc.	
	9	WO00 065180	11-02-2000	Muller et al.	Abs.(Engl), Dwg.
	10	WO00 075755	12-14-2000	Eutron Infosecurities	
	11	WO01 014179	03-01-2001	Wittwer et al.	Abs.(Engl), Dwg.
	12	WO01 038673	03-31-2001	Wittwer et al.	Abs.(Engl), Dwg.
	13	WO01 039102	11-02-2001	Muller et al.	
	14	WO01 048339	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.
	15	WO01 048342	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.
	16	WO01 061692	08-23-2001	Trek Technology	
	17	WO01 088693	11-22-2001	Seysen	Abs.(Engl), Dwg.
	18	WO01 096990	12-20-2001	Rainbow Technologies, Inc.	
	19	WO03 014887	02-20-2003	Activcard Ireland	
	20	WO03 034189	04-23-2003	Activcard Ireland	
	21	WO04 002058	12-31-2003	Gemplus	Abs.(Engl), Dwg.
	22	WO04 081706	09-23-2004	Digisafe Ltd.	
	23	WO04 081769	09-24-2004	Axalto SA	
	24	WO05 022288	2005-03-10	Alladin Knowledge Systems	

Examiner Signature _____ Date Considered _____

Electronic Acknowledgement Receipt

EFS ID:	2038706
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	02-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	08:45:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	C18_substitute_IDS_Foreign.pdf	21701 d2187f1b4bb94dc7ed070ac3b718798d0baf2160	no	1
Warnings:					

Information:	
Total Files Size (in bytes):	21701

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Note: this is not an EFS form

Filename: C18_substitute_IDS_NPL

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	1	*ACR38CT Contactless SIM Tracker Technical Specification*, Advanced Card Systems Ltd., Hong Kong.	T
	2	*ACR38DT Dual Key Technical Specifications*, Version 1.3, September 2004, Advanced Card Systems Ltd., Hong Kong.	T
	3	*Dallas Semiconductor DS1490F 2-in-1 Fob*, Dallas Semiconductor, Dallas TX.	T
	4	*Dallas Semiconductor DS9490R-DS9490B USB to 1-Wire/iButton Adaptor*, Maxim I-C, Sunnyvale CA.	T
	5	*Matsushita blends FERAM technology with smart cards*, HARA, YOSHIKO, EE Times, October 1, 2004, CMP Media, Manhasset NY.	T
	6	*Japan's Matsushita developing memory cards with smart chip function*, October 1, 2004, Mercury News, San Jose CA.	T
	7	*OTi-6828 Flash Disk Controller*, Ours Technology Inc., Taiwan.	T
	8	*Panasonic Develops RFID smartSD Card*, October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	*Panasonic Develops Industry's First SD Memory Card with Contacless Smart Card Capabilities*, October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	*Panasonic's Smart SD adds RFID to the mix*, ROJAS, PETER, October 4, 2004, Engadget LLC, New York NY.	T

Examiner Signature _____ Date Considered _____

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**11/779,299**
	Filing Date	**7/18/2007**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor	**FINN, David**
	Art Unit	
	Examiner Name	
Sheet 1 OF 2	Practitioner Docket No.	**FINN-C18**

	11	*Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply*, November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	*Digital Rights pits SIMS against Flash Cards, Card Technology*, BALABAN, DAN, November 2004, pp 24, 25, 26, 28, 30, Card Technology, Chicago IL.	T
	13	*Smart MX P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3*, October 2004, Koninklijke Philips Electronics NV, The Netherlands	T
	14	*Vodafone KK Develops Contactless Smart Card Mobile Handset*, May 6, 2004, HiTEK Magazine, Dubai	T
	15	*SmartSD Card Structure,* Panasonic	T

Examiner Signature _____ Date Considered _____

Electronic Acknowledgement Receipt

EFS ID:	2038710
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	02-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	08:46:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	C18_substitute_IDS_NPL.pdf	33616 b0a1534772baf385779696068da610ed10453bec	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	33616

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 31 050 A 1**

(51) Int. Cl.[6]:
H 04 L 25/20
H 04 L 12/40
H 04 L 29/10
G 08 C 15/00
G 08 C 19/16
G 06 F 13/00

(21) Aktenzeichen: 196 31 050.4
(22) Anmeldetag: 1. 8. 96
(43) Offenlegungstag: 5. 2. 98

(71) Anmelder:
Bergler, Frank, 75223 Niefern-Öschelbronn, DE;
Käuffert, Uwe, 75180 Pforzheim, DE

(72) Erfinder:
gleich Anmelder

(56) Entgegenhaltungen:

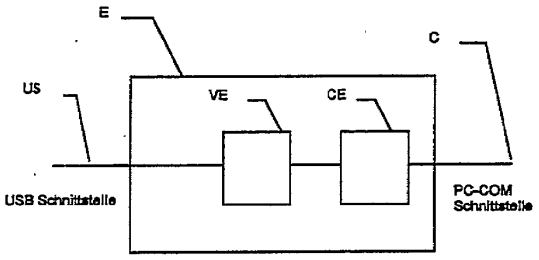
DE	39 31 511 C2
DE	41 15 242 A1
DE	33 22 690 A1
US	50 86 385 A
EP	0 17 035 A1

STRASS,Hermann: Universell, seriell, aber kein Bus. In: Elektronik 20, 1995, S.32-34,38-42;
LANGER,Klaus,D.: Softwareverarbeitung der HDLC-Ebene bitorientierter Protokolle. In: ntz, Bd. 39, 1986, H. 11, S.760,762-764,766,767;
STRASS,Hermann: Neue Stecker braucht das Land. in: DOS, Juli 1996, S.16,18;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Schnittstellenkonverter für USB

(57) Die Universal Serial Bus Schnittstelle soll auf eine andere Schnittstelle umgesetzt werden.
Die Daten von und zur USB Schnittstelle werden in einer erfindungsgemäß realisierten Einrichtung einer Verarbeitungseinheit zugeführt, entsprechend dem USB Protokoll behandelt, in ein anderes geeignetes Übertragungsprotokoll umgesetzt und dann einer anderen nicht nach USB Standard ausgelegten Schnittstelle zugeführt. Diese Schnittstelle kann zum Beispiel eine PC-COM Schnittstelle sein.



DE 196 31 050 A1

DE 196 31 050 A1

Beschreibung

Die vorliegende Erfindung betrifft eine Einrichtung zur bidirektionalen Umsetzung von Signalen zwischen einer USB Schnittstelle und einer anderen Schnittstelle.

Die Universal Serial BUS, USB, ist in der Spezifikation, Revision 1.0 vom 1 Januar 1996 beschrieben; und ist in der vorliegenden Ausgabe der Revision 1.0 öffentlich und für jedermann zugänglich.

Diese Spezifikation beschreibt sowohl die logische Struktur der USB Schnittstelle inklusive der notwendigen Protokolle, Signalisierung und Timinganforderungen als auch die physikalische Struktur. Als physikalisches Übertragungsmedium wird ausschließlich die elektrische Übertragung über ein elektrisch leitendes Kabel definiert.

Der USB Schnittstellenstandard ist ein kabelgebundener Übertragungsstandard, der insbesondere die verschiedenen Anschlußeinheiten wie Tastatur, Maus, Drucker, Video, Audio und sonstige Zusatzeinrichtungen für Workstations und PCs einheitlich mit der Zentraleinheit verbinden soll.

Bekannt sind Protokollumsetzer zwischen unterschiedlichen logischen und physikalischen Schnittstellen. Ein aus dem Stand der Technik bekannter Protokollumsetzer für ISDN konvertiert das nationale 1TR6 Protokoll auf der Benutzerseite in das europäische DSS1 auf der Netzseite.

Stand der Technik ist, daß für diese Anbindung jeweils auf die Aufgabenstellung zugeschnittene Standards verwendet werden, z. B. LPT zur Verbindung von Druckern mit PCs.

Der Erfindung liegt die Aufgabe zugrunde existierende Ein-/Ausgabeeinrichtungen, die nach einem anderen Standard als dem USB Standard arbeiten an den USB Standard anzupassen.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß die auf der USB Schnittstelle kommenden Daten empfangen und auf die andere Schnittstelle umgesetzt werden. Die Signale auf der anderen Schnittstelle werden ebenfalls empfangen und auf die USB Schnittstelle umgesetzt. Alle Anforderungen der USB Spezifikation werden dabei erfüllt.

Im Folgenden wird die Erfindung anhand eines Ausführungsbeispiels für eine Umsetzung auf die PC-COM Schnittstelle und anhand von einer Figur näher erläutert.

Fig. 1 Blockschaltbild.

Die erfindungsgemäß realisierte Einrichtung (E) weist gemäß **Fig.** 1 eine USB Schnittstelle auf und eine PC-COM Schnittstelle. Die Daten der PC-COM Schnittstelle (C) werden an die COM Einheit (CE) weitergeleitet. In der nachgeschalteten Verarbeitungseinheit (VE) werden die Daten auf das USB Protokoll umgesetzt und über die USB Schnittstelle (US) ausgegeben.

Die an der USB Schnittstelle ankommenden Daten werden gemäß der USB Spezifikation und dem vorgeschriebenen Protokoll empfangen, einer Verarbeitungseinheit (VE), welche ein Mikroprozessor oder ein Digitaler Signalprozessor DSP sein kann zugeführt. In dieser Verarbeitungseinheit (VE) werden die Daten ggf. in das für die Übertragung erforderliche Format und Protokoll umgesetzt und anschließend der COM Einheit (CE) zugeführt, um von dort über die COM Schnittstelle (C) übertragen zu werden.

Patentansprüche

1. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere PC-COM Schnittstellen nach V24 und RS232 Standard, **dadurch gekennzeichnet,** daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.

2. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere PC-LPT Drucker Schnittstellen nach Centronics Standard, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.

3. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere CAN Bus Schnittstellen, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.

4. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere LAN Schnittstellen nach Ethernet oder Token Ring Standard, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.

5. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere GGI oder CHI Schnittstellen, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.

6. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB„ Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere PCMCIA Schnittstellen, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.

7. Einrichtung nach mindestens einem der Ansprüche 1—6, dadurch gekennzeichnet, daß eine der USB Schnittstellen auf mindestens 2 unterschiedliche der in den Ansprüchen 1—6 aufgeführten anderen Schnittstellen in der Einrichtung umgesetzt wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 196 31 050 A1
Int. Cl.[6]: H 04 L 25/20
Offenlegungstag: 5. Februar 1998

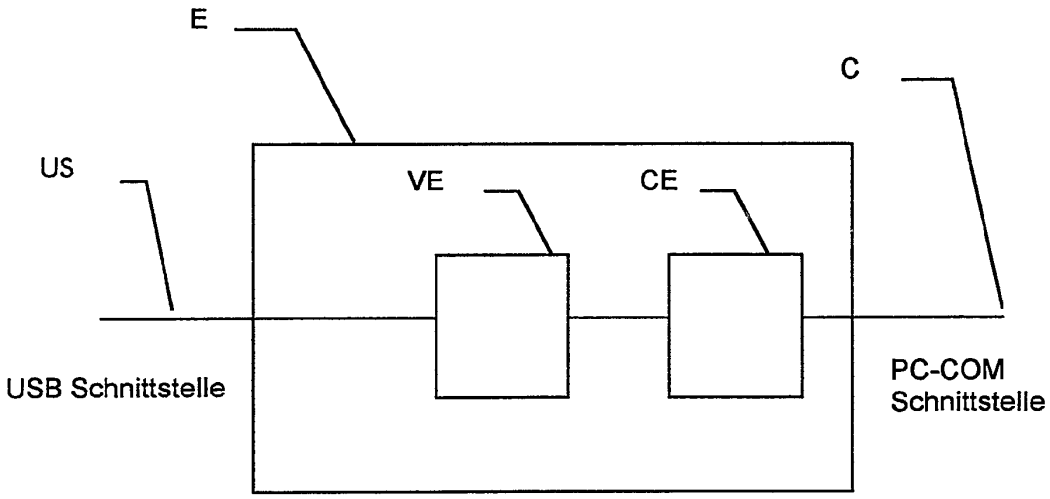


Fig. 1

TITLE

SMART CARD READER WITH CONTACTLESS ACCESS CAPABILITY

FIELD OF INVENTION

This invention relates to an electronic apparatus, and in particular smart-card readers for the dual-mode contact/contactless smart cards.

BACKGROUND OF INVENTION

A smart card consists of an IC chip typically embedded in a flat enclosure. It comes with two popular form factors. One of them is the size of a credit card which is widely used in banking and national ID card projects. The other form factor is the smaller subscriber identification module (SIM card) used in mobile phone. The IC chip itself can simply be a memory chip or a microprocessor chip. Typically, a smart card has eight electric pins which are generally referred to as C1 to C8 to communicate to the external world. Their roles and functions are defined in ISO7816 international standard. A smart card reader is a device that will make electrical contact with each of these pins, so that an external host device can communicate with the smart card through the reader. Out of these 8 pins, ISO7816 standard defines 6 of them for the use of carrying electric power, the clock and reset signals as well as data input and data output signals between the reader and the card. Pins C4 and C8 are not defined and some manufacturers are using these 2 pins to carry out special functions, which will be described later. This type of smart card is said to operate in a contact mode, as it needs to make physical contact with the card reader in order for it to get the electrical power and to communicate with the external world.

There is another kind of smart card that can operate in a contactless mode. It is based on the Radio Frequency Identification (RFID) technology. In this case, the contactless

smart card reader, also known as the interrogator, sends out the Radio Frequency (RF) signal. The contactless smart card has an antenna and RF circuitry which is tuned to receive the RF signal at this frequency. When the contactless card is in the vicinity of the interrogator, it picks up the RF signal, and uses it to power the analogue and digital circuitry within the smart card IC. The interrogator and the contactless smart card also communicate with each other through the same RF channel. The International Standardization Organization (ISO) has published a few standards that stipulate the specifications of contactless smart card operations in detail. They are the ISO14443-type A and type B standards, where the reading distance can be up to 10 cm, as well as the ISO15693 standard where the reading distance is extended to 15 cm or longer. Other vendors adopt the same operating principle but employ their own proprietary standards.

The contactless smart card operates according to the near-field wave propagation principle of the electromagnetic wave theory. Typically, inductive coupling is adopted in this case whereby the RF magnetic field generated by the interrogator induces electric current at the contactless smart card when it moves in the vicinity of the interrogator. To maximize magnetic field coupling, both the antennas of the interrogator and the contactless smart card are arranged in the form of cylindrical loop that consists of multiple turns of electrical wires. At the 13.56MHz frequency specified by the ISO standards, the antenna of the contactless smart card comprises just a few turns. These few turns can be placed along the perimeter of the rectangular shape of a normal size smart card.

Smart cards operating in contact mode have been widely used in many applications where security and privacy are the prime concerns. These include banking transaction, credit card processing, on-line electronic commerce, logical access to computer systems, as well as national identification card projects, health care and social security card projects. Another mass adoption of smart card technology is the subscriber identification card (SIM card) used in the GSM mobile phone handsets. On the other hands, contactless smart card technology is more convenient to use, as users do not need to physically insert the smart card into the card reader. Hence, it is widely used in physical access control, micro-payment of mass transit systems among many other applications. However, the

latter technology may not offer the same level of security protection as the contact mode of operation, because the wireless data transmission could be eavesdropped by a rogue contactless reader located in close proximity of the genuine one.

As a result, vendors have developed a dual-mode smart card that can operate in either contact mode or contactless mode. This card, also known as combi-card, normally has a form factor that is the same size as a normal credit card. It has 8 pin connections as per normal contact smart card which can connect to a smart card reader in contact mode of operation. It also has an embedded antenna inside the card so that it can function as a contactless card by itself.

Such a dual-mode smart card would require a smart card reader for it to perform the contact-mode operation. Unfortunately, not many computer systems carry a smart card reader as their standard peripheral device. However, most computer systems support serial and USB (Universal Serial Bus) ports. Hence, it is desirable to have a device that has a built-in smart card reader to interface with the dual-mode smart card on the one hand, and a USB or serial port to connect to a computer system on the other. If such a device needs to accommodate a credit-card size combi-card, it will be cumbersome for users to carry. Therefore, a dual-mode smart card having the SIM form factor is much preferred. This will enable many new applications. For example, users can store secret keys and password information inside the dual-mode SIM sized smart card. When the user wants to log on to a computer system, he can connect the device to a USB port. A software program can be automatically initiated to authenticate the user and allow him access to the computer. When the user wants to access certain restricted premises, it can function in contactless mode as a physical access device for the user. In another application scenario, the dual-mode smart card can be configured as a store-value card. The user can use the contact-mode of operation to top up the stored value, and use the contactless-mode of operation to pay service fee. The contact-mode ensures high security while the contactless-mode offers user convenience. In fact, the device can be made small enough as a personal electronic key that is always carried by the user in his key-chain.

However, for a dual mode smart card that has a form factor of a SIM card, the loop antenna has to be placed outside the SIM card, as the area encompassing the SIM card is

too small to capture sufficient magnetic flux from the interrogator to power the smart card IC. Some manufacturers makes use of pins C4 and C8, the two pins that are not defined in the ISO7816 standard, to connect the SIM card to the external antenna. Hence it is necessary to design and develop an antenna and its associated circuitry, and incorporate such antenna assembly to the device in the most cost-effective manner without compromising its RF reception quality.

SUMMARY OF INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide an improved apparatus that provides access to a dual-mode smart card either through a smart card reader electronic module to an external host in contact mode of operation, or through an antenna assembly to a contactless card reader in contactless mode of operation. Accordingly, the present invention provides an apparatus comprising the electronic circuitry of a smart-card reader that is adapted to connect to a dual-mode smart card in a contact mode via a smart card connector, and an antenna assembly adapted to connect to the smart card connector for contactless mode operation.

In the preferred embodiment, the entire circuitry of the smart-card reader and the antenna assembly is fabricated in a single printed circuit board so that it can reduce the production cost and improve the reliability. The antenna circuitry may comprise a loop antenna, or it may include other electronic components such as a tuning capacitor. The antenna may be fabricated as thin electrical lines running in loops around the perimeter of the printed circuit board. The circuitry of the smart card reader may be placed at the inner portion of the printed circuit board.

Another aspect of the present invention is to fabricate the antenna in the inner layers of a multi-layer printed circuit board. The loop antenna assembly may occupy more than one layer, with the antenna wire in one layer electrically connected to another layer via electrically conducting through-holes in the printed circuit board so that the multi-layer wiring loops constitutes a single loop antenna.

In a second preferred embodiment, the loop antenna may be embedded in the casing that houses the apparatus. The antenna wiring may be embedded in the casing, and its leads make electrical connection to the rest of the antenna assembly in the printed circuit board. This may minimize the number of layers of printed circuit board.

A method aspect of the present invention is for forming the antenna assembly. The method preferably comprises the steps of: constructing metal connectors in a printed circuit board to realize the circuit diagram of the smart card reader electronic module, embedding at least one metal wire around the perimeter of the printed circuit board, and electrically connecting the metal wire to the smart card connector so that the metal wire functions as an antenna for the antenna assembly for contactless mode operation.

It should be noted that the metal conductors that realize the circuit diagram of the smart card reader electronic module should not form closed loops. Moreover, for a multi-layer printed circuit board, the metal wire for the antenna may occupy more than one layers. In such case, electrically conducting pin-holes will be used to connect wires from multiple layers together so that it constitutes a single antenna.

Another prefer method embodiment comprises the steps of: embedding the smart card reader module on the printed circuit board and embedding the loop antenna on the casing of the apparatus, and electrically connecting the loop antenna to the rest of the antenna assembly.

Another method aspect of the present invention is for accessing the content of the dual-mode smart card. The method preferably comprises the steps of connecting the smart card to an external host via a smart card reader electronic module and exchanging data with the smart card via the electronic module for contact mode of operation; and having an antenna assembly electrically coupling to said smart card and exchange data with a contactless smart card reader in a contactless mode of operation.

BRIEF DESCRIPTION OF FIGURES

FIG. 1 is a block diagram of a dual-mode smart card reader module according to the invention.

FIG. 2 is a dual-mode smart card whose dimension conforms to the SIM form factor.

FIG. 3 is top view of the dual-mode smart card reader device according to the invention with the top cover removed.

FIG. 4 is the top view of the dual-mode smart card reader device according to the invention with the dual-mode smart card inserted to the smart card connector slot of the device.

FIG. 5A, 5B, 5C and 5D are the first, second, third and forth layers of the printed circuit board layouts of the device according to the invention.

FIG. 6 is a cover of the device with an antenna embedded inside the cover.

FIG. 7 shows the printed circuit board installed on the cover of the device with an antenna embedded inside the cover.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is now described in details hereinafter in the preferred embodiments. However, it will be obvious to one skilled in the art that the present invention may be practiced with variation of these specific details. Hence this invention should not be construed as limited to the embodiments set forth herein.

Referring to FIG. 1, the present invention is related to the dual-mode smart card reader module 10, which has two major components: the smart card reader electronic module 11 and the antenna assembly 12. The former establishes a communication path between the external host 21 and the smart card 20 so that the external host 21 can read and write information to the smart card 20 under the contact mode of operation. Likewise, the antenna assembly 12 provides the necessary antenna circuitry to smart card 20 so that the latter can communicate with the contactless smart card reader 22 in contactless mode of operation. In the preferred embodiment, the smart card 20 has a form factor like the SIM card as shown in FIG. 2, and the external host 21 is a computer. The smart card reader electronic module 11 provides a Universal Serial Bus (USB) port 31 for connection to the external host 21. However, it should be obvious to one skilled in the art that other interfacing protocols such as the RS232, the RS442 and the RS485 serial interface, as well as the parallel port interface can also be used. The antenna assembly 12

further comprises an antenna 14 and the antenna tuning circuitry 13. For certain dual-mode smart card, there is no need for antenna tuning and in this situation the antenna assembly 12 contains only the antenna 14.

FIG. 3 illustrates the entire apparatus of the preferred embodiment with the one part of the casing removed. The entire circuitry of the dual-mode smart card reader module 10 is implemented in the printed circuit board 33. In this preferred embodiment, the smart card reader module 10 makes use of the USB port 31 to connect to the external host 21. This module is housed in casing 32. The printed circuit board 33 contains a smart card connector 34 that has 8 pin connectors for making electrical contact with the dual-mode smart card 20. FIG. 4 shows the setting when the smart card 20 is inserted to the smart card connector 34.

FIG. 5 shows the entire layout of printed circuit board 33. In this preferred embodiment, the printed circuit board 34 has four layers. FIG. 5a and FIG. 5d are the top and bottom layers respectively for the mounting of discrete electronic components. The antenna 14 in FIG. 1 is realized in layer 2 and 3 of the printed circuit board 33. As shown in FIG. 5b and 5c, each of these two layers comprises five turns of thin electric wires that constitute a portion of the antenna. These wirings run around the perimeters of the printed circuit board so that the antenna 14 thus formed can capture the maximum amount of magnetic flux radiated from the contactless card reader 22. Thin wire 14a makes contact with layer 1 through electrically conducting pin-hole 15, and also with layer 3 through pin-hole 17. Likewise, thin wire 14b makes contact with layer 2 through pin-hole 17 and with layer 1 through pin-hole 16. As such, wiring 14a and 14b are connected together to form a single antenna 14. Antenna 14 connects to the antenna assembly 12 in printed circuit board 33, which in turn connects to smart card connector 34.

Since the electric power that can be coupled to the smart card 20 from the contactless smart card reader 22 depends on the number of turns that the loop antenna 14 has, and also the area it encloses, the wiring 14a and 14b preferably occupy the perimeter of the printed circuit board 33. To increase the number of turns, the loop antenna 14 occupies two layers of the printed circuit board in this specific embodiment,. Moreover, as surface mount technology is adopted to put electronic components to the printed circuit

board 33, the top and bottom layers are dedicated to for interconnecting electronic components together to realize the circuitry of the dual-mode smart card reader module 10. Hence in the preferred embodiment, the loop antenna 14 occupies the inner two layers. If there is no size constrain, the antenna can be co-located with the rest of the electronic circuitry and hence the number of layers in the printed circuit board 33 can be reduced. Although the present invention has been described specifically using this preferred embodiment, it is clear that many variations and combinations are possible in the light of the teaching provided herein. Specifically, the number of turns of the antenna wiring, its placement on the circuit board, and the number of layers of the printed circuit board used are variations that those skilled in the technical art can adapt to their specific applications.

In another preferred embodiment, the antenna 14 is embedded in the casing 32 as shown in FIG. 6. The antenna can be constructed using thin metal wires wound in loops or other forms, or it can be printed onto the cover using conductive inks. The main purpose is that the antenna thus formed can receive the electromagnetic wave radiated from the contactless card reader. At the printed circuit board 33, spring connectors can be placed directly underneath antenna leads 41 and 42, so that when the cover 32 encloses the printed circuit board 33, these spring connectors make electrical connections to antenna leads 41 and 42. In another preferred embodiment, flexible circuit board can be used to form the antenna 14, and the former can be glued to the back of the cover 32 by adhesive means. The antenna 14 can be connected to the printed circuit board 33 through ordinary electrical wires and connectors. It should be obvious to one skilled in the art that there can be a plurality of methods to embed the antenna 14 to the cover 32 and connect the antenna to the printed circuit board 33; and the antenna can be made using a variety of electrically conducting materials. The preferred embodiment describes herein represents only one approach to reduce the inventive idea to practice. Many other alternatives and variations may be made from the teaching above.

The preferred embodiments of the present invention are thus fully described. Although the description referred to particular embodiments, it should not be construed that the invention is limited to such embodiments, but rather construed according to the claims below.

What is claimed is:

1. An apparatus for reading a dual-mode smart card comprising
   a. a smart card connector adapted to electrically connect to said smart card;
   b. a smart card reader electronic module connecting said smart card connector to an external port, said external port adapted for electrically coupling to an external host for data exchange between said smart card and said external host;
   c. an antenna assembly adapted to electrically connect to said smart card connector for wireless data transmission between said smart card and a contactless smart card reader.
2. An apparatus according to claim 1, wherein said smart card connector is fabricated on a printed circuit board.
3. An apparatus according to claim 2, wherein said antenna assembly is fabricated in said printed circuit board.
4. An apparatus according to claim 3, wherein said printed circuit board is a multi-layer printed circuit board with at least one layer of said printed circuit board containing at least a portion of said antenna assembly.
5. An apparatus according to claim 4 wherein said printed circuit board further comprises multiple layers said antenna assembly being embedded in at least two layers of said printed circuit board with electrically conduction therebetween.
6. An apparatus as in claim 1 or 2, wherein a casing is provided for housing at least a portion of said apparatus, and the antenna of said antenna assembly is embedded as part of said casing.
7. An apparatus as in claim 1, wherein said external port is a USB port.
8. An apparatus as in claim 1, wherein said external port is a serial port.
9. In a smart card reading apparatus containing a smart card reader electronic module for connecting an export port to a smart card connector, said smart card connector adapted to electrically connect to a dual-mode smart card, said smart card electrically coupling to an antenna assembly for contactless mode of operation, a method of forming said antenna assembly comprising the steps of
   a. laying metal conductors in a printed circuit board to connect

i. electronic components of said export port,

ii. said smart card reader electronic module, and

iii. said smart card connector together.

b. embedding at least one metal wire in a position proximate the perimeter of said printed circuit board;

c. electrically connecting said metal wire to said smart card connector such that said metal wire functions as an antenna for said antenna assembly for wireless transmission.

10. A method according to claim 9 further comprising embedding at least a second metal wire in at least a second layer; and connecting said first metal wire with said second wire electrically.

11. A method according to claim 10 wherein said metal wire is embedded in the inner layers of said multiple layer printed circuit board.

12. A method of accessing a dual-mode smart card comprising the steps of connecting said smart card to an external host via a smart card reader electronic module and transferring data to and from said smart card via said electronic module for contact mode of operation; and having an antenna assembly electrically coupling to said smart card and transferring data to and from said smart card for contactless mode of operation.

13. A method according to claim 12 further comprising providing a casing to house said printed circuit board; winding an electrically conducting wire around said casing in multiple turns; and connecting said wire to said antenna assembly in said printed circuit board.

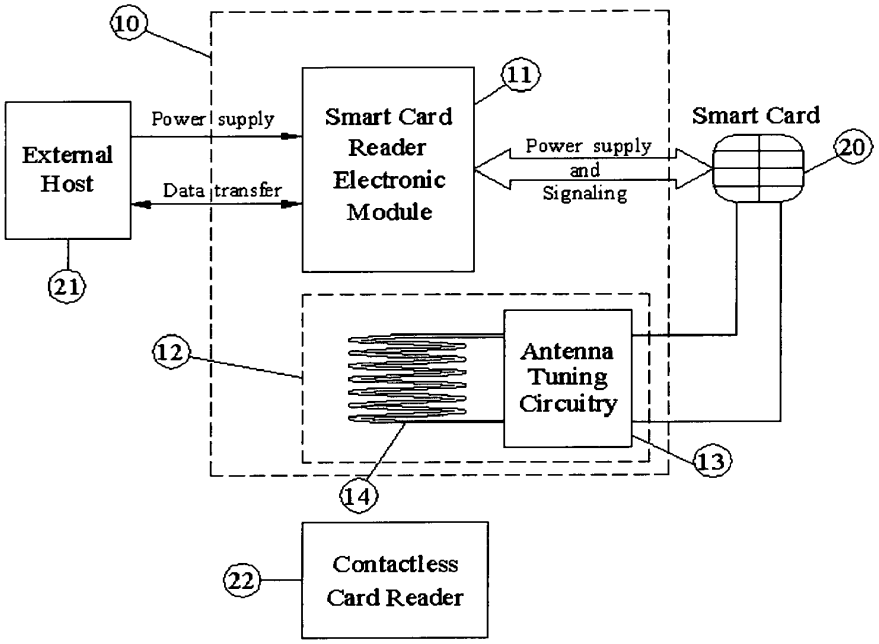


FIG.1

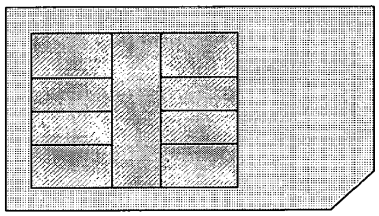


FIG. 2

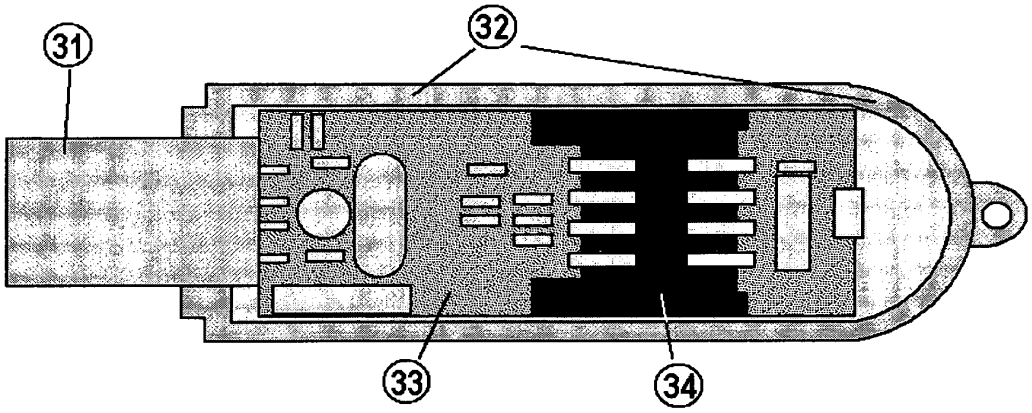


FIG.3

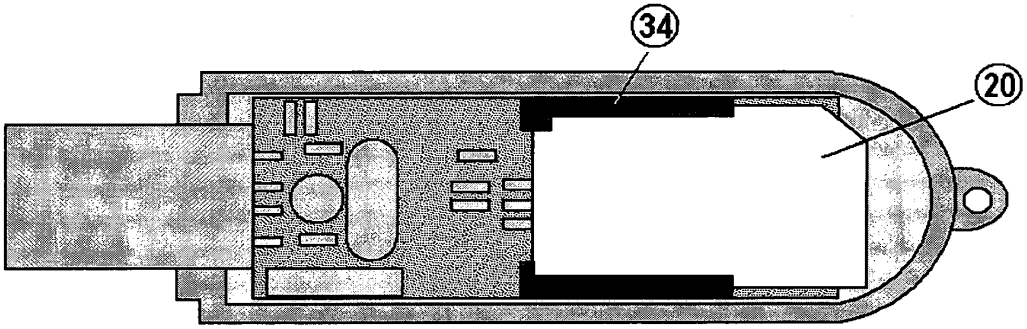


FIG.4

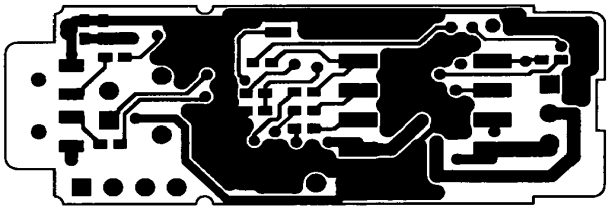


FIG. 5A

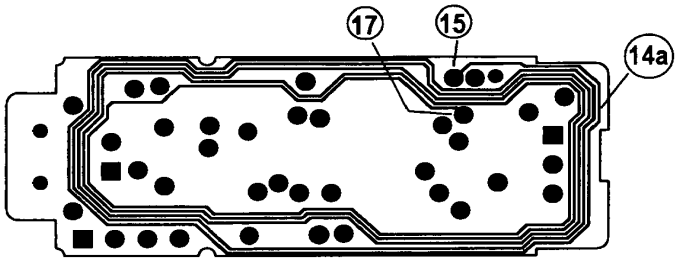


FIG. 5B

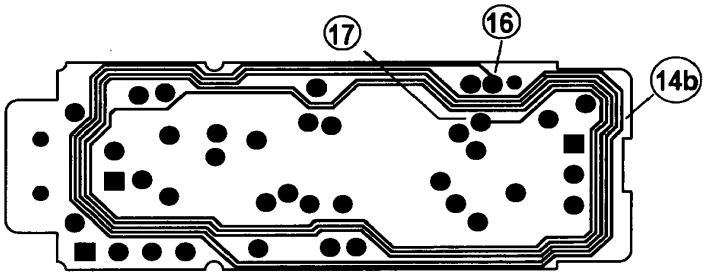


FIG. 5C

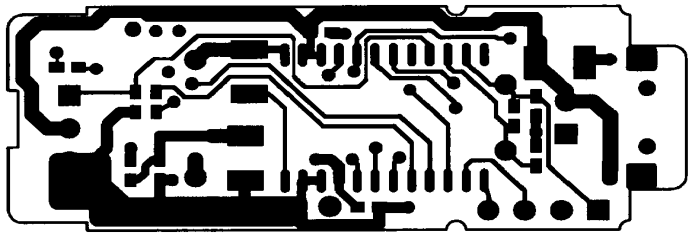


FIG. 5D

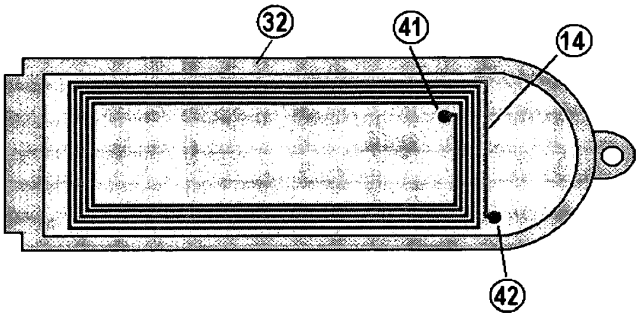


FIG. 6

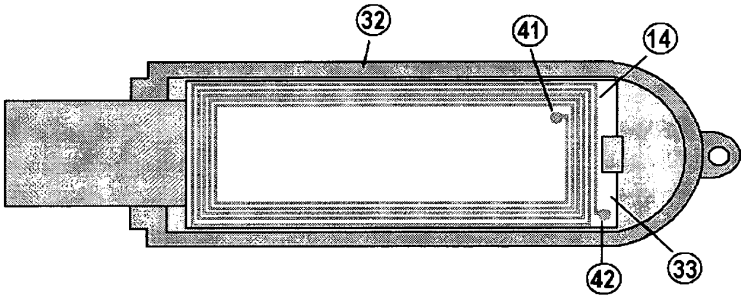


FIG. 7

TITLE

A SMART CARD RELEASING MECHANISM FOR SMART CARD READER

FIELD OF INVENTION

This invention relates to an electronic apparatus, and in particular a smart-card reader that possesses a quick release mechanism for users to retrieve the inserted smart card easily.

BACKGROUND OF INVENTION

Smart IC cards have been widely used in many applications. It consists of an IC chip embedded in a flat enclosure and typically comes with two types of form factors. One of them is the size of a normal credit card. The other is a smaller Subscriber Identification Module (SIM) widely used in mobile phones and is generally referred to as SIM card. A smart card reader is a device that provides a communication path for the host computer to access the content of the smart card. There are smart card readers specially made for the SIM card. Since the SIM card is small enough, the corresponding reader can be made in a size that is handy to carry. It can be used as a secured token for logging on to computer systems or conducting e-commerce transactions. In another application, such a reader can be used to upload the information stored in the SIM card of a mobile phone to a host computer database.

However, it is not easy to remove the SIM card from the reader in existing products. The user typically needs to take a portion of the device's cover away first, and then use his finger to slide the SIM card away from the smart card connector within the device. It is therefore very inconvenient for the user if he needs to access the contents of many SIM cards in a short time. The present invention describes a quick-release mechanism that can

be easily incorporated to a smart card reader so that the user can retrieve the smart card at ease.

SUMMARY OF INVENTION

In view of the background discussion, it is an object of this invention to provide an easy-to-use smart card dispensing mechanism to eject the smart card from a smart card reader apparatus. Accordingly, the present invention relates to an apparatus comprising a housing, a printed circuit board fitted inside the housing with a receiving site to accommodate a smart card, and a smart card dispensing module disposed in between the housing and the printed circuit board. One side of the dispensing module is at least partially exposed to the exterior of the housing while the other side makes mechanical contact to the smart card when the latter is inserted to the apparatus. The first side is adapted to receive a user triggering movement that causes the dispensing module to eject the smart card from the receiving site.

In a preferred embodiment, the housing of the apparatus comprises first and second covers, with an opening on the second cover. One side of the dispensing module comprises a first protruded element that fits to the opening of the second cover for the user to apply his triggering movement. The other side of the dispensing module comprises a second protruded element that makes contact to the smart card when the latter is inserted to the apparatus. In the preferred embodiment, the insertion of the smart card pushes the dispensing module to a first position inside the apparatus. When the user applies a triggering movement onto the first protruding element of the dispensing module, it causes the dispensing module to slide to a second position and eject the smart card from the receiving site.

In the present preferred embodiment, the first protruded element of the dispensing module has at least one groove to facilitate the user to apply his triggering movement. Furthermore, the opening of the second cover has a wider opening at the exterior side compared to the interior side. In addition, the dispensing module further comprises an elongated arm in one sliding direction and a knot at the end of the elongated arm.

Correspondingly, the interior side of the second cover further comprises at least 2 notches so that the knob can rest on one of these notches securely.

The method aspect of the present invention is related to a user-friendly process to release a smart card from the above-described device in its broadest embodiment. The method comprises the steps of pushing the dispensing module to a first position when the smart card is inserted to the device, and ejecting the smart card from the receiving site when the user applies the triggering movement to the first protruding element of the dispensing module, forcing the latter to slide to the second sliding position.

BRIEF DESCRIPTION OF FIGURES

FIG. 1 is the top view of the interior of smart card reader device according to the invention with the second cover removed.

FIG. 2 is a smart card whose dimension conforms to the SIM form factor.

FIG. 3 is the top view of the smart card reader device according to the invention with the smart card inserted into the receiving site of the device.

FIG 4A and 4B are the top view and side view of the first cover that houses the device.

FIG 5A and 5B are the top view and side view of the second cover that houses the device.

FIG. 6A, 6B and 6C are the perspective view, top view and side view of the dispensing module.

FIG. 7A and 7B are the cross-section side views of the apparatus showing respectively the first position of the dispensing module when the smart card is inserted into the device and the second position when it is pushed by the user to eject the smart card.

FIG. 8A and 8B illustrate the beveled edge of the opening of the second cover and its relative positioning against the dispensing module.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is now described in details hereinafter in the preferred embodiments. However, it will be obvious to one skilled in the art that the present invention may be practiced with variation of these specific details. Hence this invention should not be construed as limited to the embodiments set forth herein.

FIG. 1 shows a printed circuit board 20 fitted inside the first cover 11. The printed circuit board 20 connects the electronic components soldered in it to implement the smart card controller logic. One of the components is the receiving site 21 specially made to house the SIM card. FIG. 2 depicts the smart card 22 in SIM form factor. The printed circuit board 20 also connects to a Universal Serial Bus (USB) connector 23 that serves as a mean to communicate to the host computer. However, it should be obvious to one skilled in the art that other interfacing protocols such as the RS232, RS485, or RS422 serial protocol and other parallel interfaces can also be adopted. FIG. 3 shows the apparatus with the smart card 22 inserted into the receiving site 21 thereof. FIG. 4A and 4B are the top and side views of the first cover 11 of the housing, whilst FIG. 5A and 5B are the top and side views of the second cover 30 respectively. Both the first and second covers 11 and 30 respectively have recesses 12 and 34 at the front so that when the first cover 11 are placed on top of the second cover 30, an open space at the front of the apparatus is formed so that the smart card 22 can slide in. The second cover has an opening 31 and also a plurality of notches 32 as shown in FIG. 5A. FIG. 6A, 6B and 6C are the perspective, top and side views of the dispensing module 40 that is fitted in between the second cover 30 and the printed circuit board 20. The dispensing module 40 comprises a first protruding element 43 that is fitted to the opening 31 of the second cover 30. It also comprises a second protruding element 45 on the other surface of the dispensing module 40, and an elongated arm 41. The end of the elongated arm 41 comprises a knob 42. The dispensing module 40 can slide inside the apparatus with little restriction. FIG. 7A indicates a cross section view of the apparatus when smart card 22 is inserted. Specifically, when the smart card 22 is being inserted, it makes contact to the second protruding element of the dispensing module 45, and pushes the dispensing module 40 to a first position inside the apparatus. When the smart card 22 is fully inserted,

it sits on the receiving site 21 which has electrical contacts that connect to the respective contacts of the smart card 22.

To release the smart card 22 from the apparatus, a user can apply a triggering movement by placing his finger on the first protruding element 43 of the dispensing module 40, and exert a force to push it outward to a second position. As a result, the smart card 22 is disengaged from the receiving site 21 and is partially exposed outside the apparatus as shown in FIG. 7B so that it can be retrieved by the user easily.

In the preferred embodiment, the first protruding element 43 of the dispensing module 40 further comprises a plurality of grooves 44 to facilitate the user to securely place his fingers onto the dispensing module 40 and to exert force. Moreover, the second cover 30 comprises a plurality of notches 32 so that knob 42 can rest on one of these notches 32. This will prevent the dispensing module 40 to slide freely inside the apparatus and causes it to either rest on a first position or a second position as mentioned earlier.

Yet another invention in the present preferred embodiment is related to the shape of the opening 31 of the second cover 30 as shown in FIG. 8A. The opening 31 comprises a beveled edge 35 that is wider in the exterior side compared to the interior side 36. When the first protruding element 43 is fitted to the opening 31 as shown in FIG. 8B, the top of the first protruding element 43 of the dispensing module 40 needs not be higher than the second cover 30 to cause unevenness when the apparatus is placed on a flat surface, yet the beveled edge 35 allows the user's finger to get deeper into the opening 31 so that the finger can make a firmer contact with the first protruding element 43.

The preferred embodiments of the present invention are thus fully described. Although the description referred to specific embodiments, it should be understood that the invention is not limited to such embodiments, but rather construed according to the claims below.

What is claimed is:

1. A smart card reader apparatus comprising:
   a. a housing
   b. a printed circuit board disposed within said housing and implementing a smart card reader module, said printed circuit board further comprising a receiving site adapted to receive a smart card,
   c. a smart card dispensing module disposed within said housing, said smart card dispensing module further having a first side at least partially exposed to the exterior of said housing and adapted to receive user instruction and a second side adapted to mechanically couple to said smart card such that a triggering movement of the user on said first side of said dispensing module can cause said dispensing module to eject said smart card from said receiving site.
2. An apparatus according to claim 1 wherein said housing comprising a first cover and a second cover, said second cover further comprising an opening for exterior access of said first side of said smart card disposing module by said user.
3. An apparatus according to claim 2 wherein said opening of said second cover further comprising an exterior side and an interior side, said exterior side having a beveled edge with outer perimeter wider than the inner perimeter to allow easy access.
4. An apparatus according to claim 2 wherein said dispensing module is dispose between said housing and said printed circuit board, said dispensing module further adapted to slide to a first position when said smart card is inserted in said receiving site and to a second position when said user exerts said triggering movement.
5. An apparatus according to claim 4 wherein said first side of said dispensing module further comprising a first protruded element extending through said opening of said second cover adapted for receiving said triggering movement of said user.
6. An apparatus according to claim 4 wherein said second side of said dispensing module further comprising a second protruded element adapted to establish mechanical contact with said smart card when it is inserted to said apparatus.

7. An apparatus according to claim 5 wherein said first protruded element of said dispensing module has at least one groove to facilitate said user to exert said triggering movement.
8. An apparatus according to claim 2 wherein said dispensing module further comprising an elongated arm in one sliding direction and a knob at the end of said elongated arm.
9. An apparatus according to claim 8 wherein the interior of second cover further comprising at least 2 notches so that said knob of said elongated arm of said dispensing module rests on one of said notches of said second cover securely.
10. A method of ejecting a smart card from an apparatus that comprises a housing, a printed circuit board that houses a smart card receiving site, a first cover of said housing, a second cover with an opening, a dispensing module disposed in between said printed circuit board and said second cover, a first protruding element in one surface of said dispensing module fitted to said opening of said second cover and a second protruding element in the opposite surface of said dispensing module comprising:
    a. pushing said dispensing module to a first sliding position when said smart card is inserted and fitted onto said smart card receiving site,
    b. ejecting said smart card from said receiving site when said user applies said triggering movement onto said first protruding element of said dispensing module causing said dispensing module to slide to said second sliding position.

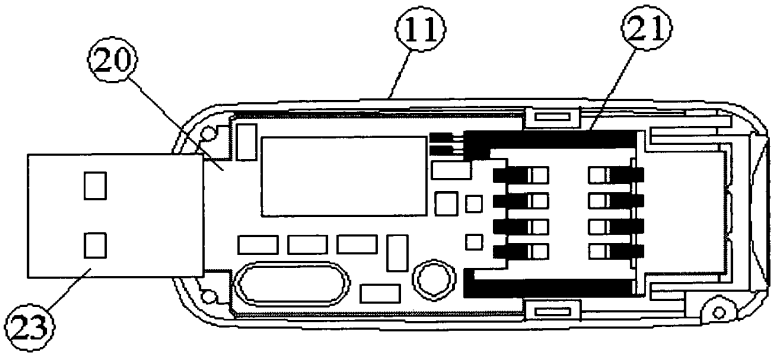


FIG. 1

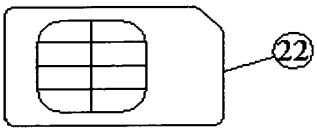


FIG. 2

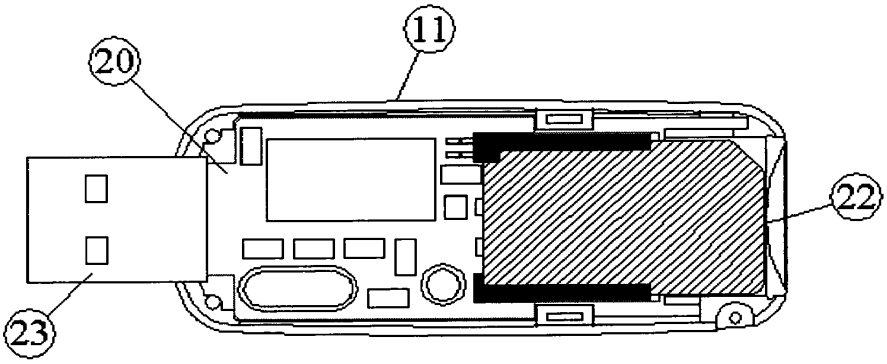


FIG. 3

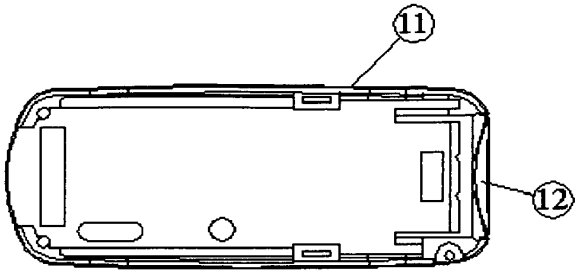


FIG. 4A

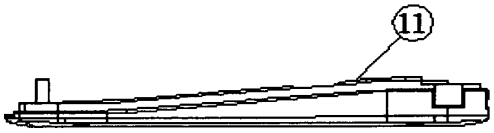


FIG. 4B

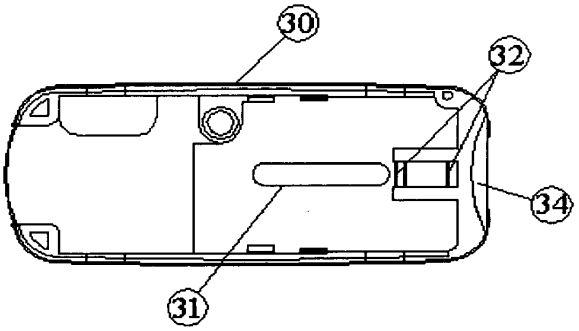


FIG. 5A

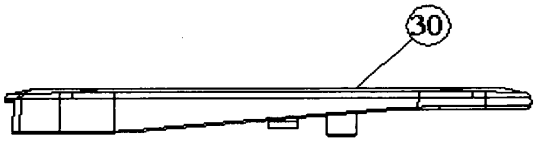


FIG. 5B

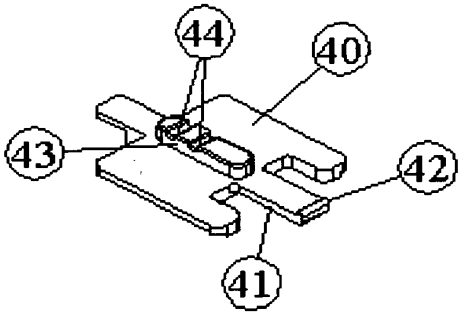


FIG. 6A

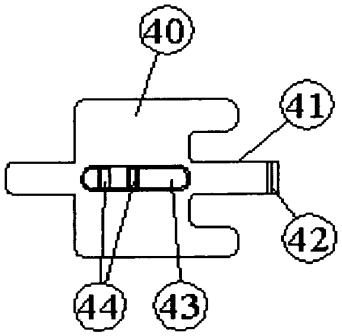


FIG. 6B

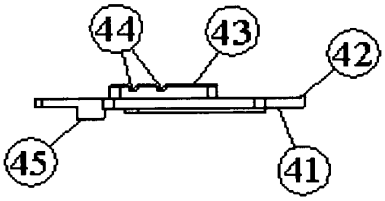


FIG. 6C

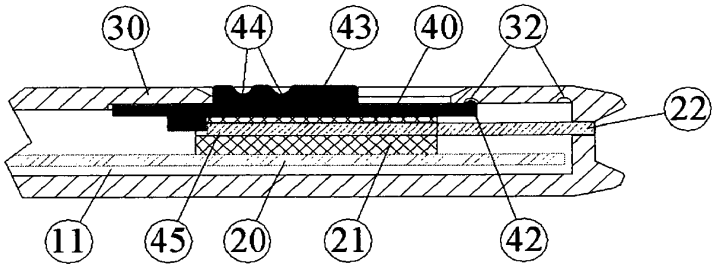


FIG. 7A

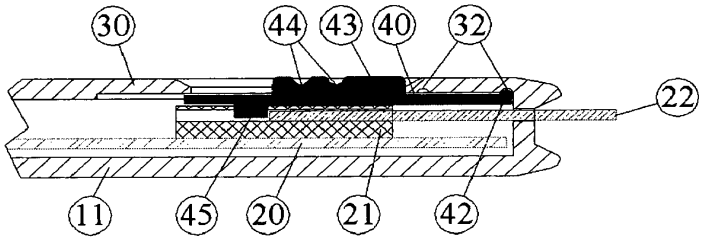


FIG. 7B

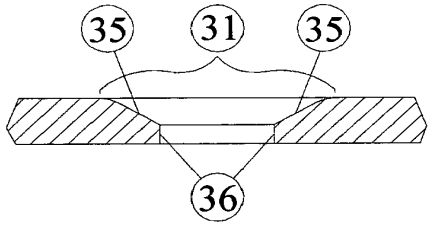


FIG. 8A

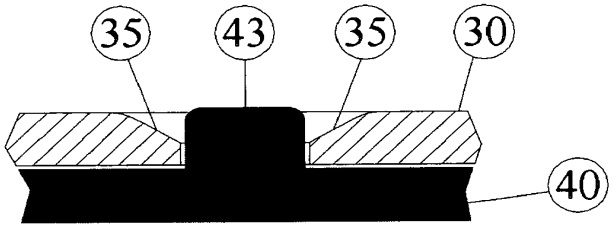


FIG. 8B

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-246720
(P2004-246720A)
(43)公開日　平成16年9月2日(2004.9.2)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 9/445	G06F	9/06	610A	5B014
G06F 1/00	G06F	13/10	330B	5B076
G06F 13/10	G06F	15/00	330B	5B085
G06F 15/00	G06F	15/00	390	
	G06F	9/06	610L	

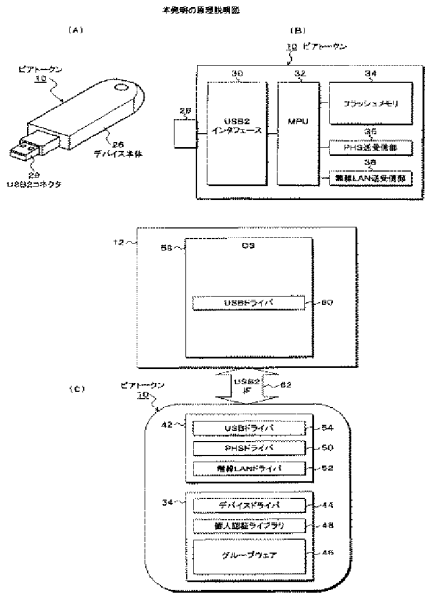
審査請求 未請求　請求項の数 5　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願2003-37225(P2003-37225)
(22)出願日　平成15年2月14日(2003.2.14)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100079359
弁理士　竹内　進
(72)発明者　佐沢　真一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　佐藤　裕一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　千田　陽介
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
最終頁に続く

(54)【発明の名称】情報処理デバイス、情報処理方法及びプログラム

(57)【要約】
【課題】任意のパーソナルコンピュータに個人認証を必要とするグループウェア等の個人の作業環境を簡単に構築して利用可能とする。
【解決手段】ピアトークン１０と呼ばれる情報処理デバイスは、電源供給とデータ転送が可能なパーソナルコンピュータ１２のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ４４、ＵＳＢドライバ５４、個人認証ライブラリ４８、グループウェア４６、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリ３４をもつ。ピアトークン１０をパーソナルコンピュータ１２のデバイスポートに接続すると、デバイスドライバのインストール、個人認証ライブラリのインストールによる個人認証を経てアプリケーションプログラムをインストールして実行させる。
【選択図】　図１



【特許請求の範囲】
【請求項1】
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、
外部装置に対し無線回線により情報を送受する第１無線通信部と、
外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、
デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリと、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせ、インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させ、前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部と、
を備えたことを特徴とする情報処理デバイス。
【請求項2】
請求項１記載の情報処理デバイスに於いて、前記アプリケーションプログラムは複数の情報処理装置でデータを共有するピアツーピア型のグループウェア処理プログラムであることを特徴とする情報処理デバイス。
【請求項3】
請求項１記載の情報処理デバイスに於いて、前記不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すディレクトリ情報を登録し、前記アプリケーションプログラムは、他の情報処理装置の差込み時に、前記レジストリ情報により前記サーバからファイルを取得して前記自己の情報処理装置の作業環境を構築することを特徴とする情報処理デバイス。
【請求項4】
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスの情報処理方法に於いて、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる個人認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を備えたことを特徴とする情報処理方法。
【請求項5】
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコ

ネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスのコンピュータに、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を実行させることを特徴とするプログラム。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、任意のパーソナルコンピュータに対し個人のコンピュータ環境を構築する携帯型の情報処理デバイス、情報処理方法及びプログラムに関し、特に、ピアツーピア型のグループウェアのコンピュータ環境を簡単に構築する情報処理デバイス、情報処理方法及びプログラムに関する。
【０００２】
【従来の技術】
従来、自分のパーソナルコンピュータと同じ環境を出張などの外出先で実現する方法としては、ラップトップやＰＤＡといった携帯型のデバイスに個別に自己の作業環境を構築しておき、事前に作業に必要なデータを日常的に使用しているデスクトップ等からメールの添付や無線回線などを利用して転送し、これを持ち運んで使用している。
【０００３】
また出張先によっては、そこに設置しているデスクトップ等を自由に使用できる場合があることから、文書入力といった汎用的なアプリケーションで足りる場合には、パーソナルコンピュータを借用して作業することができる。
【０００４】
【特許文献１】
販売元株式会社サクセス、製造元エニワン株式会社、“ＵＳＢストレージ［ビー・エニィウェアー］”、［平成１５年２月３日検索］、インターネット＜ＵＲＬ　：　ＨＹＰＥＲＬＩＮＫ　ｈｔｔｐ：／／ｂｅｅｍａｉｌ．ｊｐ／ａｎｙｗｈｅｒｅ．ｈｔｍｌ　ＵＲＬ：／／ｗｗｗ．ｂｅｅｍａｌ．ｊｐ／／ａｎｙｗｈｅｒｅ．ｈｔｍｌ＞
【０００５】
【発明が解決しようとする課題】
しかしながら、パーソナルコンピュータの環境は、デスクトップやラップトップといったパーソナルコンピュータ毎に固有な場合がほとんどであり、例えば、メールの場合、事務所等に設置して使用しているデスクトップと出張に持ち歩くラップトップとでは、アドレス帳などの環境や受信メール本体に常に差分が生じてしまい、非常に不便な状況が発生している。
【０００６】
このような問題を解決するため、例えばウェブメールやＩＭＡＰ４等のプロトコルによるサーバによる一元管理の方法もあるが、一元管理に伴う個人毎の容量制限やクライアント

・サーバモデルによる反応速度の低下といった問題がある。

【０００７】

また持ち歩いているラップトップにつき、無線ＬＡＮやＰＨＳを使ってメール等を通信する場合、それぞれ専用のパーソナルコンピュータ向けのＭＣＩＡカードが必要であり、場合によってはパーソナルコンピュータ毎にドライバソフトのインストールし、必要な設定作業を行うといった面倒な作業が要求される。

【０００８】

更に、サーバ等にアクセスしてデータを利用する場合、通常、ＩＤとパスワードを入力する個人認証を必要とし、そのため出張時にラップトップを使用する場合にも煩雑な認証操作が必要となる。この問題を解消するものとしてＵＳＢトークンまたはＩＣカードによる個人認証デバイスが存在する。しかし、これらの個人認証デバイスは、個人認証を行う機能に限られており、個人のコンピュータ環境の構築には対応していない。

【０００９】

一方、メモリステックのようにメモリのみを内蔵したカードやトークンも存在するが、これらは単なるメモリ機能しか持たず、個人のコンピュータ環境の構築には対応していない。

【００１０】

更にＵＳＢの内部にメールソフトを予めインストールしたデバイスも存在するが（特許文献１）、用途がメールに限られており、認証を含む汎用的なアプリケーションに対応したコンピュータ環境の構築には対応できない。

【００１１】

本発明は、任意のパーソナルコンピュータに個人認証を必要とするグループウェア等の個人の作業環境を簡単に構築して利用できる情報処理デバイス、情報処理方法及びプログラムを提供することを目的とする。

【００１２】

【課題を解決するための手段】

図１（Ａ）（Ｂ）（Ｃ）は本発明の原理説明図である。本発明の情報処理デバイス（ピアトークン１０）は、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部（ＰＨＳ送受信部３６）と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部（無線ＬＡＮ送受信部３８）と、デバイスドライバ４４、ポートドライバ、個人認証ライブラリ４８、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリ（フラッシュメモリ３４）と、ポートコネクタを情報処理装置（パーソナルコンピュータ１２）のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせ、インストールされたデバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合にアプリケーションプログラムをインストールして実行させ、認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部とを備えたことを特徴とする。

【００１３】

このため本発明は、情報処理デバイスを任意のパーソナルコンピュータやＰＤＡ等のデバイスポートに差し込むだけで、個人認証画面が自動的に立ち上がり、個人認証を済ませた後は、グループウェア等のアプリケーション画面が立ち上がり、外部との送受信を含む作業をすぐ始めることができる。

【００１４】

また無線通信機能が二重化されており、使用場所の無線環境に合わせて自動切換えして外部装置に確実にアクセスできる。

【００１５】
更にアプリケーションの実行で使用されたデータは全て不揮発メモリに保存され、また本発明のデバイスを抜いて処理を終えると、パーソナルコンピュータにインストールしたプログラムやドライバは全てアンインストールされ、本発明のデバイスを差し込んで使用したパーソナルコンピュータ本体の環境をまったく侵蝕することがない。
【００１６】
ここでデバイス本体２６は持ち運び自在なキー型である。またデバイスポートは例えばＵＳＢ２コネクタ２８であり、ポートドライバはＵＳＢドライバ５４である。更に第１無線通信部はＰＨＳ無線回線を使用するＰＨＳ送受信部３６であり、第２無線通信部は無線ＬＡＮを使用する無線ＬＡＮ送受信部３８である。
【００１７】
本発明の情報処理デバイスによりインストールするアプリケーションプログラムは、複数の情報処理装置でデータを共有するピアツーピア型のグループウェア４６の処理プログラムである。
【００１８】
このようにアプリケーションプログラムがグループウェア処理プログラムの場合、個人認証ライブラリは第１又は第２無線通信部により外部の認証サーバに接続して認証処理を実行させる。
【００１９】
グループウェア処理プログラムは、不揮発メモリに共有データを保持し、起動時にグループウェアに属している他の情報処理装置の保持している共有データとの同期をとる。即ち、グループウェア処理プログラムは、自己の共有データと他の情報処理装置との非同期を検知した場合、他の装置から差分データを受信してマージすることにより共有データの同期をとる。このため出張先のコンピュータを使用する際にも、最新の共有データを利用できる。
【００２０】
グループウェア処理プログラムは、使用済みファイルを不揮発メモリに格納する際にメモリ容量の不足を検知した場合、ファイルリストの末尾に格納しているファイルをグループウェアに属する他の情報処理装置に転送した後にファイルを消去して保存先のリンク情報を格納し、その後に使用済みファイルをファイルリストの先頭位置に格納する。
【００２１】
このためデバイス内蔵メモリに制約があっても、グループウェアに属する例えば近隣のピア装置となるパーソナルコンピュータに共有データを転送保持させ、そのリンク情報のみをデバイス内に保持することで、メモリ容量に制限があっても共有データを確実に保存できる。このデバイスの不揮発性メモリに保持したリンク情報は、自分のパーソナルコンピュータを使用する際に、本発明のデバイスを差し込むことによりリンク情報で指定される保存先から実データを取得して保持することができる。
【００２２】
また情報処理デバイスにあっては、不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すレジストリ情報を登録し、アプリケーションプログラムは、他の情報処理装置の差込み時に、不揮発メモリに登録しているレジストリ情報によりサーバからファイルを取得して自己の処理装置の作業環境を構築する。
【００２３】
本発明の別の形態にあっては、情報処理デバイスのポートコネクタにより接続する情報処理装置は携帯電話であり、この場合、アプリケーションプログラムは、交通機関の改札ゲートの通過時にゲート開制御と課金処理を行うことを特徴とする。また情報処理デバイスのポートコネクタにより接続する情報処理装置は携帯電話であり、アプリケーションプログラムは、自動販売機との間で商品の購入処理を行うことを特徴とする。このように交通機関の改札や自動販売機の利用につき、無線機能を利用した処理が簡単にできる。
【００２４】

本発明は任意のパーソナルコンピュータにグループウェア等の個人の作業環境を簡単に構築して利用できる情報処理方法を提供する。

【００２５】

即ち、本発明は、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスの情報処理方法であって、

ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせる起動ステップと、

インストールされたデバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合にアプリケーションプログラムをインストールして実行させる実行ステップと、

認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時にデバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を備えたことを特徴とする。

【００２６】

本発明は、任意のパーソナルコンピュータにグループウェア等の個人の作業環境を簡単に構築して利用できるコンピュータで実行されるプログラムを提供する。

【００２７】

即ち、本発明のプログラムは、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスのコンピュータに、

ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせる起動ステップと、

インストールされた前記デバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合にアプリケーションプログラムをインストールして実行させる実行ステップと、

認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時にデバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を実行させることを特徴とする。

【００２８】

なお、本発明の情報処理方法及びプログラムの詳細は、情報処理デバイスと基本的に同じになる。

【００２９】

【発明の実施の形態】

図２は、本発明によるピアトークンと呼ばれる情報処理デバイスが適用されるシステム環境の説明図である。

【００３０】
図２において、本発明の処理デバイスはピアトークン１０として実現されている。ピアトークン１０は無線ＬＡＮとＰＨＳの二重化された通信機能を持ち、個人認証環境及びグループウェアシステム環境を不揮発メモリ上に内蔵したトークン型の外部ペリフラル装置である。
【００３１】
このピアトークン１０は、例えば出張先で使用することのできるパーソナルコンピュータで１２のＵＳＢ２ポートに差し込むことで、使用先となるパーソナルコンピュータ１２の環境を犯すことなく認証作業を行い、且つグループウェアシステム環境をパーソナルコンピュータ１２上に構築し、ピアツーピア型のグループウェアによる処理を可能とする。
【００３２】
このようなピアトークン１０の使用環境にあっては、ピアトークン１０の無線ＬＡＮ及びＰＨＳの通信機能を利用して、ＰＨＳ基地局２０または無線ＬＡＮに対応したホットスポット２２との間に通信回線を確立し、インターネット１６を経由して例えばプロキシサーバ１８を介したＬＡＮ１５に接続されているグループウェアに属するピア装置１４－１～１４－３や、インターネット１６に直接接続されるピア装置１４－４との間でデータを共有するグループウェアシステムを構築する。また、ピアトークン１０を使用先となるパーソナルコンピュータ１２に差し込んだ際の個人認証の処理に対応し、インターネット１６を介して認証サーバ２４が設けられている。
【００３３】
図３は、本発明によるキー型のピアトークン１０の外観を示している。ピアトークン１０は、樹脂成型されたパッケージによるデバイス本体２６をキー型に構成し、デバイス本体２６の一端にパーソナルコンピュータやＰＤＡなどの情報処理装置に接続するためのデバイスコネクタとして例えばＵＳＢ２コネクタ２８を設けている。
【００３４】
ここでＵＳＢ２インタフェースは、パーソナルコンピュータ及びＰＤＡ側のＵＳＢ２ポートに対するコネクタ接続でピアトークン１０に対し電源供給を行うと同時にデータ転送を行うことができる。
【００３５】
図４は、本発明によるピアトークン１０のハードウェア構成のブロック図である。図４において、ピアトークン１０にはパーソナルコンピュータやＰＤＡに差し込むためのＵＳＢ２コネクタ２８が設けられ、これに続いてＵＳＢ２インタフェース３０及びＭＰＵ３２が設けられている。
【００３６】
ＭＰＵ３２に対しては、不揮発メモリであるフラッシュメモリ３４が接続される。またＭＰＵ３２に対しては、外部装置との無線回線によるデータ転送を行うためＰＨＳ送受信部３６と無線ＬＡＮ送受信部３８が設けられている。
【００３７】
図５は、図４のフラッシュメモリ３４の格納内容となるメモリマップの説明図である。このメモリマップ４０に示すように、フラッシュメモリ３４には、デバイス処理プログラム４２、デバイスドライバ４４、アプリケーションプログラムとしてのグループウェア４６、個人認証ライブラリ４８、ＰＨＳドライバ５０、無線ＬＡＮドライバ５２及びＵＳＢドライバ５４が予め格納されている。
【００３８】
このようなプログラム領域に続く残りの領域はデータ領域５５となっており、この実施形態のアプリケーションであるグループウェアシステム環境の構築により送受信されたファイルデータが格納される。このデータ領域は、グループウェアシステム環境の場合には、右側に取り出して示すようにファイルリスト５６と実データ域５７で構成されている。
【００３９】
ここで、メモリマップ４０の先頭に格納されているデバイス処理プログラム４２は、ＭＰ

Ｕ３２による実行でピアトークン１０のＯＳとなるデバイス処理部として動作する。次のデバイスドライバ４４は、ピアトークン１０をパーソナルコンピュータやＰＤＡに差し込んだ際のピアトークン１０とのやり取りを行うためのプログラムであり、パーソナルコンピュータやＰＤＡ側にこのデバイスドライバ４４がない場合には、初期処理によりデバイスドライバ４４をインストールして、ピアトークン１０とのやり取りを行わせる。

【００４０】

グループウェア４６はアプリケーションプログラムであり、パーソナルコンピュータやＰＤＡ側にインストールされたデバイスドライバ４４の処理により差し込み先にダウンロードされてグループウェアシステム環境を作り、ピアツーピア型のデータ共有による送受信を行う。

【００４１】

個人認証ライブラリ４８は、グループウェア４６のインストールに先立つ個人認証処理のために差込み先にインストールされ、認証画面を開くことでユーザによるＩＤとパスワードの入力を受け、外部の認証サーバ２４とのやり取りで認証処理を行う。

【００４２】

ＰＨＳドライバ５０は図４のＰＨＳ送受信部３６を動作し、図２のようにＰＨＳ基地局２０との間に無線回線を確立して、ピアトークン１０の差込みで個人認証ライブラリ４８及びグループウェア４６がインストールされた使用先となるパーソナルコンピュータ１２のグループウェアシステム環境における例えば認証サーバ２４との間の認証のための通信、あるいはピア装置１４－１～１４－４との間のピアツーピアのデータ送受信を行う。

【００４３】

無線ＬＡＮドライバ５２は、図４の無線ＬＡＮ送受信部３８を制御し、図２のホットスポット２２との間で無線回線を確立し、同じくグループウェアシステム環境における個人認証処理や他のピア装置１４－１～１４－４との間のデータ共有のための送受信を行う。

【００４４】

このＰＨＳドライバ５０と無線ＬＡＮドライバ５２は、２つの無線回線を切り替えて使用するために設けられており、ピアトークン１０を差し込んだパーソナルコンピュータやＰＤＡの使用環境に応じ、いずれか一方の通信回線を自動的に選択して外部装置との間の送受信を行う。

【００４５】

図６は、本発明のピアトークン１０をパーソナルコンピュータ１２に差し込んでＵＳＢ２インタフェース６２による接続を確立した起動時の説明図である。パーソナルコンピュータ１２のＵＳＢに図３に示すピアトークン１０のＵＳＢ２コネクタ２８を差し込むと、パーソナルコンピュータ１２側からＵＳＢ２インタフェース６２の電源ラインを通じてピアトークン１０に電源供給が行われ、図４に示したピアトークン１０のハードウェアが起動し、図５のデバイス処理プログラム４２がＭＰＵ３２のメモリ領域に読み込まれて実行され、このデバイス処理プログラム４２の実行により、ＵＳＢドライバ５４、ＰＨＳドライバ５０及び無線ＬＡＮ５２が動作状態となる。

【００４６】

ピアトークン１０をパーソナルコンピュータ１２に差し込んだ際にパーソナルコンピュータ１２側にピアトークン１０のデバイスドライバ４４が存在しなかった場合には、図７のようなインストール要求画面４５がパーソナルコンピュータ１２側で表示され、デバイスドライバ４４のインストールを促す。

【００４７】

そこで、ユーザはインストール要求画面４５に続いてアイテム４５－１に示されている「一覧または特定の場所からインストールする」を選択して移行ボタン４５－２を操作すると、パーソナルコンピュータ１２のＵＳＢドライバ６０からピアトークン１０のＵＳＢドライバ５４にインストール要求のためのコマンドが転送され、図８のようにフラッシュメモリ３４からデバイスドライバ４４が読み出され、パーソナルコンピュータ１２のＯＳ５８の処理機能の１つとしてデバイスドライバ４４－１がインストールされる。

【００４８】
ピアトークン１０のデバイスドライバ４４－１がインストールされると、図９のようにデバイスドライバ４４－１によってピアトークン１０から個人認証ライブラリ４８－１がインストールされ、認証画面がパーソナルコンピュータ１２に表示される。
【００４９】
このためユーザは、認証画面の入力枠に対しＩＤとパスワードを入力して認証を要求すると、図２のようにＰＨＳ基地局２０またはホットスポット２２にある無線ＬＡＮのいずれかによる無線回線により認証サーバ２４に対し認証要求が行われ、正しいユーザであれば承認応答が得られる。
【００５０】
このような認証に成功すると、パーソナルコンピュータ１２側のデバイスドライバ４４－１は、図１０のようにピアトークン１０のグループウェア４６をパーソナルコンピュータ１２のＯＳ５８の配下のアプリケーションプログラムであるグループウェア４６－１としてインストールし、これによってグループウェアシステム環境がパーソナルコンピュータ１２側に構築される。
【００５１】
ここで、パーソナルコンピュータ１２はピアトークン１０を保有しているユーザが例えば出張などにより借用した装置であり、ピアトークン１０の差込みにより、借用したパーソナルコンピュータ１２上にユーザ個人のグループウェアシステム環境を個人の認証処理のみをもって簡単に構築することができる。
【００５２】
図１１は、パーソナルコンピュータ１２から本発明のピアトークン１０を外した際の説明図である。パーソナルコンピュータ１２にピアトークン１０を差し込んでグループウェアシステム環境による共有データの送受信や処理を行って作業を終了したならば、グループウェアシステム環境のアプリケーション終了を行った後にピアトークン１０をパーソナルコンピュータ１２から外し、ＵＳＢ２インタフェース６２による接続を切り離す。
【００５３】
このピアトークン１０の切り離しに先立ってグループウェアのアプリケーション終了操作が行われると、パーソナルコンピュータ１２からピアトークン１０に対し終了通知が行われ、ピアトークン１０側で必要な終了処理が行われると同時に、パーソナルコンピュータ１２側にあっては、図１１のようにパーソナルコンピュータ１２側にインストールされているデバイスドライバ４４－１、個人認証ライブラリ４８－１及びグループウェア４６－１のアンインストールが自動的に行われる。
【００５４】
またグループウェアシステム環境の構築で送受信されたデータについては、全てピアトークン１０のフラッシュメモリ３４に保存されている。このため、ピアトークン１０をパーソナルコンピュータ１２から外した場合、ピアトークン１０の差込みで構築した環境は全て削除され、ピアトークン１０によりパーソナルコンピュータ１２を利用しても、使用後にあってはパーソナルコンピュータ１２にピアトークン１０の使用による環境を一切残すことがなく、パーソナルコンピュータ１２の環境をピアトークン１０の使用で侵すことがない。
【００５５】
図１２は、本発明のピアトークン１０を出張先で借りた装置に接続した際の処理手順のフローチャートである。
【００５６】
図２において、ピアトークン１０をステップＳ１でパーソナルコンピュータ１２のＵＳＢ２ポートに接続すると、パーソナルコンピュータ１２にあっては、ステップＳ１０１でＵＳＢ２ポートに対するデバイスの存在を検知し、ピアトークン１０のデバイスドライバを持たない場合には、ステップＳ１０２でデバイスドライバのインストールを行う。
【００５７】

即ち、パーソナルコンピュータ１２は図７のようなインストール要求画面を表示し、このインストール要求画面に対するユーザの操作でデバイスドライバのインストール要求をピアトークン１０に対し行い、これを受けてピアトークン１０は、ステップＳ２でデバイスドライバをパーソナルコンピュータ１２に転送し、デバイスドライバがインストールされて実行される。

【００５８】

次にパーソナルコンピュータ１２側にあっては、インストールされたデバイスドライバの実行で、ステップＳ１０３において認証ライブラリのインストールを行う。即ち、ピアトークン１０に対し認証ライブラリのインストール要求を行い、これを受けてピアトークン１０は、ステップＳ３で個人認証ライブラリの転送を行い、パーソナルコンピュータ１２における認証ライブラリのインストールと実行が行われる。

【００５９】

認証ライブラリが実行されると、ステップＳ１０４で認証画面が表示され、この認証画面に対しユーザはＩＤとパスワードを入力することで、ピアトークン１０に対し認証要求を行う。ピアトークン１０は、ステップＳ４でＰＨＳまたは無線ＬＡＮ経由で認証要求のための送受信を外部の認証サーバとの間で行い、認証サーバから認証結果を受け、ステップＳ５で認証結果をパーソナルコンピュータ１２に通知する。

【００６０】

パーソナルコンピュータ１２にあっては、ステップＳ１０５で認証を取得した場合には、ステップＳ１０６以降の処理に進む。認証が取得できなかった場合には、ステップＳ１１０の処理に進む。認証を取得した場合には、まずステップＳ１０６でピアトークン１０からのグループウェアのインストールを行う。

【００６１】

即ち、ピアトークン１０に対しグループウェアのインストール要求を行い、これを受けてピアトークン１０がステップＳ６でグループウェアの転送を行い、パーソナルコンピュータ１２にグループウェアがインストールされて実行される。

【００６２】

このようにしてパーソナルコンピュータ１２でグループウェアシステム環境が構築されると、ステップＳ１０７で共有ファイルの同期処理を行う。共有ファイルの同期処理は、グループウェアシステム環境に属している他のピア装置との間で共有データが同じになるように差分データの転送によるマージ処理を行う。

【００６３】

この共有ファイルの同期処理に伴う他のピア装置との間のやり取りのため、ピアトークン１０にあっては、ステップＳ７のようにＰＨＳまたは無線ＬＡＮによる転送処理を行う。

【００６４】

続いてステップＳ１０８で、グループウェアシステム環境の構築の下にピアツーピアによるグループウェアの運用が行われる。このグループウェアの運用における他のピア装置との間のデータのやり取りについても、ピアトークン１０はステップＳ８のように、ＰＨＳまたは無線ＬＡＮによる転送処理を行う。

【００６５】

ステップＳ１０９でグループウェアの終了が判別されると、ステップＳ１１０で終了通知をピアトークン１０に対し行った後、ステップＳ１１１でピアトークン１０の差込みによりインストールしたデバイスドライバ、個人認証ライブラリ及びグループウェアのアンインストールを自動的に行う。

【００６６】

またピアトークン１０にあっては、パーソナルコンピュータ１２からの終了通知を受けて、ステップＳ９でポート切り離しに伴う電源断に対する終了処理を行う。最終的に、パーソナルコンピュータ１２からピアトークン１０をステップＳ１０で抜き外し、これによってパーソナルコンピュータ１２にあっては、ステップＳ１１２でＵＳＢ２ポートのデバイス存在を認識してＵＳＢの処理を終了させる。

【００６７】
図１３は、図１２のグループウェアシステム環境を構築した際のパーソナルコンピュータ１２のステップＳ１０７における共有ファイル同期処理の詳細を示したフローチャートである。
【００６８】
図１３において、共有ファイル同期処理は、ステップＳ１０１でピアトークン１０に対し保存ファイルの更新情報を要求する。これを受けてピアトークン１０にあっては、ステップＳ１でファイル名と更新情報をパーソナルコンピュータ１２に応答する。
【００６９】
続いてステップＳ１０２で、パーソナルコンピュータ１２はグループウェアに属する他のピア装置に対し、ピアトークン１０に保存している共有ファイルの更新情報を要求する。これを受けてピアトークン１０は、ステップＳ２でＰＨＳまたは無線ＬＡＮで他のピア装置に対し共有ファイルの更新情報をアクセスして結果を通知する。
【００７０】
続いてステップＳ１０３で、ピアトークン１０と他のピア装置とで更新日の異なるファイルについて他のピア装置に対し差分データの転送を要求し、これを受けてピアトークン１０は、ステップＳ３でＰＨＳまたは無線ＬＡＮで他のピア装置にアクセスし、差分データを取得する。
【００７１】
このため、ステップＳ１０４でピアトークン１０に対し差分データのマージによるファイル更新を指示する。これを受けてピアトークン１０は、ステップＳ４で他のピア装置から受信した差分データを対応する保存ファイルとマージすることでファイル更新を行う。
【００７２】
なおステップＳ４の差分データのマージはピアトークン１０側で行わず、パーソナルコンピュータ１２側で行って、結果をピアトークン１０のメモリに保存するようにしてもよい。
【００７３】
このようにピアトークン１０をパーソナルコンピュータ１２に差し込んでグループウェアシステム環境を構築すると、最初にピアトークン１０に保存している共有データの同期処理が行われるため、その後のグループウェアシステム環境でのファイル利用は常に最新のファイルを対象に行うことができる。
【００７４】
図１４は、グループウェアシステム環境がピアトークン１０の差込みで構築されたパーソナルコンピュータ１２におけるファイルアクセスの処理手順のフローチャートである。
【００７５】
まずステップＳ１０１でパーソナルコンピュータ１２側でのファイルオープンが行われると、このファイルオープン要求がピアトークン１０に伝えられ、ステップＳ１で該当ファイルをフラッシュメモリ３４から読み出して転送し、ステップＳ１０２で必要とするファイル処理を行う。
【００７６】
またステップＳ１０３で、オープンしたファイルのクローズが判別されると、ステップＳ１０４でファイルをピアトークン１０に転送し、フラッシュメモリ３４に格納する。
【００７７】
ここで、ステップＳ１０２のファイル処理においてオープンしたファイルについて新たなデータを追加するなどしてファイル容量が増加する場合があり、ファイルオープン時にはメモリ容量が十分であったものが、ファイルクローズに伴うメモリ格納時にはフラッシュメモリ３４のメモリ容量が不足する場合がある。
【００７８】
そこでピアトークン１０にあっては、ステップＳ１０４からファイルクローズに伴うファイル転送を受けると、ステップＳ２でメモリ容量が不足するか否かチェックする。もしメ

モリ容量が不足した場合にはステップＳ３に進み、図５のデータ領域５５に格納しているファイルリスト５６の末尾のファイルｎに対応したファイルｎデータを取得し、ステップＳ４で他のピア装置例えば図２におけるパーソナルコンピュータ１２に対し近隣となるピア装置１４－４に転送して保存する。

【００７９】

続いてステップＳ５でファイルｎの実データを消去し、ここに他のピア装置の保存を示すリンク情報を格納する置き換えを行う。このようにファイルｎのデータを消去してそのリンク情報に置き換えることで、リンク情報の必要容量はごく少ないことから実データ域５７に空き容量を確保できる。

【００８０】

そしてステップＳ６で、ファイルクローズに伴い転送された使用済みファイルをファイルリスト５６の先頭位置に格納する。もちろんファイルリストの末尾のファイルを１つ、他のピア装置に転送して実データを消去してもなおメモリ容量が不足する場合には、再度、末尾のファイルを削除してメモリ空き容量を確保する処理を、メモリ容量の不足が解消するまで繰り返すことになる。

【００８１】

このため、ピアトークン１０のメモリ容量に制約があっても、実データを他のピア装置に保存してそのリンク情報をピアトークン１０に保存することで、ピアトークン１０におけるメモリ容量不足の影響を受けることなく、グループウェアシステム環境において使用している共有データの実質的な保存と利用が実現できる。

【００８２】

図１５は、本発明のピアトークンを携帯電話に接続して、交通機関改札のゲートシステムや自動販売機の制御処理を行う他の実施形態の説明図である。

【００８３】

図１５において、携帯電話６１は、図２の実施形態におけるパーソナルコンピュータ１２の場合と同様、ＵＳＢ２ポートに相当するデバイスポートを持っており、ピアトークン１０の差込みで電源供給と同時にデータ転送を可能とする。

【００８４】

ピアトークン１０のフラッシュメモリには、例えば図１６のメモリマップ６８に示すように、図５のメモリマップ４０の内容に加えて新たに、ゲート処理プログラム７０と自動販売機処理プログラム７２が格納されており、ピアトークン１０の携帯電話６１に対する差込みでインストールされてアプリケーションプログラムとして動作させることができる。

【００８５】

図１７は、ゲートシステム６４を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャートである。

【００８６】

図１７において、携帯電話６４にピアトークン１０を差し込んだ状態で交通機関の改札ゲートを通過しようとすると、ゲートの通信可能領域に入ったときにピアトークン１０はステップＳ１でゲートを認識し、ステップＳ２でゲート検知通知を携帯電話６１に送る。

【００８７】

これを受けて携帯電話６１側は、ステップＳ１０１でゲートイン要求をピアトークン１０に行い、ステップＳ３でＰＨＳまたは無線ＬＡＮによる無線送受信でゲートシステム６４に対しゲート要求を送り、応答結果を受信して携帯電話６４に返す。

【００８８】

このゲートイン要求に対し、ゲートシステム６４にあっては、改札ゲートを開くか、あるいはユーザの通過に対しロックを解除する。ゲートシステム６４からの応答情報には入場駅を示す入場情報が含まれていることから、ステップＳ１０２で入場情報を保持する。

【００８９】

このようにして改札ゲートに入った後は、ステップＳ４でピアトークン１０は再度、ゲート認識をチェックしており、利用者が到着駅のゲートから出ようとする際にゲート認識を

行って、ステップＳ５でゲート検知通知を携帯電話６１側に送る。これを受けて携帯電話６１は、ステップＳ１０３でゲートアウト要求をピアトークン１０のステップＳ６の無線送受信を介してゲートシステムに対し行い、このゲートアウト要求を受けてゲートシステム６４は、計算された料金データを応答する。

【００９０】

料金データを受けた携帯電話６１側にあっては、ステップＳ１０４で料金精算処理を行う。この料金精算処理は、予め保存しているプリペイド料金からの減額あるいは銀行口座から引き出している電子マネーの支払いなど、適宜の精算処理が行われる。

【００９１】

精算処理の結果はステップＳ７の無線送受信を通じてゲートシステム６４に通知され、精算確認応答を受けて、ステップＳ１０５で処理を終了し、一方、ゲートシステム６４にあっては精算確認に伴いゲート開あるいはゲートロック解除を行って、ユーザのゲート通過を可能とする。

【００９２】

図１８は、図１５の自動販売機６６を対象とした本発明のピアトークンと携帯電話における処理手順のフローチャートである。携帯電話６４に本発明のピアトークン１０を差し込んだ状態でユーザが自動販売機の前に立つと、ピアトークン１０はステップＳ１で自動販売機からの電波を受信して認識し、ステップＳ２で自動販売機の検知通知を携帯電話６１側に行う。

【００９３】

これに伴いユーザは、携帯電話６１を使用してステップＳ１０１で商品の購入要求を行う。例えば携帯電話６１の画面上に商品に選択画像が表示され、ユーザは購入したい商品を選択して実行要求することで、商品の購入要求がピアトークン１０のステップＳ３の無線送受信を通じて自動販売機に伝えられ、自動販売機より請求代金がピアトークン１０を介して携帯電話６１側に送られる。

【００９４】

そこで、ステップＳ１０２において購入代金の精算処理を行うと、プリペイド料金からの購入代金の残額あるいは銀行口座から引き落とした電子マネーの支払いがステップＳ４の無線送受信を通じて行われ、自動販売機から精算確認応答が得られると、ステップＳ１０３で終了処理を行う。

【００９５】

このような図１７における交通機関のゲート処理や図１８の自動販売機処理における代金精算結果はピアトークン１０のフラッシュメモリに保存され、ユーザが自分のパーソナルコンピュータの設置場所に戻ってピアトークンを差し込むと、ピアトークン１０に保存されている精算情報が自分のパーソナルコンピュータ側に転送されて自動的に編集され、ユーザの資産情報にマージするなどの処理を行わせることができる。

【００９６】

なお、グループウェアシステム環境における共有データの使い方として、自分のパーソナルコンピュータの実体データはサーバに保管しておき、サーバのファイル管理に使用しているネットワーク設定、各種アカウントなどのレジストリ情報をピアトークンに登録し、本発明のピアトークンを別のパーソナルコンピュータに挿入してレジストリ情報に基づくサーバからの共有ファイルの転送を行わせることで、本発明のピアトークンを別のパーソナルコンピュータに挿入すると同時に、自分が通常使用している作業環境を直ちに実現することができる。

【００９７】

また上記の実施形態は、ピアトークンに格納するアプリケーションとしてグループウェアプログラム、ゲート処理プログラム、自動販売機処理プログラムを例に取るものであったが、本発明はこれに限定されず、無線回線を利用して他の装置との間でデータのやり取りを行う適宜のアプリケーションをピアトークンに格納してパーソナルコンピュータやＰＤＡ、更には携帯電話に差し込むことで、差込み先の装置にアプリケーションプログラム環

境を構築して利用することができる。
【００９８】
また本発明は、その目的と利点を損なうことのない適宜の変形を含み、更に実施形態に示した数値による限定は受けない。
【００９９】
ここで本発明の特徴をまとめると次の付記のようになる。
（付記）
（付記１）
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、
外部装置に対し無線回線により情報を送受する第１無線通信部と、
外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、
デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリと、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせ、インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させ、前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部と、
を備えたことを特徴とする情報処理デバイス。（１）
【０１００】
（付記２）
付記１記載の情報処理デバイスに於いて、デバイス本体は持ち運び自在なキー型であることを特徴とする情報処理デバイス。
【０１０１】
（付記３）
付記１記載の情報処理デバイスに於いて、前記デバイスポートはＵＳＢ２ポートであり、前記ポートドライバはＵＳＢ２ドライバであることを特徴とする情報処理デバイス。
【０１０２】
（付記４）
付記１記載の情報処理デバイスに於いて、前記第１無線通信部はＰＨＳ無線回線を使用するＰＨＳ通信部であり、前記第２無線通信部は無線ＬＡＮを使用する無線ＬＡＮ通信部であることを特徴とする情報処理デバイス。
【０１０３】
（付記５）
付記１記載の情報処理デバイスに於いて、前記アプリケーションプログラムは複数の情報処理装置でデータを共有するピアツーピア型のグループウェア処理プログラムであることを特徴とする情報処理デバイス。（２）
【０１０４】
（付記６）
付記５記載の情報処理デバイスに於いて、前記アプリケーションプログラムがグループウェア処理プログラムの場合、前記個人認証ライブラリは前記第１又は第２無線通信部により外部の認証サーバに接続して認証処理を実行させることを特徴とする情報処理デバイス。
【０１０５】

（付記７）
付記１記載の情報処理デバイスに於いて、前記不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すディレクトリ情報を登録し、前記アプリケーションプログラムは、他の情報処理装置の差込み時に、前記レジストリ情報により前記サーバからファイルを取得して前記自己の情報処理装置の作業環境を構築することを特徴とする情報処理デバイス。（３）
【０１０６】
（付記８）
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスの情報処理方法に於いて、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる個人認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を備えたことを特徴とする情報処理方法。（４）
【０１０７】
（付記９）
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスのコンピュータに、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を実行させることを特徴とするプログラム。（５）
【０１０８】
【発明の効果】
以上説明してきたように本発明によれば、キー型に形成された小型の情報処理デバイスを例えば出張先で使用することのできるパーソナルコンピュータのデバイスポートに差し込

むだけで、個人認証画面が自動的に立ち上がり、個人認証を済ませた後はグループウェアなどのアプリケーション画面が立ち上がり、外部との送受信を含む作業をすぐ始めることができる。

【０１０９】

また外部との通信に使用する無線通信機能がＰＨＳと無線ＬＡＮにより二重化されており、使用場所の無線環境に対応して有効な側に自動切替して外部に確実にアクセスすることができる。

【０１１０】

更に、情報処理デバイスの差込みによるアプリケーションの実行で使用されたデータは全てデバイス側の不揮発メモリに保存され、また情報処理デバイスを抜いて処理を終えると、パーソナルコンピュータなどの差込み側の装置にはインストールしたプログラムやドライバは全てアンインストールされて残ることがなく、差込み先の装置の環境を全く侵すことなく、本発明の情報処理デバイスの差込みによるアプリケーション環境の利用が実現できる。

【図面の簡単な説明】

【図１】本発明の原理説明図

【図２】本発明が適用されたシステム環境の説明図

【図３】本発明によるキー型ピアトークンの外観の説明図

【図４】本発明によるピアトークンのハードウェア構成のブロック図

【図５】図４の不揮発メモリの格納内容となるメモリマップの説明図

【図６】本発明のピアトークンを使用先となるパーソナルコンピュータに接続した起動時の説明図

【図７】ピアトークンの接続による使用先となるパーソナルコンピュータのインストール要求画面の説明図

【図８】図６に続いて使用先となるパーソナルコンピュータにデバイスドライバがインストールされた説明図

【図９】図８に続いて使用先となるパーソナルコンピュータに個人認証ライブラリがインストールされた説明図

【図１０】図９に続いて使用先となるパーソナルコンピュータにグループウェアがインストールされた説明図

【図１１】使用先となるパーソナルコンピュータのデバイスポートから本発明のピアトークンを外した際の説明図

【図１２】本発明のピアトークンを使用先となるパーソナルコンピュータに接続した際の処理手順のフローチャート

【図１３】共有ファイル同期処理における本発明のピアトークンと使用先となるパーソナルコンピュータの処理手順のフローチャート

【図１４】ファイルアクセスにおける本発明のピアトークンと使用先となるパーソナルコンピュータの処理手順のフローチャート

【図１５】本発明のピアトークンを携帯電話に接続して交通機関改札のゲートシステムや自動販売機の制御処理を行う実施形態の説明図

【図１６】図６のピアトークンにおける不揮発メモリのメモリマップ説明図

【図１７】ゲートシステムを対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート

【図１８】自動販売機を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート

【符号の説明】

１０：ピアトークン（情報処理デバイス）

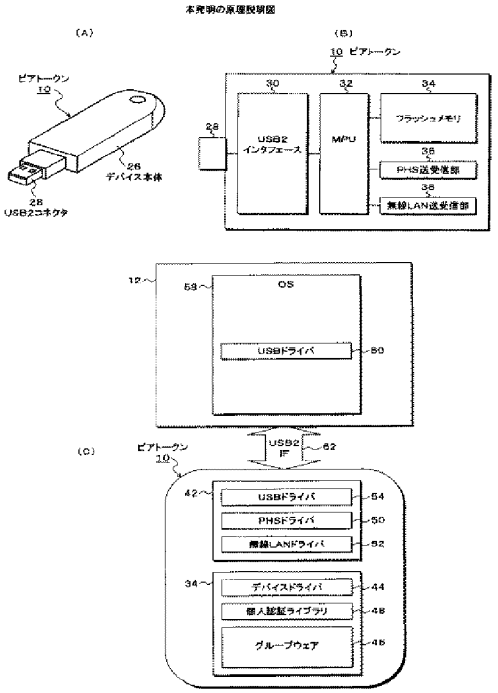
１２：パーソナルコンピュータ

１４－１～１４－４：ピア装置

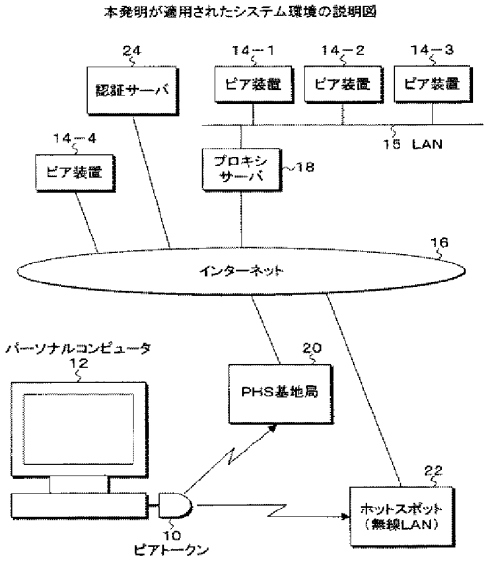
１５：ＬＡＮ

１６：インターネット
１８：プロキシサーバ
２０：ＰＨＳ基地局
２２：ホットスポット（無線ＬＡＮ）
２４：認証サーバ
２６：デバイス本体
２８：ＵＳＢ２コネクタ
３０，６２：ＵＳＢ２インタフェース
３２：ＭＰＵ（プロセッサ）
３４：フラッシュメモリ（不揮発メモリ）
３６：ＰＨＳ送受信部
３８：無線ＬＡＮ送受信部
４０，６８：メモリマップ
４２：デバイス処理プログラム（トークンＯＳ）
４４：デバイスドライバ
４５：インストール要求画面
４６：グループウェア
４８：個人認証ライブラリ
５０：ＰＨＳドライバ
５２：無線ＬＡＮドライバ
５４，６０：ＵＳＢドライバ
５５：データ領域
５６：ファイルリスト
５７：実データ域
５８：使用先となるパーソナルコンピュータＯＳ
６１：携帯電話
６４：ゲートシステム
６６：自動販売機
７０：ゲート処理プログラム
７２：自動販売機処理プログラム

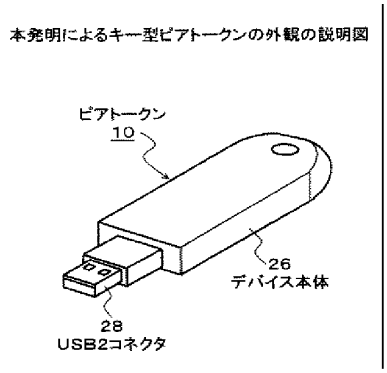
【図1】


本発明の原理説明図
(A)
(B)
10 ピアトークン
ピアトークン
10
26
デバイス本体
28
USB2コネクタ
30
32
34
28
USB2
インタフェース
MPU
フラッシュメモリ
36
PHS送受信部
38
無線LAN送受信部
12
OS
58
USBドライバ
50
(C)
ピアトークン
10
USB2
IF
62
42
USBドライバ
54
PHSドライバ
50
無線LANドライバ
52
34
デバイスドライバ
44
個人認証ライブラリ
48
グループウェア
46

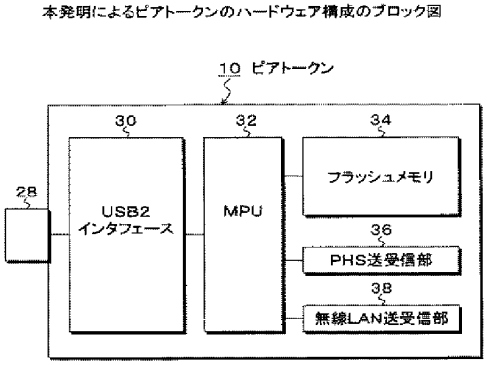
【図2】


本発明が適用されたシステム環境の説明図
24
認証サーバ
14-1
ピア装置
14-2
ピア装置
14-3
ピア装置
14-4
ピア装置
15 LAN
プロキシ
サーバ
18
16
インターネット
パーソナルコンピュータ
12
20
PHS基地局
22
ホットスポット
（無線LAN）
10
ピアトークン

【図3】

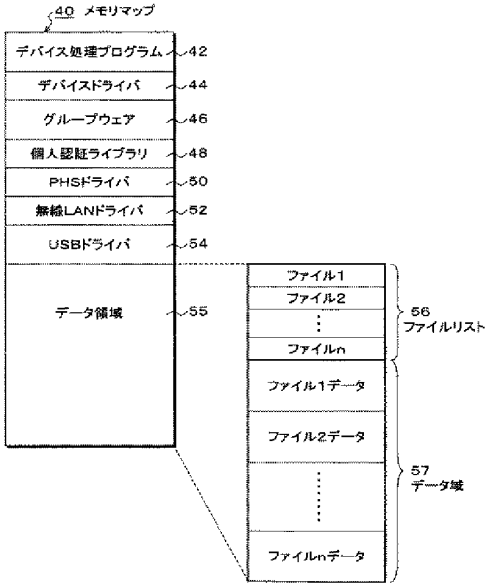

本発明によるキー型ピアトークンの外観の説明図
ピアトークン
10
26
デバイス本体
28
USB2コネクタ

【図4】


本発明によるピアトークンのハードウェア構成のブロック図
10 ピアトークン
30
32
34
28
USB2
インタフェース
MPU
フラッシュメモリ
36
PHS送受信部
38
無線LAN送受信部

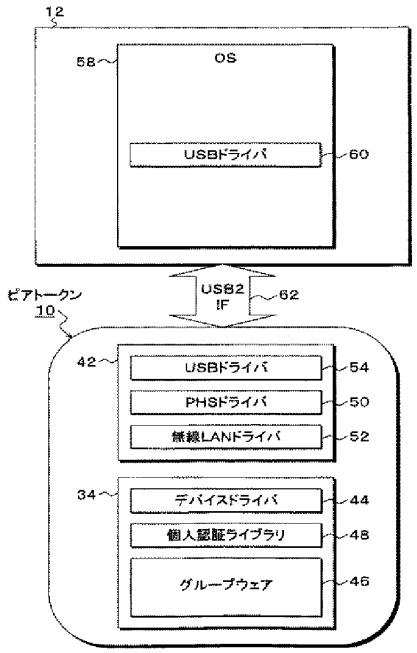
【図5】

図4の不揮発メモリの格納内容となるメモリマップの説明図

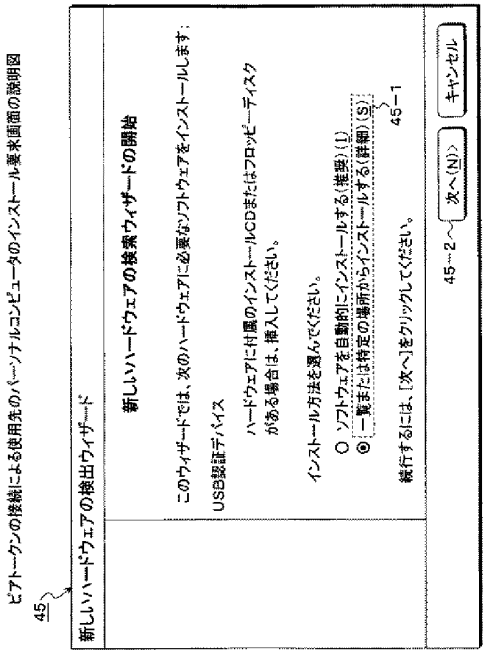


【図6】

本発明のピアトークンを使用先のパーソナルコンピュータに接続した起動時の説明図

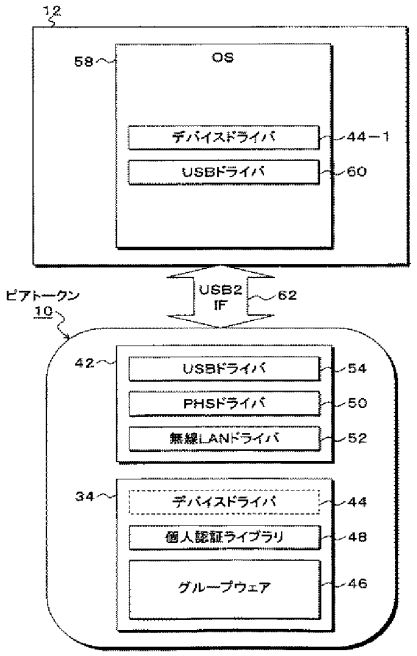


【図7】



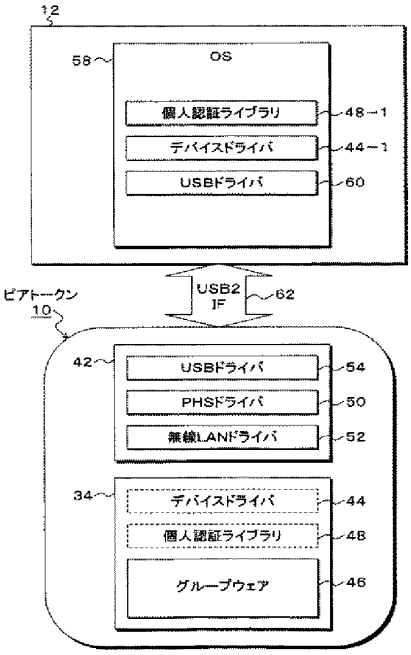
【図8】

図6に続いて使用先のパーソナルコンピュータにデバイスドライバがインストールされた説明図



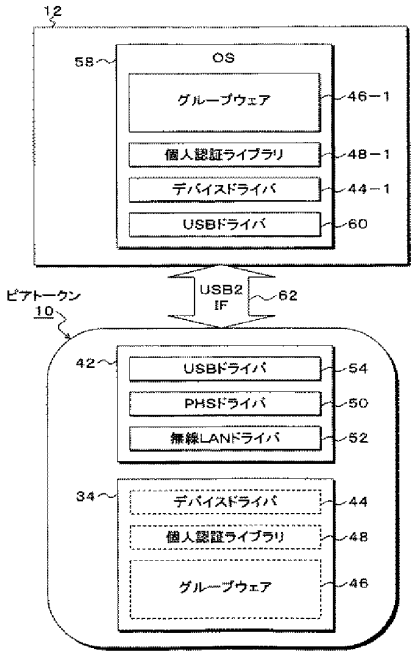
【図9】

図8に続いて使用先のパーソナルコンピュータに個人認証ライブラリがインストールされた説明図



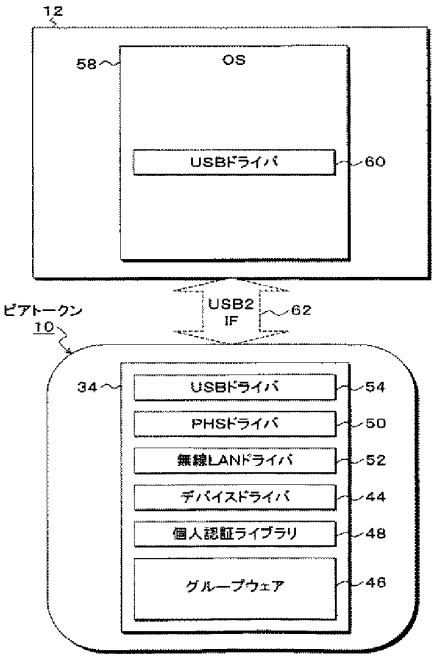
【図10】

図9に続いて使用先のパーソナルコンピュータにグループウェアがインストールされた説明図



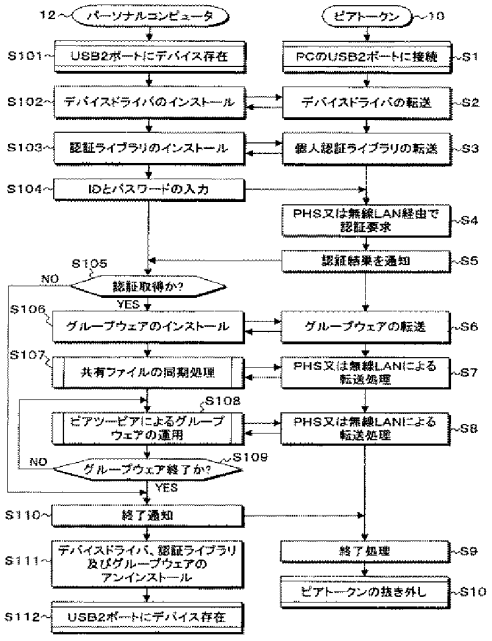
【図11】

使用先のパーソナルコンピュータのデバイスポートから本発明のピアトークンを外した際の説明図

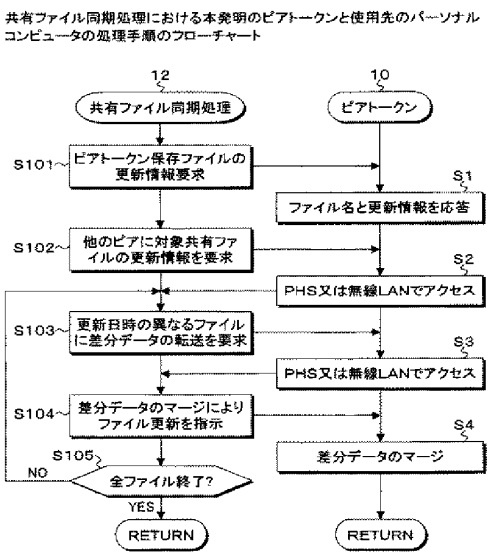


【図12】

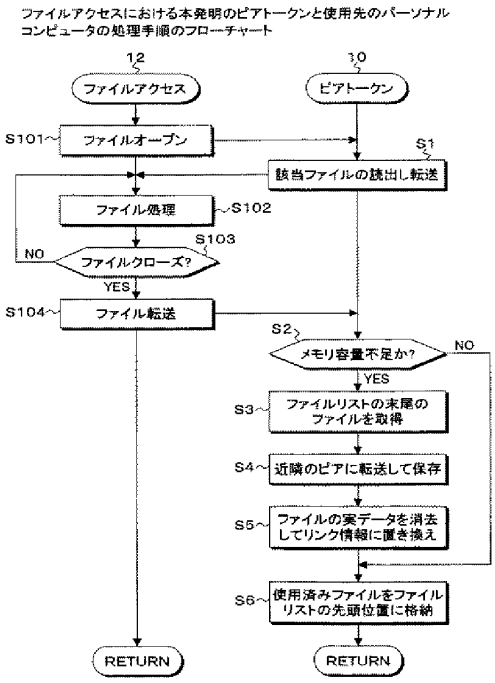
本発明のピアトークンを使用先のパーソナルコンピュータに接続した際の処理手順のフローチャート



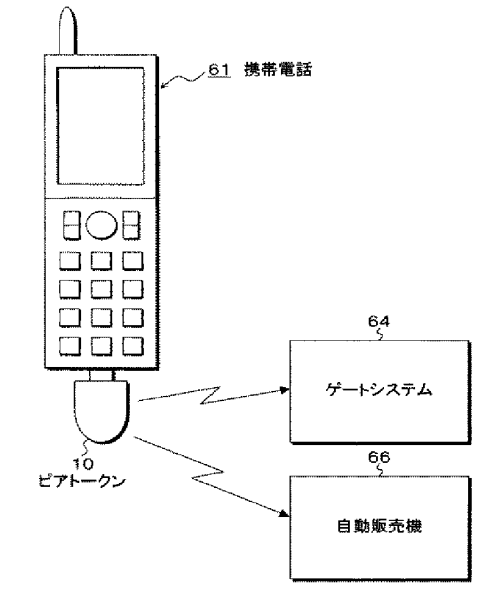
【図13】



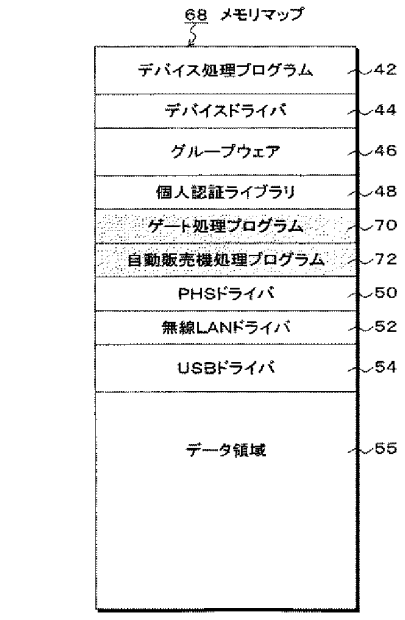
【図14】



【図15】

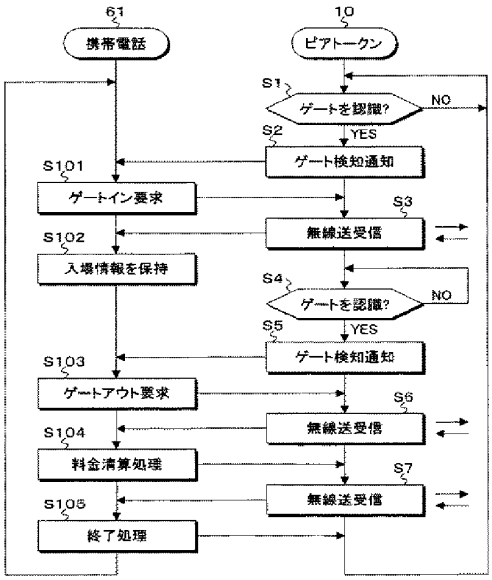


【図16】



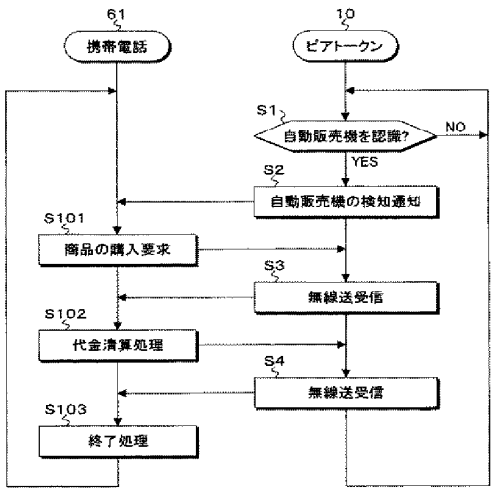
【図17】

ゲートシステムを対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート



【図18】

自動販売機を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート



(51)Int.Cl.[7]	FI	テーマコード（参考）
	Ｇ０６Ｆ　9/06　６６０Ｅ	

Ｆターム(参考) 5B014 FA14
5B076 AB20 BA05 BA10 BB12 BB18 FB01
5B085 AA04 AE02 AE12 AE23 BE01 BE04 BG01 BG02 BG07

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60, G07F 7/02

A1

(11) International Publication Number: **WO 99/52051**

(43) International Publication Date: 14 October 1999 (14.10.99)

(21) International Application Number: PCT/GB99/00575

(22) International Filing Date: 25 February 1999 (25.02.99)

(30) Priority Data:
09/054,844 3 April 1998 (03.04.98) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MC only)*: IBM UNITED KINGDOM LIMITED [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

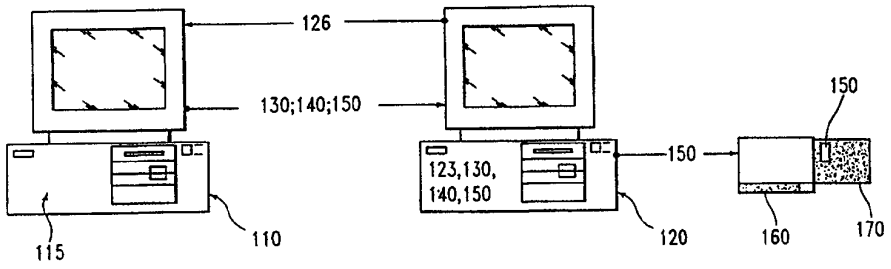
(72) Inventors: PALMER, Charles, Campbell; 293 Waccabuc Road, Goldens Bridge, New York, NY 10526 (US). PALMER, Elaine, Rivette; 293 Waccabuc Road, Goldens Bridge, New York, NY 10526 (US). SMITH, Sean, William; 19 Bridge Street, Cornwall, New York, NY 12518 (US).

(74) Agent: WILLIAMS, Julian, David; IBM United Kingdom Limited, Intellectual Property Dept., Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(81) Designated States: CN, HU, JP, KR, PL, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: AUTHENTICATED ELECTRONIC COUPON ISSUING AND REDEMPTION



(57) Abstract

An online coupon issuing and redemption system and method receives requests for coupons from consumers, presents advertisements and issues coupons to consumers electronically. The system presents advertisements before issuing the coupons, such that an issuer may be assured its targeted consumer is receiving its advertisements. The coupons are issued on a smart card, thereby eliminating a need for paper coupons. The coupons are digitally signed in order to prevent fraud. In order to prevent further fraudulent tampering of coupons, the redemption station includes a tamper–protected coprocessor for performing operations on the coupons. The system further includes capability for the redemption station to link to an issuing station for electronic reimbursements.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

AUTHENTICATED ELECTRONIC COUPON ISSUING AND REDEMPTION

The present invention relates to an electronic advertisement and coupon issuance and redemption.

Retailers and manufacturers often sponsor incentive programs for persuading consumers to buy their products. These incentives include discount coupons distributed to consumers whereby a consumer may redeem the coupon when purchasing an associated item. Such coupons are usually distributed in paper forms.

The problems associated with paper coupons today are that the retailer and manufacturers who advertise cannot assure that consumers who use paper coupons have actually read the product advertisements which accompany the coupons. The advertisers do not have a way of knowing who is viewing their advertisements and cannot dynamically adjust the advertisement to fit the viewer's tastes and interests.

In addition, many cases of fraud related to paper coupons are occurring today. For example, paper coupons are easily counterfeited. Some consumers commit fraud by redeeming coupons for merchandise they have not purchased. Some retailers also commit fraud by redeeming coupons for merchandise which consumers have not purchased.

Manufacturers must rely on the cashiers and computer systems at retail establishments to assure that consumers who redeem coupons have actually bought the targeted product and that the coupons redeemed were not expired at the time of redemption. Retailers often rely on their cashiers to enforce coupon redemption rules. Other retailers rely on computerized systems to compare coupon bar codes to the consumer's purchases.

U.S. patent number 4880964 by Donahue describes paper coupons with bar codes printed on them, and thus does not solve the deficiencies of paper coupons described above. U.S. patent number 5710866 by Christensen et al. describes electronically generated coupons but requires a database of customers and spent coupons which is costly to maintain. It also requires online connection to the database at redemption time to determine if the coupon is valid.

In accordance with the present invention, there is now provided a coupon issuing system for electronically presenting advertisements and generating coupons, said system comprising: at least one issuing station for generating and transmitting electronic advertisements and electronic coupons according to predetermined criteria; at least one customer station

to transmit from a user to the issuing station a request for an electronic coupon, for receiving electronic advertisements and electronic coupons from the issuing station, and for presenting the advertisement to the user for interaction with the user; at least one smart card for holding information including said electronic coupons; at least one smart card reader/writer for communicating information held in said at least one smart card to said at least one customer station; and at least one software program to monitor a status of the interaction of the user with the advertisement; whereby when said at least one software program detects a predefined status, said at least one software program transfers said electronic coupons to said smart card via said smart card reader/writer.

Viewing the present invention from another aspect, there is now provided a system for redeeming electronic coupons comprising: at least one redemption station; and at least one smart card reader/writer linked to said redemption station; whereby said redemption station selects and updates via said at least one smart card reader/writer, coupons stored in a smart card, deleting expired coupons and also those matching purchased items.

Viewing the present invention from yet another aspect, there is now provided a method for advertising and issuing at least one coupon electronically, said method comprising: receiving a request for said electronic coupon from a consumer; generating at least one electronic advertisement and said electronic coupon; transmitting said electronic advertisement and said electronic coupon to a consumer's station for presentation to said consumer; monitoring said consumer's interaction with said advertisement; and transferring said electronic coupon to a smart card, if said consumer's interaction with said advertisement meets a predefined status.

In a preferred embodiment of the present invention there is provided an online coupon issuing and redemption system. The issuing system includes an issuing station. The issuing station is generally comprised of a computer located usually at a manufacturer's site. The issuing station typically generates advertisements and coupons electronically. The issuing system also includes a consumer station, usually a computer and a smart card reader/writer generally located at the consumer site. The smart card reader/writer may be linked to the consumer computer either directly or via a LAN or other network connections.

The issuing station and consumer station are linked via a communications network. When a consumer makes requests via the consumer station for coupons, the issuing station transmits the advertisement and coupons it generated to the consumer station. The issuing station also

has a capability of digitally signing the coupons. Digital signatures insure the authenticity of the coupons as well as that of the issuer and the issuing station. Also included in the transmission is a program having a capability to run on the consumer station. The program is responsible for making sure that the consumer absorbs the entire advertisement and transferring the coupons to a smart card via the smart card reader/writer linked to the consumer station.

This assures the advertisers that a consumer actually perceives the advertisement for a product before receiving discount coupons.

The redemption system generally comprises a redemption station, typically a computer, and a smart card reader/writer linked to the redemption computer. The redemption system is typically located at a purchasing site. When a consumer is ready to make a purchase, the consumer inserts the smart card having electronic coupons stored in it into the smart card reader/writer linked to the redemption station. The redemption system reads the coupons via the smart card reader/writer and matches the purchased items with coupons. The matched coupons are extracted from the smart card, so that they may not be used again. At the same time, the redemption system deletes any expired coupons stored in the smart card.

The redemption system also may include a tamper-protected secure coprocessor. In order to protect a manufacturer from fraudulent merchants and customers, operations which assess the validity of coupons, operations which update, collect, store, or delete coupons may take place inside a tamper-protected hardware boundary. The hardware boundary is part of typical tamper-protected secure coprocessors and smart cards.

This provides a tamper-protected access to the coupons stored in the smart cards.

Embodiments of the present invention may include a database of coupons stored in the issuing station. The database may include a list of coupons issued or already spent. When a consumer is ready to redeem the coupons, the redemption station links to the database and validates the coupons stored in the consumer's smart card by comparing the smart card coupons with a list of coupons in the database. Only the valid coupons matching the list in the database may be actually redeemed.

In embodiments of the present invention there may be provided a communications link between a redemption station and an issuing station. Such a link is established when a merchant wants reimbursements from the manufacturer for the coupons the merchant redeemed to the consumers.

Typically the redemption computer sends electronic coupons which have been digitally signed to the issuing computer. The issuing computer validates the electronic signatures on the coupon. If the signatures are valid, the manufacturer reimburses the merchants for the valid coupons. This provides a mechanism for the manufacturer to electronically reimburse the merchants.

Preferred embodiments of the present invention will now be described by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is an exemplary diagram illustrating a physical architecture of an issuing system embodying the present invention;

Figure 2 is a flow diagram illustrating one possible logic flow of issuing software running on the issuing computer embodying the present invention;

Figure 3 is a flow diagram illustrating one possible logic flow of advertisement viewing software running on the viewing computer embodying the present invention;

Figure 4 is a flow diagram illustrating one possible logic flow for interaction between advertisement viewing software and issuing software;

Figure 5 is an illustrative example showing a physical layout of a redemption system architecture embodying the present invention;

Figures 6 and 7 are a flow diagram illustrating one possible logic flow in the redemption system during a typical point of sale;

Figure 8 is a flow diagram illustrating a possible logic flow in a typical daily coupon close-out;

Figure 9 is an illustrative example showing a physical layout of a software-based redemption system embodying the present invention.

Figure 1 is an exemplary diagram illustrating a physical architecture of an issuing system embodying the present invention. An authenticated electronic coupon issuing system shown in Figure 1 includes an issuing station, typically a computer 110 running issuing software 115; a viewing station, typically an advertisement viewing computer 120 running advertisement viewing software 123 which sends requests for coupons 125 to an issuing computer 110; an advertisement viewing computer 120 running advertisement applet software 130; an electronic advertisement 140; an

electronic coupon which is digitally signed 150; a dispensing smart card reader/writer 160; a customer's smart card 170 holding an electronic coupon 150. A typical smart card may be a chip card having an integrated circuit that is resistant to physical tampering. An issuing station typically comprises a computer at a manufacturer or clearing house site. Likewise, a viewing station typically comprises of a computer at a customer site. A customer is typically a consumer who receives coupons electronically and makes purchases using the coupons.

A dispensing smart card reader/writer 160 is attached to an advertisement viewing computer 120 and is accessible by advertisement applet software 130.

Issuing software 115, advertisement viewing software 123, and advertisement applet software 130 are typically purchased from software vendors. An electronic advertisement 140 is supplied by an advertisement content vendor. A customer's smart card 170 may be purchased from a smart card vendor. Likewise, a customer's smart card reader/writer 160 may be supplied by a smart card reader/writer vendor. An issuing computer 110 and an advertisement viewing computer 120 may be obtained from computer hardware vendors. An electronic coupon 150 is generated by issuing software 115. A request for coupons 125 is generated by advertisement viewing software 123.

Figure 2 is a flow diagram illustrating one possible logic flow of issuing software running on the issuing computer of the present invention. Initially in step 210, the issuing software awaits a request from an advertisement viewing computer. A request includes information about the customer, such as his interests (e.g., propensity for playing tennis), and demographics (e.g., a senior citizen). In step 220, the issuing software retrieves a customer's interest profile and demographics from a request. In step 230, the issuing software selects an electronic advertisement which matches a customer's interest profile and demographics. For example, if a customer is a senior citizen, the issuing software selects an electronic advertisement targeted at senior citizens, not one targeted at teenagers. In step 240, the issuing software generates an electronic coupon which is digitally signed.

Digital signatures are generally created by piping a sender's private key and the contents of the message into an algorithm. The output of the algorithm is the digital signature. The recipient can verify the digital signature by using the sender's public key and the message. The digital signature is secure because it would be virtually impossible for another computer to produce the identical digital signature. Each user has the responsibility of protecting the private key.

In step 250, the issuing software transmits an electronic advertisement, advertisement applet software, and an electronic coupon to an advertisement viewing computer. The issuing software then waits for another request from the advertisement viewing software.

Figure 3 is a flow diagram illustrating one possible logic flow of advertisement viewing software running on the viewing computer of the present invention. In step 310, the advertisement viewing software awaits a request for a coupon from a customer. In step 315, the viewing software obtains information about a customer, such as his interests and demographics. The viewing software may obtain the information directly from a customer through a dialogue, or from a customer's smart card, or from a file on the viewing computer. In step 320, the viewing software includes a customer's interest profile and demographics with a request for a coupon. In step 325, the viewing software transmits a request for a coupon to an issuing computer. In step 330, the viewing software awaits a response from an issuing computer. If there is no response, the viewing software times out, in step 335, displays an error message and, in step 310, awaits for another request from a customer. If there is a response from an issuing computer, the viewing software receives advertisement applet software, an electronic advertisement, and an electronic coupon as shown in step 340. In step 350, the viewing software then runs advertisement applet software. The software determines, in step 360, if the customer viewed an entire advertisement. In step 370, if the applet software times out or if a customer exited the software prematurely, the viewing software terminates the session and returns to wait for another request from a customer in step 310. In step 380, if the applet determines that a customer did view the entire advertisement, the applet software transmits an electronic coupon which is digitally signed to a customer's smart card via a dispensing smart card reader/writer.

An example of viewing software may include a World Wide Web (Web) page having a uniform resource locator (URL) address which a consumer may access via a Web browser. The URL address would be located in the web server linked to an issuing station. The Web page may have a number of parameter fields as input fields which the consumer is required to fill. The Web page with the parameters may then be transmitted to the web server at the issuing station. The web server together with issuing software may then use the parameters to generate electronic advertisements and coupons, transmitting them with an applet software to the viewing software. The viewing software typically launches the applet software. The launched applet software displays the advertisements on the consumer station, controlling the station's interaction with the consumer. The applet software may also be responsible for transferring the coupons to the consumer's smart card. Furthermore, the applet software may provide

interactivity, for example, requiring that the consumer answer questions about the product or advertisement, to assure that the consumer is truly absorbing the advertising information.

Figure 4 is a flow diagram illustrating one possible logic flow for interaction between advertisement viewing software and issuing software. In step 420, an advertisement viewing computer requests an electronic coupon from an issuing computer. In step 430, an issuing computer transmits advertisement applet software, an electronic advertisement, and an electronic coupon which is digitally signed to an advertisement viewing computer. In step 440, an advertisement viewing computer runs applet software. The applet software displays an electronic advertisement. In step 450, the applet software determines how to proceed based on whether or not a customer viewed an entire advertisement. In step 460, if a customer does not view an entire electronic advertisement, the advertisement applet software terminates the session and awaits another request, step 410. If, however, a customer views an entire electronic advertisement, in step 470, the applet software rewards the customer by transmitting an electronic coupon which is digitally signed to a customer's smart card. The smart card is typically inserted into a dispensing smart card reader/writer. Furthermore, the advertisement applet software may be interactive, requiring that a customer answer questions about a product or advertisement, to assure that a customer is truly absorbing the advertising information. Secure protocols, tamper-protected hardware, or record keeping databases typical in electronic money systems may be employed to prevent consumers and retailers from double spending or duplicating the electronic coupons. A suitable example for such secure protocols are described in detail in M. Bellare et al., "iKP - A Family of Secure Electronic Payment Protocols", July 12, 1995, available from IBM.

Electronic coupons are not printed, therefore they cannot be printed over and over again, or photocopied. The number of electronic coupons a smart card may hold may be limited.

Figure 5 is an illustrative example showing a physical layout of a redemption system architecture embodying the present invention. An authenticated coupon redemption system as shown in Figure 5 comprises a redemption computer 510, a tamper-protected secure coprocessor 520, a redemption smart card reader/writer 530, a customer's smart card storing a digitally signed electronic coupon 150, and an issuing station. An issuing station is typically comprised of a computer 110 and is generally resident at a manufacturer or at a clearing house that performs the duties for a manufacturer or a group of manufacturers. A redemption smart card reader/writer 530 is typically attached to a redemption computer 510. A

tamper-protected secure coprocessor 520 is connected to a redemption computer 510 either directly or via a communications network. A redemption computer 510 may also be connected to an issuing computer 110, typically via phone line 570.

Figures 6 and 7 are a flow diagram illustrating a possible logic flow in the redemption system during a typical point of sale. In step 610, a consumer inserts the smart card 170 Figure 1 into a redemption smart card reader/writer 530 Figure 5. The smart card includes electronic coupons which have been digitally signed 150 Figure 1. In step 620, the smart card sends a list of all coupons stored in it to a redemption computer 510 Figure 5. In step 630, a redemption computer forwards the list of coupons and optionally a list of items purchased to a tamper-protected secure coprocessor 520 Figure 5. In step 640, the tamper-protected secure coprocessor 520 Figure 5 examines the list of all coupons, and assembles a list of those which have expired. In step 650, the tamper-protected secure coprocessor 520 Figure 5 requests a redemption computer to send a command to a smart card to delete expired coupons. Next, in step 660, the tamper-protected secure coprocessor searches for non-expired coupons that match actual items purchased. If there are no matching items, in step 670, the tamper-protected secure coprocessor tells the redemption computer that no items matched the coupon list. If there are matching items, in step 680, the tamper-protected secure coprocessor assembles a list of matching items and valid coupons. In step 690, the coprocessor requests the redemption computer to send a command to the smart card to extract valid matching coupons. In step 695, the smart card sends the valid matching coupons to the tamper-protected secure coprocessor.

In order to protect a manufacturer from fraudulent merchants and customers, operations which assess the validity of coupons, operations which update, collect, store, or delete coupons take place inside a tamper-protected hardware boundary 655. The hardware boundary is part of typical tamper-protected secure coprocessors and smart cards. A typical tamper-protected secure coprocessor may be a tamper-protected computing device having a microprocessor and memory in a tamper-protected enclosure, such as the IBM 4758.

Figure 8 is a flow diagram illustrating a possible logic flow during a typical daily coupon close-out. In step 710, a redemption computer 510 Figure 5 connects to the issuing computer 110 Figure 5 or clearing house computer. Such connection would generally occur at the end of the day, or at some appropriate period of time. In step 720, the redemption computer 510 Figure 5 sends electronic coupons which have been digitally signed 150 Figure 5 to the issuing computer 110 Figure 5. In step 730, the issuing

computer validates the electronic signatures on the coupons. In step 740, the clearing house reimburses the merchant for the valid coupons.

Figure 9 is an illustrative example showing a physical layout of a software-based redemption system embodying the present invention. The embodiment shown in Figure 9 replaces the tamper-protected secure coprocessor 520 Figure 5 in the redemption computer 510 Figure 5 with a database of coupons 810 in the issuing computer 110 Figure 5. The database includes either a list of already spent coupons (so as to reject them if they are presented a second time) or a list of unspent coupons, from which it deletes coupons as they are presented for redemption. When a merchant connects to the issuing computer 110 to redeem the coupons, the issuing computer 110 searches the database 810 to determine if the coupons are valid. Only the valid coupons found in the database 810 may then be redeemed.

While the invention has been particularly shown and described with respect to a preferred embodiment thereof, it will be understood by those skilled in the art that the foregoing and other changes in form and details may be made therein without departing from the scope of the invention.

Claims

1. A coupon issuing system for electronically presenting advertisements and generating coupons, said system comprising:

at least one issuing station for generating and transmitting electronic advertisements and electronic coupons according to predetermined criteria;

at least one customer station to transmit from a user to the issuing station a request for an electronic coupon, for receiving electronic advertisements and electronic coupons from the issuing station, and for presenting the advertisement to the user for interaction with the user;

at least one smart card for holding information including said electronic coupons;

at least one smart card reader/writer for communicating information held in said at least one smart card to said at least one customer station; and

at least one software program to monitor a status of the interaction of the user with the advertisement;

whereby when said at least one software program detects a predefined status, said at least one software program transfers said electronic coupons to said smart card via said smart card reader/writer.

2. A system as claimed in claim 1, wherein said system further includes a user interface program for displaying information including request forms and the advertisements, whereby the advertisements are presented visually to the user via the customer station.

3. A system as claimed in claim 2, wherein said user interface program comprises a Web browser running on the customer station.

4. A system as claimed in claim 3, wherein said at least one software program includes a platform independent program downloadable dynamically from said issuing station, said at least one software program further controlling displays in conjunction with said Web browser.

5. A system as claimed in claim 1, wherein said issuing station digitally signs said electronic coupons before downloading said electronic coupons to said customer station.

6. A system as claimed in claim 1, wherein said advertisements are updated over predefined intervals.

7. A system for redeeming electronic coupons comprising:

at least one redemption station; and

at least one smart card reader/writer linked to said redemption station;

whereby said redemption station selects and updates via said at least one smart card reader/writer, coupons stored in a smart card, deleting expired coupons and also those matching purchased items.

8. A system as claimed in claim 7, wherein said system further includes at least one tamper-protected secure coprocessor, whereby operations which assess the validity of coupons including operations which update, collect, store, or delete coupons take place inside said tamper-protected secure coprocessor thereby preventing fraudulent tampering of said coupons.

9. A system as claimed in claim 7, wherein said system further includes at least one issuing station linked to said redemption station, whereby coupons collected by said redemption station are reimbursed by said at least one issuing station.

10. A system as claimed in claim 9, wherein said at least one issuing station includes a database for storing lists of coupons, whereby validation of redeemed coupons are performed by matching said redeemed coupons with said lists of coupons.

11. A method for advertising and issuing at least one coupon electronically, said method comprising:

receiving a request for said electronic coupon from a consumer;

generating at least one electronic advertisement and said electronic coupon;

transmitting said electronic advertisement and said electronic coupon to a consumer's station for presentation to said consumer;

monitoring said consumer's interaction with said advertisement; and

transferring said electronic coupon to a smart card, if said consumer's interaction with said advertisement meets a predefined status.

12. A method as claimed in claim 11, wherein said method further includes the step of retrieving an interest and demographic profile for said consumer before the step of generating.

13. A method as claimed in claim 11, wherein said step of generating includes digitally signing said electronic coupon.

14. A method as claimed in claim 11, wherein said method further includes the steps of:

reading a list of said electronic coupon stored in said smart card;

deleting from said smart card said electronic coupon which have expired;

matching valid said electronic coupon with purchased items; and

extracting valid matching said electronic coupon,

whereby said consumer's electronic coupon is redeemed at a purchasing location when said consumer purchases items associated with said electronic coupon stored in said smart card.

15. The method according to claim 14, wherein said method further includes the steps of:

establishing a connection to an issuing station;

sending said electronic coupon to said issuing station;

validating said electronic coupon; and

reimbursing a merchant for valid said electronic coupon,

whereby said issuing station periodically reimburses merchants collecting said electronic coupon.

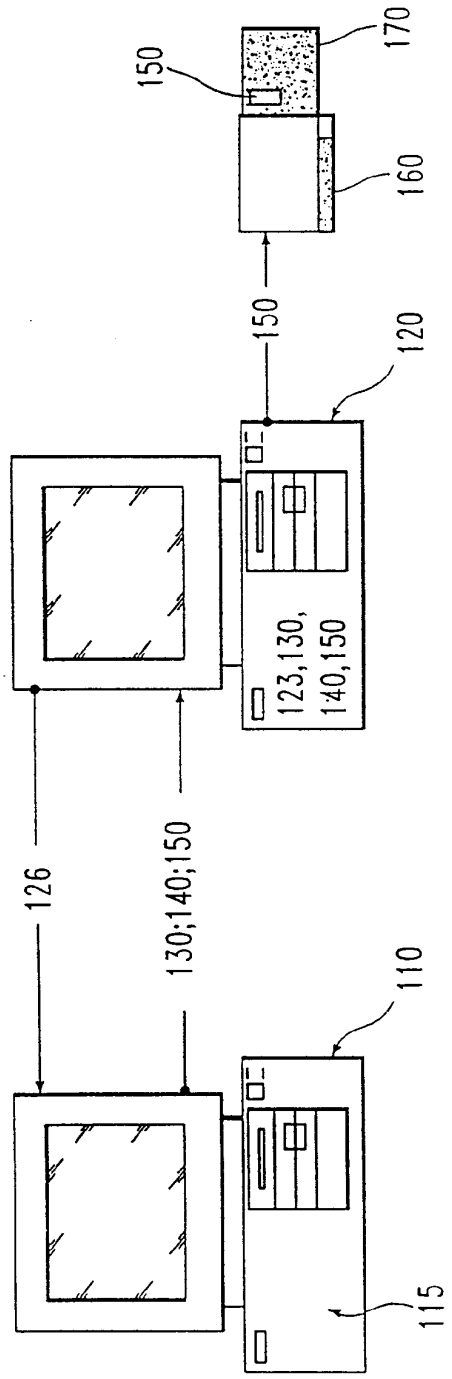


FIG. 1

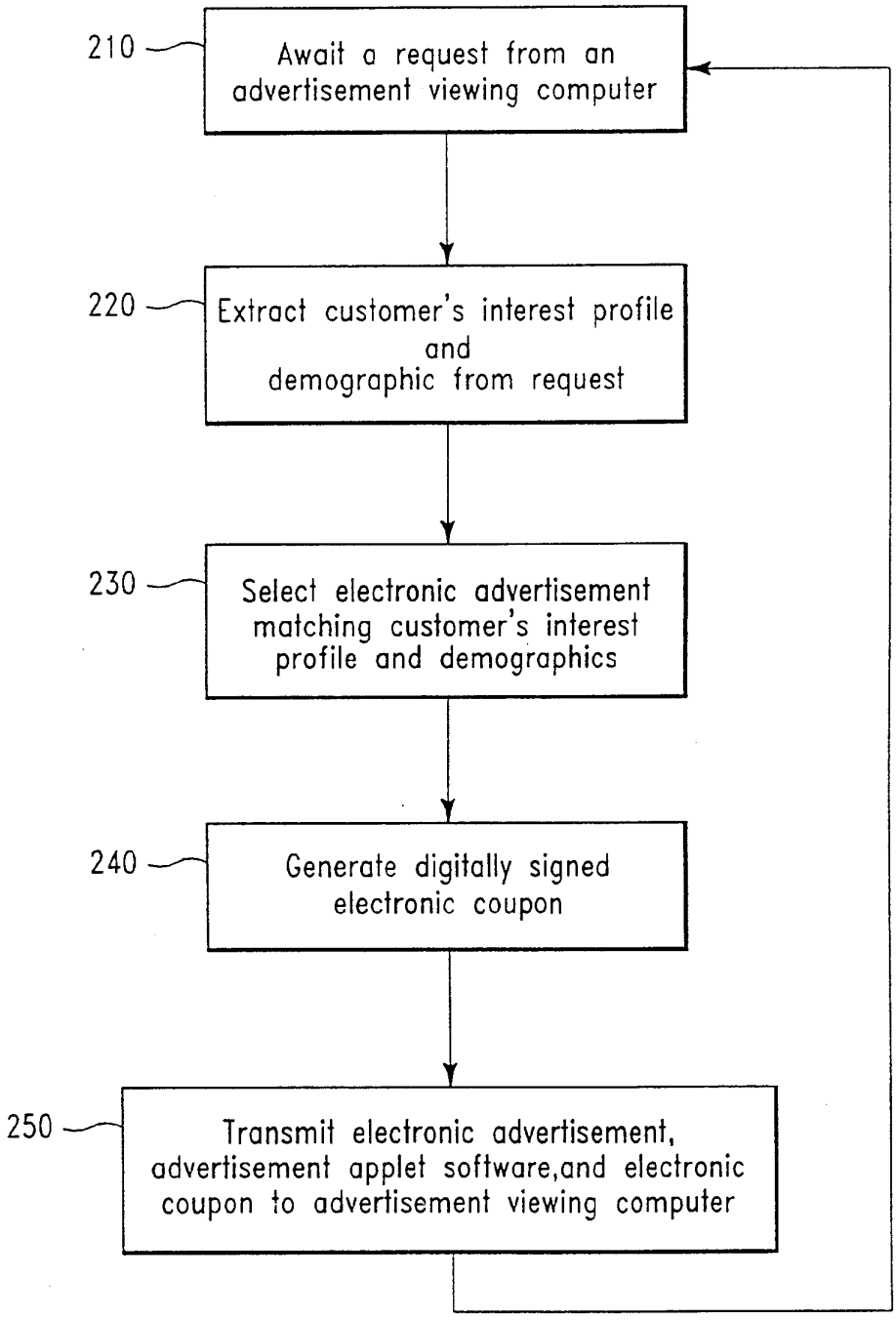

210
Await a request from an advertisement viewing computer
220
Extract customer's interest profile and demographic from request
230
Select electronic advertisement matching customer's interest profile and demographics
240
Generate digitally signed electronic coupon
250
Transmit electronic advertisement, advertisement applet software,and electronic coupon to advertisement viewing computer

FIG. 2

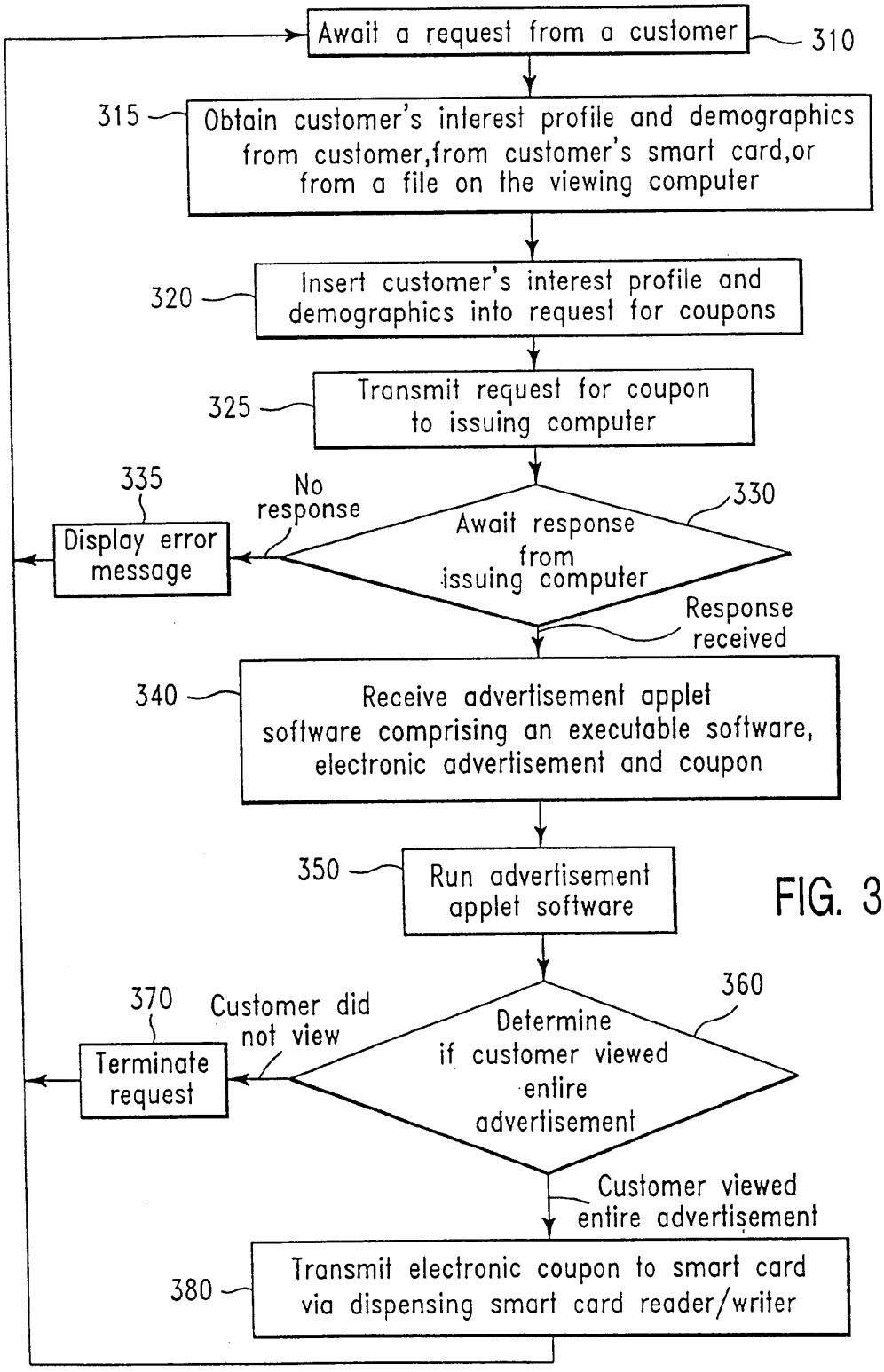
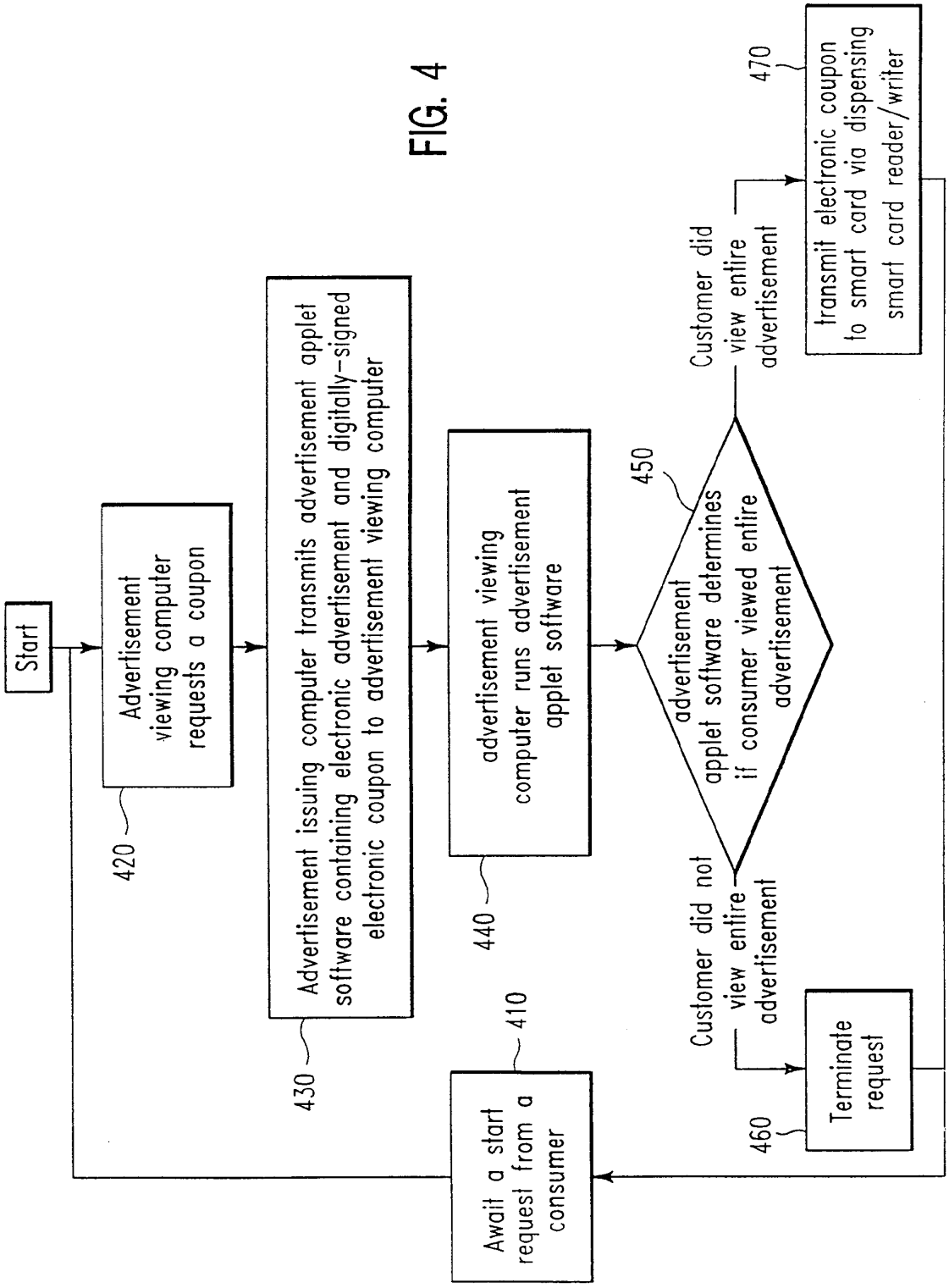

Await a request from a customer
310
315
Obtain customer's interest profile and demographics from customer,from customer's smart card,or from a file on the viewing computer
320
Insert customer's interest profile and demographics into request for coupons
325
Transmit request for coupon to issuing computer
335
No response
330
Display error message
Await response from issuing computer
Response received
340
Receive advertisement applet software comprising an executable software, electronic advertisement and coupon
350
Run advertisement applet software
370
Customer did not view
360
Terminate request
Determine if customer viewed entire advertisement
Customer viewed entire advertisement
380
Transmit electronic coupon to smart card via dispensing smart card reader/writer

FIG. 3

FIG. 4


Start
Advertisement viewing computer requests a coupon
420
Advertisement issuing computer transmits advertisement applet software containing electronic advertisement and digitally-signed electronic coupon to advertisement viewing computer
430
advertisement viewing computer runs advertisement applet software
440
advertisement applet software determines if consumer viewed entire advertisement
450
Customer did view entire advertisement
transmit electronic coupon to smart card via dispensing smart card reader/writer
470
Customer did not view entire advertisement
Terminate request
460
Await a start request from a consumer
410

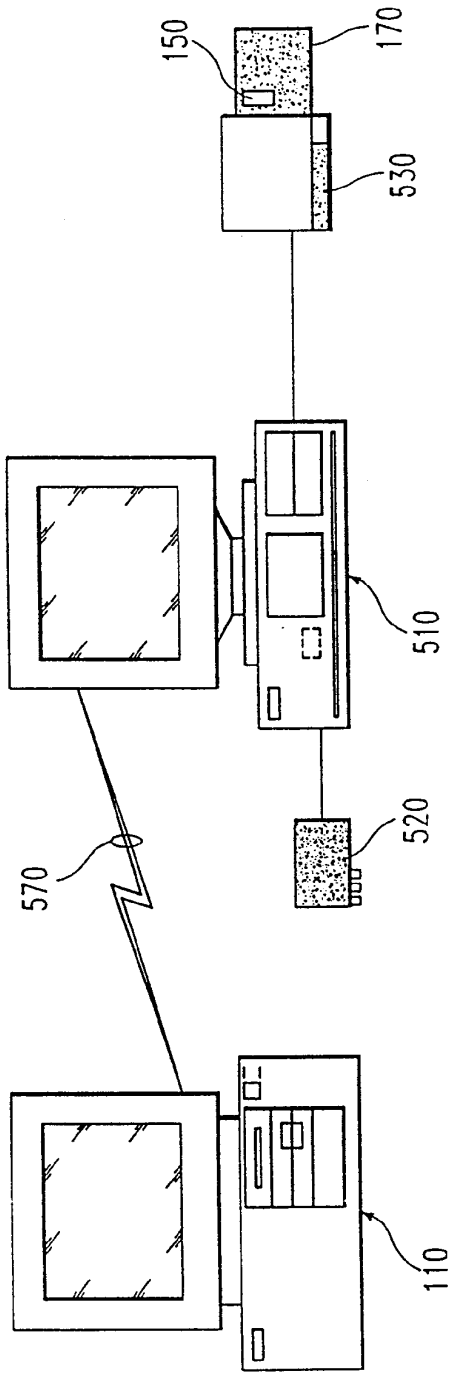


FIG. 5

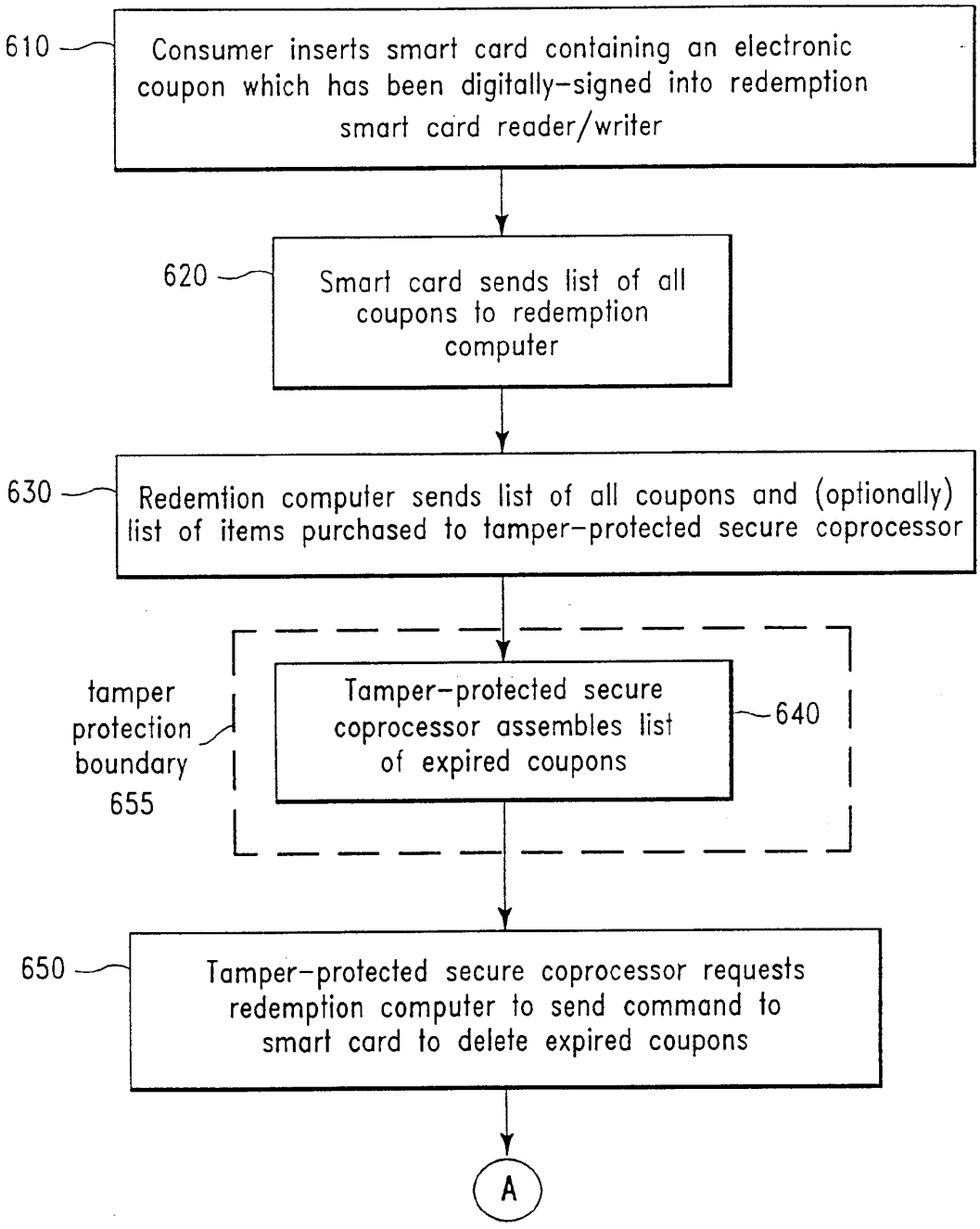

610
Consumer inserts smart card containing an electronic coupon which has been digitally-signed into redemption smart card reader/writer
620
Smart card sends list of all coupons to redemption computer
630
Redemtion computer sends list of all coupons and (optionally) list of items purchased to tamper-protected secure coprocessor
tamper protection boundary 655
Tamper-protected secure coprocessor assembles list of expired coupons
640
650
Tamper-protected secure coprocessor requests redemption computer to send command to smart card to delete expired coupons
A

FIG. 6

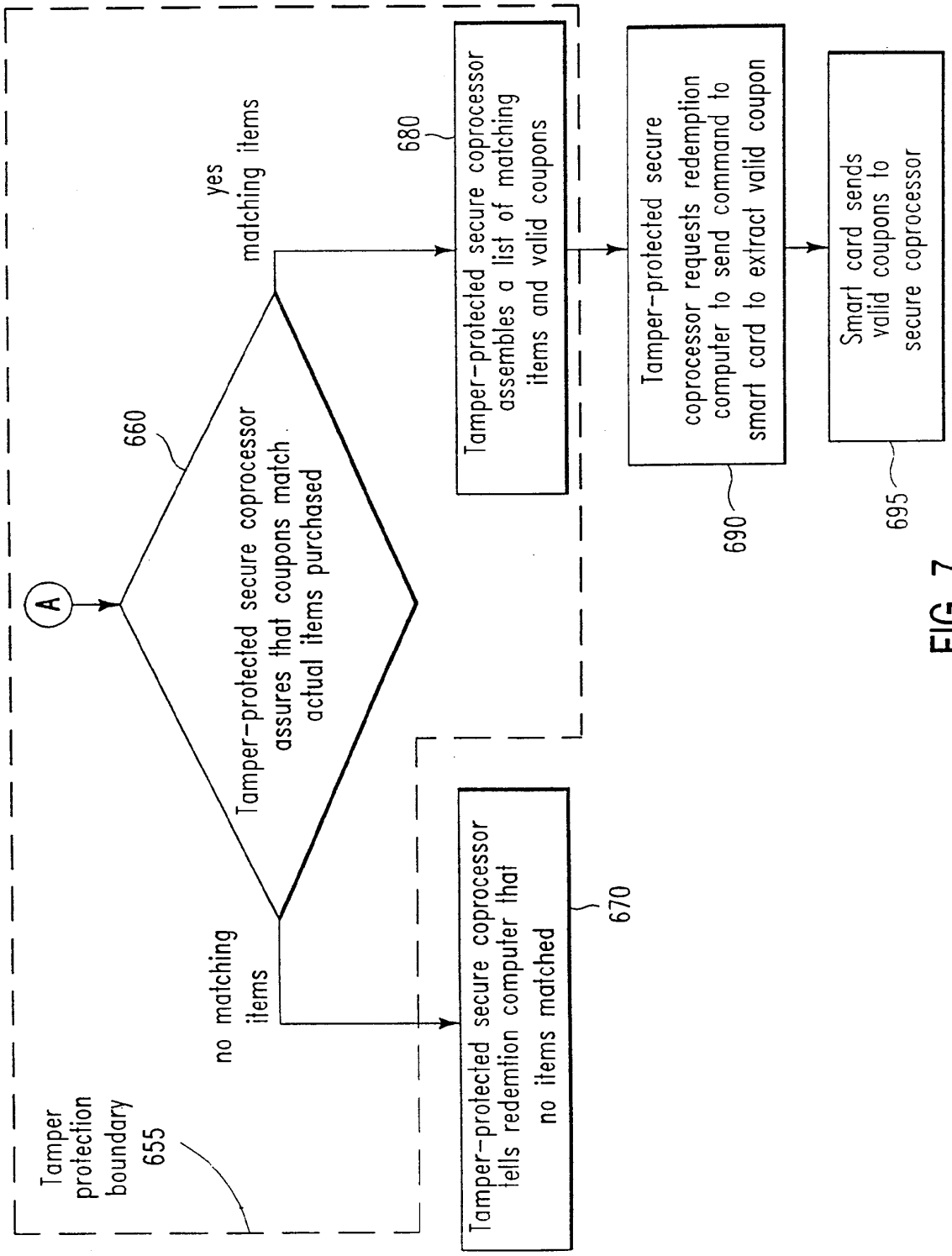

Tamper protection boundary 655
A
660
Tamper-protected secure coprocessor assures that coupons match actual items purchased
yes matching items
no matching items
680
Tamper-protected secure coprocessor assembles a list of matching items and valid coupons
Tamper-protected secure coprocessor requests redemption computer to send command to smart card to extract valid coupon
690
Smart card sends valid coupons to secure coprocessor
695
Tamper-protected secure coprocessor tells redemtion computer that no items matched
670

FIG. 7

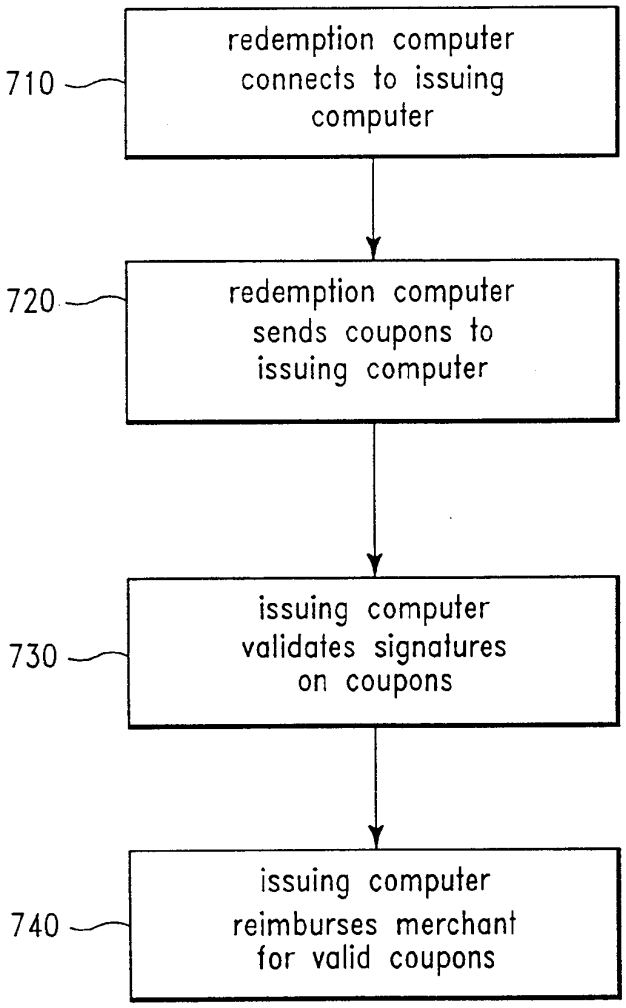

710
redemption computer connects to issuing computer
720
redemption computer sends coupons to issuing computer
730
issuing computer validates signatures on coupons
740
issuing computer reimburses merchant for valid coupons

FIG. 8

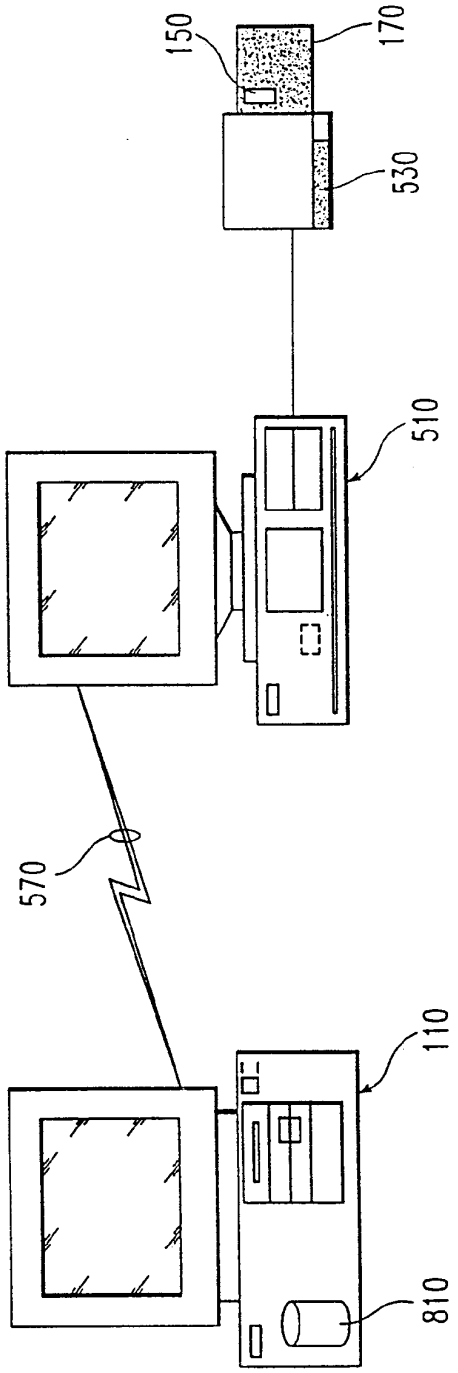


FIG. 9

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/GB 99/00575

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F17/60 G07F7/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G07F G07G

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 30410 A (POWELL KEN R) 21 August 1997	1-3
A	see abstract see page 4, line 15 - line 31 see page 7, line 28 - page 13, line 23 see figures 1,4,5,9,10	7,11,12
A	US 5 594 493 A (NEMIROFSKY FRANK R) 14 January 1997 see column 3, line 49 - column 6, line 67 see column 11, line 30 - column 12, line 32 see column 13, line 30 - line 43 see column 15, line 21 - line 32 see figure 7	1,2,7
A	US 5 557 721 A (FITE KENNETH R ET AL) 17 September 1996	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 June 1999	16/06/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bocage, S

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/GB 99/00575

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 380 991 A (VALENCIA LUIS ET AL) 10 January 1995	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Interr ıal Application No
PCT/GB 99/00575

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9730410 A	21-08-1997	US 5806044 A	08-09-1998
		AU 2050797 A	02-09-1997
		CA 2246774 A	21-08-1997
US 5594493 A	14-01-1997	AU 683352 B	06-11-1997
		AU 1684395 A	08-08-1995
		CA 2181705 A	27-07-1995
		EP 0761063 A	12-03-1997
		JP 9508993 T	09-09-1997
		WO 9520294 A	27-07-1995
		US 5880769 A	09-03-1999
		US 5767896 A	16-06-1998
US 5557721 A	17-09-1996	WO 9117530 A	14-11-1991
US 5380991 A	10-01-1995	AU 1175195 A	06-06-1995
		WO 9514287 A	26-05-1995

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G06F 1/00

A1

(11) Internationale Veröffentlichungsnummer: **WO 99/38062**

(43) Internationales Veröffentlichungsdatum: 29. Juli 1999 (29.07.99)

(21) Internationales Aktenzeichen: PCT/EP99/00250

(22) Internationales Anmeldedatum: 18. Januar 1999 (18.01.99)

(30) Prioritätsdaten:

198 02 316.2	22. Januar 1998 (22.01.98)	DE
198 41 886.8	11. September 1998 (11.09.98)	DE

(81) Bestimmungsstaaten: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(71) Anmelder: KOBIL COMPUTER GMBH [DE/DE]; Weinsheimer Strasse 71, D–67547 Worms (DE).

(72) Erfinder: ISMET, Koyun; Weinsheimer Strasse 71, D–67547 Worms (DE).

(74) Anwalt: REBLE, KLOSE & SCHMITT; Patente + Marken, Postfach 12 15 19, D–68066 Mannheim (DE).

(54) Title: METHOD AND DEVICE FOR CREATING PASSWORDS

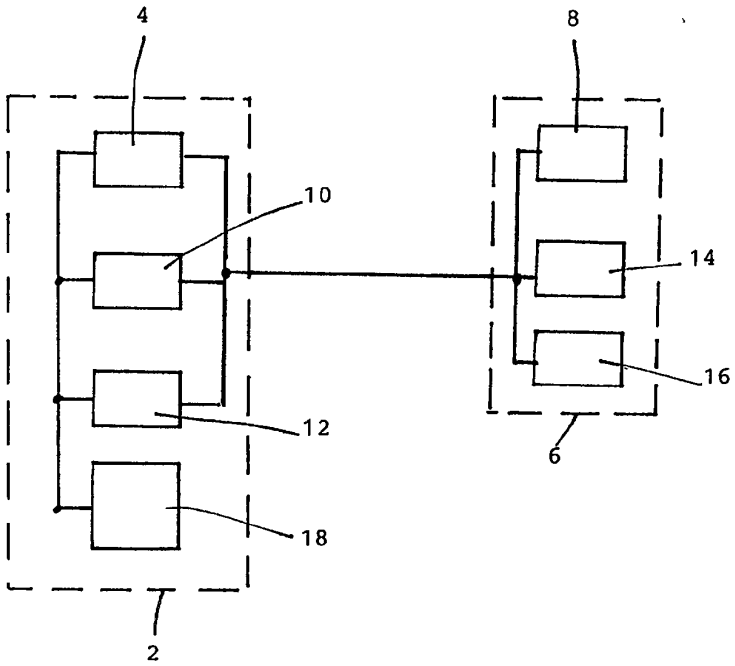
(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ERZEUGUNG VON PASSWÖRTERN

(57) Abstract

According to the invention, a non–repetitive password is created by both the user and the server. Access is then only permitted when both passwords match.

(57) Zusammenfassung

Einmalpaßwort wird sowohl vom Benutzer als auch vom Server erzeugt. Zugang wird nur dann gewährt, wenn diese beiden Paßwörter übereinstimmen.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren und Vorrichtung zur Erzeugung von Paßwörtern

Die Erfindung bezieht sich auf ein Verfahren zur Erzeugung von Paßwörtern gemäß den im Oberbegriff des Patentanspruchs 1 angegebenen Merkmalen. Ferner bezieht sich die Erfindung auf eine Vorrichtung zur Durchführung des Verfahrens.

In der Computertechnik gibt es viele Situationen, in denen aus sicherheitstechnischen Gründen eine Authentifizierung eines Benutzers vorgenommen werden muß. Diese Problemstellung ist insbesondere in unsicheren Netzen, wie beispielsweise der Rechnerzugang im Internet oder beim Homebanking via Modem und Telefonnetz von besonderer Bedeutung. Ein potentieller Angreifer darf durch Abhören einer beliebig langen Sequenz von Paßwörtern, welche ein Benutzer oder Client C zur erfolgreichen Berechtigungsüberprüfung oder Authentifizierung beim Server benutzt, nicht in der Lage sein, ein künftiges gültiges Paßwort für den Benutzer oder Client C zu berechnen.

Die Lösung dieser Aufgabe erfolgt gemäß den im Patentanspruch 1 angegebenen Merkmalen sowie gemäß den im Vorrichtungsanspruch angegebenen Merkmalen.

Die erfindungsgemäße Lösung besteht darin, daß der Benutzer dem Rechner ein nur für eine aktuelle Session gültiges Paßwort übergibt, welches ihn eindeutig als den berechtigten Benutzer oder authentischen Client charakterisiert. Der Rechner und insbesondere der Server ist seinerseits in der Lage, das für diesen bestimmten Benutzer aktuell gültige Einmalpaßwort zu bestimmen. Dem Benutzer wird ein weiterer Zugang nur dann gestattet, wenn das eingegebene Paßwort und das vom Rechner berechnete Paßwort übereinstimmen. Wesentlich ist, daß das jeweilige Paßwort immer nur ein einziges Mal gültig ist, welches durch synchrone Berechnung einmalig erzeugt worden ist. Die Sicherheit gegen unbefugte Benutzung ist somit auch in unsicheren Netzen, wie beispielsweise im Internet oder beim Homebanking via Modem und Telefonnetz gewährleistet. Alle Benutzer oder Teilnehmer verwenden das gleiche Verschlüsselungsverfahren oder Kryptosystem, wobei die zugrundeliegende Verschlüsselungsfunktion $f_{k(C)}$ durch einen geheimen Schlüssel k(C) parametrisiert ist. Alle Berechnungen sowohl auf der Benutzerseite als auch auf der Rechnerseite werden in bevorzugter Weise auf einer Prozessorchipkarte durchgeführt, welche zur Durchführung des genannten Verschlüsselungsverfahrens ausgebildet ist. Erfindungsgemäß gelangt eine durch einen geheimen Schlüssel k(C) parametrisierte Schar von Permutationen, d.h. von bijektiven Funktionen auf deren Argumentbereich, $f_{k(C}:D\rightarrow D$ zum Einsatz. Diese Schar genügt wenigstens einer, bevorzugt mehreren der folgenden Bedingungen:

1. Die Definitionsmenge (und Bildmenge) D ist endlich und besitzt hinreichend viele Elemente. Sie enthält insbesondere mindestens 2^{54} viele Elemente.

2. Die Menge aller zulässigen Schlüssel ist hinreichend mächtig. Sie enthält insbesondere mindestens 2^{66} viele Elemente.

3. $f_{k(C)}$ ist eine zufällige Funktion ("random function") in dem Sinne, daß bei beliebigem vorgegebenem Argument x aus der Definitionsmenge D die Wahrscheinlichkeit, ein bestimmtes Element y aus D als Ergebnis der Funktionsauswertung zu erhalten, ungefähr gleich $1/|D|$ ist, wenn man zufällig und gleichverteilt einen Schlüssel k(C) aus der Menge aller möglichen Schlüssel auswählt.

4. Bei Kenntnis einer Folge von Werten $x_0, x_1, \ldots\ldots, x_n$ aus der Definitionsmenge D, wobei $x_{i+1} = f_{k(C)}(x_i)$ für $0 \leq i < n$ gelte, soll es einem potentiellen Angreifer in der

Praxis auch mit Hilfe leistungsfähiger Computer unmöglich sein, in vertretbarer Zeit den Schlüssel k(C) zu bestimmen oder $x_{n+1} = f_{k(C)}(x_n)$ zu berechnen.

Der Rechner und der Benutzer verfügen beide über einen geheimen Startwert, welcher Startwert $x_{o,c}$ vom Server initial zufällig erzeugt wird und in einer sicheren Umgebung in den geheimen, von außen nicht zugänglichen Speicherbereich der Chipkarte des Benutzers geschrieben wird. Des weiteren wird mittels des Rechners ein zufälliger geheimer Schlüsselwert k(C) ermittelt und von diesem in einen von außen nicht zugänglicher Speicherbereich eines Datenträgers, insbesondere einer Chipkarte des Benutzers C geschrieben. Die Chipkarte wird dann an den Benutzer C ausgegeben. Des weiteren enthält der Rechner eine nur von Autorisierten zugängliche Datenbank, in welcher die Zuordnung des dem jeweiligen Benutzer zugeordneten geheimen Schlüssels k(C) und das letzte vom Benutzer C benutzte Paßwort $x_{n,c}$ gespeichert ist. Ferner ist in der Chipkarte des Benutzers C in einem gesicherten Speicherbereich dauerhaft der jeweilige geheime Schlüsselwert k(C) sowie das letzte benutzte Paßwort $x_{n,c}$ gespeichert. Des weiteren wird erfindungsgemäß die Benutzung bereits existierender Hard- und Firmware beim Benutzer ermöglicht. So können beispielsweise die bekannten EC-Karten mit Chip benutzt werden, welche als Prozessor-Chipkarten ausgebildet sind und auf welche neben Standardanwendungen, Electronic Cash und elektronische Geldbörse weitere Applikationen nachgeladen werden können. Die von deutschen Banken derzeit ausgegebene EC-Karte vermag standardmäßig folgende Verschlüsselungsverfahren auszuführen: Den Data Encryption Standard, kurz DES, sowie Triple-DES. Des weiteren können die in Mobiltelefonen eingesetzten Chipkarten verwendet werden. Hierbei besitzt ein Benutzer bereits einen geeigneten Chipkartenleser, nämlich sein Mobiltelefon, welches darüber hinaus über ein Display und eine Tastatur verfügt. Weitere Ausgestaltungen und Besonderheiten der Erfindung sind in den Unteransprüchen angegeben.

Die Erfindung wird nachfolgend an Hand des in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert.

Der Rechner 2 enthält eine erste Einheit 4 zur Durchführung eines bekannten Kryptoverfahrens mit der Verschlüsselungsfunktion $f_{k(C)}$. Der Benutzer erhält einen Datenträger 6, insbesondere in Form einer Chipkarte, welche eine zweite Einheit 8 zur Durchführung des genannten Kryptoverfahrens gemäß $f_{k(C)}$ aufweist. Als Verschlüsselungsverfahren gelangen insbesondere die heute üblichen symmetrischen Kryptosysteme wie DES, Triple-DES oder IDEA zur Verwendung. Anstelle der genannten Verschlüsselungsfunktion $f_{k(C)}$ kann erfindungsgemäß die zugehörige Entschlüsselungsfunktion $f_{k(C)}^{-1}$ verwendet

werden. Der Rechner 2 enthält ferner eine erste Kompenente 10 zur Erzeugung eines geheimen Startwertes $x_{0,c}$ sowie eine zweite Komponente 12 zur Erzeugung eines geheimen Schlüssels k(C). Der Datenträger bzw. die Chipkarte 6 enthält einen ersten Speicher 14 für den geheimen Startwert $x_{o,c}$ sowie einen weiteren Speicher 16 für den geheimen Schlüssel k(C). Schließlich enthält der Rechner 2 eine Datenbank 18, welche nur für Autorisierte zugänglich ist und in welcher die Zuordnung des Benutzers bzw. der Chipkarte mit deren geheimen Schlüssel k(C) sowie das letzte vom Benutzer C benutzten Paßwort $x_{n,c}$ gespeichert sind. Alle Benutzer oder Teilnehmer des erfindungsgemäßen Verfahrens oder der erfindungsgemäßen Vorrichtung verwenden das gleiche Kryptosystem mit der gleichen Verschlüsselungsfunktion $f_{k(c)}$ und / oder die zugehörenden Entschlüsselungsfunktion $f_{k(C)}^{-1}$. Es sei festgehalten, daß die Verschlüsselungsfunktion $f_{k(C)}$ eine Permutation, also eine bijektive Funktion auf den Argumentbereich ist, und daß anstelle der genannten Verschlüsselungsfunktion bedarfsweise die zugehörende Entschlüsselungsfunktion verwendbar ist. Die zum Einsatz gelangende Verschlüsselungsfunktion $f_{k(C)}$ ist durch den geheimen Schlüssel k(C) parametrisiert.

Der bevorzugt mittels des Rechners 2 initial zufällig erzeugte geheime Startwert $x_{o,c}$ wird im Rahmen der Erfindung auf den Datenträger 6 in dessen ersten Speicherbereich 14 geschrieben. Ferner wird der bevorzugt gleichfalls mittels des Rechners 2 erzeugte zufällige Schlüssel k(C) in den zweiten von außen gleichfalls nicht zugänglichen Speicherbereich 16 des Datenträgers 6 des Benutzers C geschrieben. Der derart vorbereitete Datenträger bzw. die Chipkarte 6 wird dann dem Benutzer C übergeben und ermöglicht jederzeit dessen Authentifizierung oder Feststellung der Zugriffsberechtigung auf den Rechner 2. Lautet das zuletzt von C benutzte Paßwort $x_{n,c}$, so finden Client C und Server das nächste gültige Paßwort durch Berechnen von

$$x_{n+1,C} = f_{k(C)}\,(x_{n,\,C}).$$

Im Rahmen der Erfindung ist folglich für den Benutzers mittels des derart vorbereiteten Datenträgers 6 die Möglichkeit geschaffen, dem Rechner jeweils nur für die gewünschte Session ein einmaliges gültiges Paßwort zu übergeben, welches ihn eindeutig als authentischen Benutzer charakterisiert. Der Rechner, insbesondere der Server, ist seinerseits in die Lage versetzt, das für diesen einen Benutzer aktuell gültige Einmalpaßwort zu bestimmen. Ein weiterer Zugang ist für den Benutzer nur dann ermöglicht, wenn das eingegebene Paßwort und das vom Rechner berechnete Paßwort übereinstimmen. Das Einmalpaßwort wird für jede Session oder Transaktion neu erzeugt und ist nur für dieses einzige Mal gültig.

Alternativ kann unter der Voraussetzung, daß die Verschlüsselungsfunktion $f_{k(C)}$ eine Permutation dargestellt, anstelle der Verschlüsselungsfunktion $f_{k(C)}$ die zugehörige Entschlüsselungsfunktion $f_{k(C)}^{-1}$ verwendet werden, wobei die Berechnung des nächsten gültigen Paßworts nach der Formel erfolgt:

$$x_{n+1,C} = f_{k(C)}^{-1}(x_{n,C}).$$

Da ein sicheres Kryptosystem, beispielsweise DES, Triple-DES oder IDEA zum Einsatz gelangt, kenn ein Unbefugter auch bei Kenntnis von $x_{o,C}$ bis $x_{n,C}$ auch das nächste Paßwort $x_{n+1,C}$ nicht berechnen bzw. das Verschlüsselungsverfahren $f_{k(C)}$ nicht berechnen. Durch den Einsatz der genannten heute gängigen symmetrischen Kryptosysteme kann auf die Verwendung der Entschlüsselungsfunktion $f_{k(C)}^{-1}$ anstelle der Verschlüsselungsfunktion $f_{k(C)}$ verzichtet werden, da aus der Kenntnis der expliziten Verschlüsselungsfunktion effizient auf einfache Art und Weise die betreffende Entschlüsselungsfunktion bestimmbar ist.

Damit die Software, welche die Kyptoalgorithmen ausführt, nicht durch Unbefugte manipuliert werden kann, werden in zweckmäßiger Weise die erste Einheit 4, die erste Komponente 10, die zweite Komponente 12 und der zweite Speicherbereich 16 ganz oder teilweise auf einer hochsicheren Prozessorchipkarte realisiert.

Bezugszeichen

2	Rechner
4	erste Einheit
6	Datenträger / Chipkarte
8	zweite Einheit
10	erste Komponente
12	zweite Komponente
14	erster Speicherbereich
16	zweiter Speicherbereich
18	Datenbank

Patentansprüche

1. Verfahren zur Erzeugung von Paßwörtern und zur Überprüfung der Zugriffsberechtigung auf einen Rechner unter Verwendung einer durch einen bevorzugt geheimen Schlüssel k(C) parametrisierte Schar von Permutationen und/oder einer Verschlüsselungsfunktion und eines einem Benutzer zugeordneten Paßworts,
dadurch gekennzeichnet, daß ausgehend von einem geheimen Startwert unter Einbeziehung eines zuvor benutzten Paßwortes, insbesondere des zuletzt benutzten Paßwortes, das nächste gültige Paßwort berechnet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die durch synchrone Berechnung sowohl im Rechner als auch auf der Benutzerseite erzeugten Paßworte nur einmalig benutzt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die durch den geheimen Schlüssel k(C) parametrisierte Schar von Permutationen, also von bijektiven Funktionen auf deren Argumentbereich, $f_{k(C)}:D\rightarrow D$ zum Einsatz gelangen, die folgenden Bedingungen ganz oder teilweise derart genügt, daß die Definitionsmenge und/oder die Bildmenge D endlich sind und hinreichend viele Elemente, insbesondere mindestens 2^{54} Elemente aufweisen und/oder daß die Menge aller zulässigen Schlüssel hinreichend mächtig ist und bevorzugt mindestens 2^{66} viele Elemente aufweist.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Funktion $f_{k(C)}$ eine zufällige Funktion (random function) derart ist, daß bei beliebigem vorgegebenem Argument x aus der Definitionsmenge D die Wahrscheinlichkeit, ein bestimmtes Element y aus D als Ergebnis der Funktionsauswertung zu erhalten, ungefähr gleich $1/|D|$ ist, wobei bevorzugt zufällig und/oder gleichverteilt ein Schlüssel k(C) aus der Menge aller möglichen Schlüssel ausgewählt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß bei Kenntnis einer Folge von Werten $x_0, x_1, \ldots, x_n$ aus der Definitionsmenge D, wobei $x_{i+1} = f_{k(C)}(x_i)$ für $0 \leq i < n$ gelte, es einem potentiellen Angreifer in der Praxis auch mit Hilfe leistungsfähiger Computer unmöglich ist, in vertretbarer Zeit den Schlüssel k(C) zu bestimmen oder $x_{n+1} = f_{k(C)}(x_n)$ zu berechnen.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die zugrundliegende Verschlüsselungsfunktion oder Entschlüsselungsfunktion durch den geheimen Schlüsselwert parametrisiert ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß auf der Rechnerseite eine Zuordnung des geheimen Schlüsselwertes sowie des letzten vom Benutzer genutzten Paßwortes zu diesem Benutzer erfolgt.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die Berechnungen auf der Rechnerseite und / oder auf der Seite des Benutzers durchgeführt werden, vorzugsweise auf einer zur Durchführung des Verschlüsselungsverfahrens ausgelegten Prozessor-Chipkarte.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß auf der Benutzerseite, insbesondere auf einer Chipkarte in einem gesicherten Speicherbereich dauerhaft der geheime Schlüsselwert sowie das zuletzt von ihr benutzte Paßwort gespeichert sind.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der geheime Startwert insbesondere mittels des Rechners, initial und zufällig erzeugt wird und in sicherer Umgebung in einem geheimen, von außen nicht zugänglichen Speicherbereich beim Benutzer, insbesondere dessen Chipkarte, gespeichert wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß mittels des Rechners der zufällige, geheime Schlüsselwert erzeugt wird und in einen von außen nicht zugänglichen zweiten Speicherbereich des Benutzers, insbesondere dessen Chipkarte, geschrieben und / oder gespeichert wird.

12. Vorrichtung zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß der Rechner (2) eine erste Einheit (4) zur Durchführung des Verschlüsselungsverfahrens enthält und / oder eine zweite Einheit (8) zur Erzeugung des geheimen Startwertes enthält.

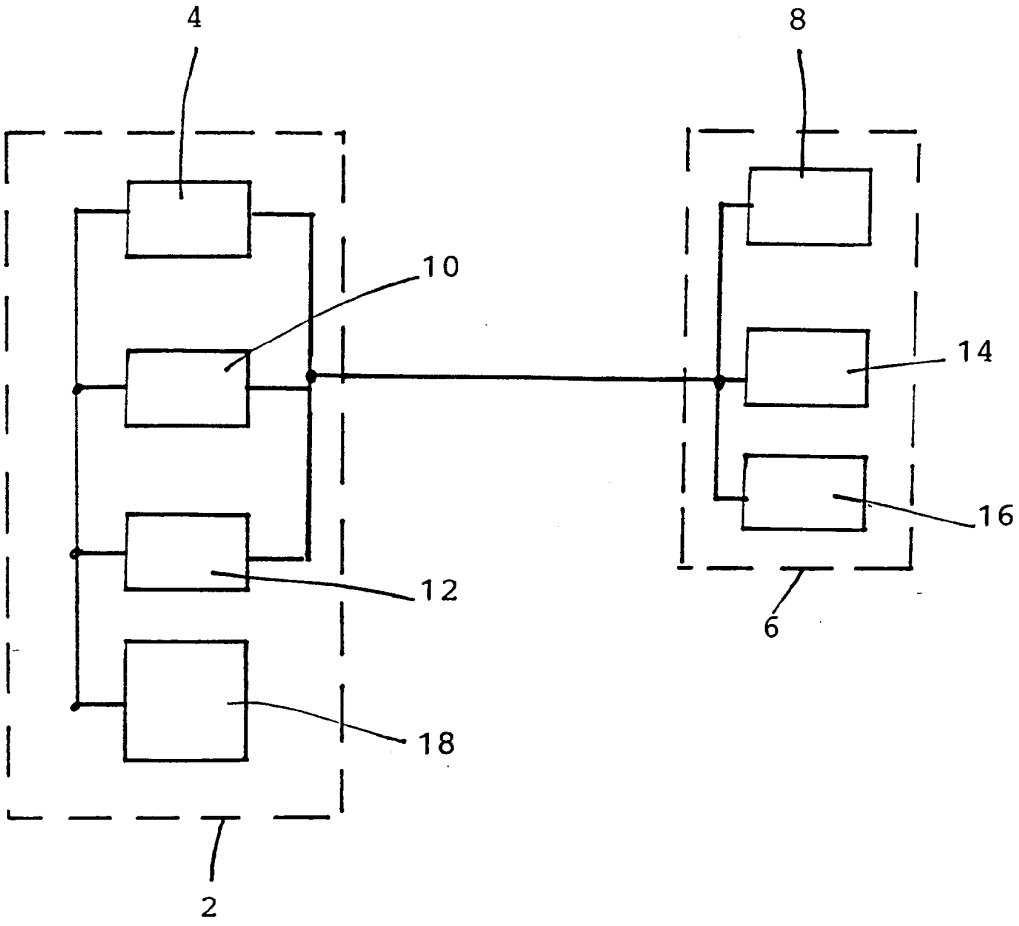
13. Vorrichtung nach Anspruch 12, dadurch gekennzeichnet, daß der Rechner (2) eine erste Speicherkomponente (10) für den geheimen Startwert und / oder eine zweite Speicherkomponente (12) für den Schlüsselwert und / oder eine Datenbank (18) enthält, in welcher eine Zuordnung zum jeweiligen Benutzer erfolgt, und zwar insbesondere

dessen geheimer Schlüsselwert und / oder des letzten vom jeweiligen Benutzer benutzten Paßworts gespeichert ist.

14. Vorrichtung nach einem der Ansprüche 12 oder 13, dadurch gekennzeichnet, daß auf der Benutzerseite ein Datenträger (6), insbesondere eine Chipkarte vorgesehen ist, welche eine zweite Einheit (8) zur Durchführung der Verschlüsselungsverfahrens aufweist.

15. Vorrichtung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, daß der Datenträger bzw. die Chipkarte (6) einen gesicherten ersten Speicherbereich (14) für den geheimen Startwert und / oder einen zweiten gesicherten Speicherbereich (16) für das zuletzt benutzte Paßwort enthält.

16. Vorrichtung nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, daß die erste Einheit (4) und/oder die erste Komponente (10) und/oder die zweite Komponente (12) und/oder die Datenbank (18) auf einer hochsicheren Prozessorchipkarte vorgesehen sind.


4
8
10
14
16
12
6
18
2

INTERNATIONAL SEARCH REPORT

Inter. ..onal Application No
PCT/EP 99/00250

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F F06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 060 263 A (BOSEN ROBERT J ET AL) 22 October 1991 see figures 1-4,6 see column 5, line 49 - column 9, line 35	1,2,4, 6-10
A	EP 0 262 025 A (FUJITSU LTD) 30 March 1988 see figures 1,2,4,6 see column 2, line 36 - line 56 see column 3, line 18 - column 4, line 50	1,6,8-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 1999	06/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. ...nal Application No
PCT/EP 99/00250

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5060263 A	22-10-1991	NONE	
EP 0262025 A	30-03-1988	JP 2086924 C	02-09-1996
		JP 8007720 B	29-01-1996
		JP 63073348 A	02-04-1988
		CA 1298653 A	07-04-1992
		DE 3784824 A	22-04-1993
		DE 3784824 T	11-09-1997
		US 4853522 A	01-08-1989

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/00250

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F F06F G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 060 263 A (BOSEN ROBERT J ET AL) 22. Oktober 1991 siehe Abbildungen 1-4,6 siehe Spalte 5, Zeile 49 - Spalte 9, Zeile 35	1,2,4, 6-10
A	EP 0 262 025 A (FUJITSU LTD) 30. März 1988 siehe Abbildungen 1,2,4,6 siehe Spalte 2, Zeile 36 - Zeile 56 siehe Spalte 3, Zeile 18 - Spalte 4, Zeile 50	1,6,8-10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. Juni 1999	06/07/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interna. onales Aktenzeichen
PCT/EP 99/00250

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5060263 A	22-10-1991	KEINE	
EP 0262025 A	30-03-1988	JP 2086924 C	02-09-1996
		JP 8007720 B	29-01-1996
		JP 63073348 A	02-04-1988
		CA 1298653 A	07-04-1992
		DE 3784824 A	22-04-1993
		DE 3784824 T	11-09-1997
		US 4853522 A	01-08-1989

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 :		(11) Internationale Veröffentlichungsnummer: **WO 00/36252**
E05B 49/00, 19/00	**A1**	(43) Internationales Veröffentlichungsdatum: 22. Juni 2000 (22.06.00)

(21) **Internationales Aktenzeichen:** PCT/EP99/09251

(22) **Internationales Anmeldedatum:** 29. November 1999 (29.11.99)

(30) **Prioritätsdaten:**
198 58 165.3 16. Dezember 1998 (16.12.98) DE

(71) **Anmelder** *(für alle Bestimmungsstaaten ausser US)*: HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, D–42551 Velbert (DE).

(72) **Erfinder; und**
(75) **Erfinder/Anmelder** *(nur für US)*: JACOB, Dirk [DE/DE]; Breslauer Strasse 13, D–42579 Heiligenhaus (DE).

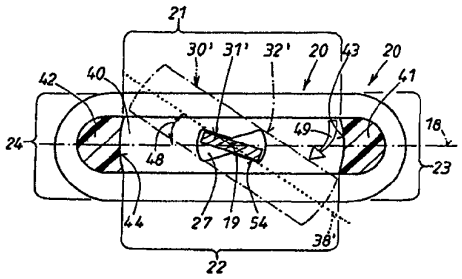
(74) **Anwalt:** MENTZEL, Norbert; Kleiner Werth 34, D–42275 Wuppertal (DE).

(81) **Bestimmungsstaaten:** AU, BR, CN, IN, JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) **Title:** ELECTRONIC KEY, ESPECIALLY FOR MOTOR VEHICLES

(54) **Bezeichnung:** ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR KRAFTFAHRZEUGE



(57) **Abstract**

The invention relates to an electronic key comprising electronic components for receiving or transmitting signals. Said components are integrated in a housing (20). A mechanical emergency key (30') is provided in case of an electronics failure. Said emergency key (30') can be inserted into a recess (27) in the housing (20) together with its key shaft (31'). The aim of the invention is to produce a key which can be handled easily. To this end, one end of the housing is provided with a recess which is undercut at least in places and which usually prevents the inserted emergency key (30') from being pulled out. Usually, the key is in a holding position in the housing (20) with an essentially positive fit. However, the emergency key can be turned in the recess (27) of the housing (20) from a holding position to a release position (30') in which the positive fit between the widening (32') in the key (30') and the recess is eliminated in the pull–out direction of the emergency key.

(57) Zusammenfassung

Bei einem eletronischen Schlüssel sind elektronische Bauteile zum Aussenden bzw. Empfangen von Signalen in ein Gehäuse (20) integriert. Wenn die Elektronik versagt, ist ein mechanischer Notschlüssel (30') vorgesehen, der mit seinem Schlüsselschaft (31') in eine Aufnahme (27) im Gehäuse (20) einsteckbar ist. Um einen bequem zu handhabenden Schlülssel zu entwickeln, wird vorgeschlagen, das eine Gehäuseende mit einem Ausbruch zu versehen, der wenigstens bereichsweise hinterschnitten ist und normalerweise, bei eingestecktem Notschlüssel (30') eine Herausziehbewegung verhindert. Normalerweise befindet sich der Schlüssel in einer im wesentlichen formschlüssigen Haltelage im Gehäuse (20). Der Notschlüssel ist aber in der Aufnahme (27) des Gehäuses (20) aus einer Haltelage in eine Löselage (30') verdrehbar, in welcher der Formschluss zwischen einer Verbreiterung (32') im Schlüssel (30') und dem Ausbruch in Richtung der Herausziehbewegung des Notschlüssels beseitigt ist.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Elektronischer Schlüssel, insbesondere für Kraftfahrzeuge

Die Erfindung richtet sich auf einen Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Dieser ist nicht nur als elektronischer Schlüssel ausgebildet, sondern umfasst auch einen mechanischen Notschlüssel. Der Notschlüssel dient dazu um bei Ausfall der Elektronik das Schloss mechanisch öffnen zu können.

Bei dem bekannten Schlüssel dieser Art hat das Gehäuse des elektronischen Schlüssels eine Aufnahme für den Notschlüssel. Im Gebrauchsfall lässt sich der Notschlüssel an einer als Schlüsselkopf fungierenden Verbreiterung od. dgl. erfassen. Ein Problem besteht darin, die Einstecklage des Notschlüssels in der Aufnahme zu sichern. Diese Sicherung soll aber nicht die Handhabung des Notschlüssels beim Einstecken und Herausziehen behindern.

Der Erfindung liegt die Aufgabe zugrunde, einen bequem zu handhabenden Schlüssel zu entwickeln, der im Gehäuse im Einsteckfall zuverlässig gehalten wird. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angegebenen Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Verbreiterung des Schlüssels dient zweckmäßigerweise auch als Handhabe des Notschlüssels und besteht in der Regel aus einen Schlüsselkopf. Es versteht sich,

dass eine solche Verbreiterung nicht die Funktion der Handhabe vom Notschlüssel haben muss. Der Einfachheit wegen soll nachfolgend diese Verbreiterung aber stets mit „Schlüsselkopf" bezeichnet werden. Bezüglich des Gehäuses lässt sich der Schlüsselkopf zwischen zwei zueinander drehversetzten Lagen überführen, nämlich einer seine Position im Gehäuse sichernden Haltelage und einer seine Entnahme aus dem Gehäuse ermöglichenden Löselage. In der Haltelage liegt ein Formschluss vor, wo die Verbreiterung bzw. der Schlüsselkopf wenigstens bereichsweise in einem Ausbruch des einen Gehäuseendes sich befindet. In der Haltelage ist ein Herausziehen des Notschlüssels aus dem Gehäuse nicht möglich. Das Herausziehen ist aber schnell und bequem ausführbar, weil der Schlüsselkopf in einer im wesentlichen senkrecht zur Ebene des Ausbruchs liegenden Richtung nicht vom Gehäuse überdeckt ist und in die demgegenüber verdrehte Löselage bewegt werden kann. Diese Bewegung erfolgt als Drehung um eine in Längsrichtung des Schlüsselschafts verlaufende Drehachse. In der Löselage ist der Schlüsselkopf nicht mehr formschlüssig erfasst. Dann ist eine translatorische Bewegung des Notschlüssels im Sinne eines Herausziehens möglich. Das Herausziehen des Notschlüssels aus dem Gehäuse in der Löselage erfolgt also in einer drehversetzten Ebene bezüglich der vorausgehend in der Haltelage bestehenden Position zwischen Gehäuse und Schlüsselkopf.

Diese Bewegung der Bauteile beim Kuppeln und Entkuppeln lässt sich als „Einrenkbewegung" beschreiben. Die Verbreiterung des Schlüssels bzw. der zu seiner Handhabung dienende Schlüsselkopf können eine ausreichend große Fläche aufweisen, ohne die Sicherungsfunktion in der Haltelage zu gefährden. Dadurch ist die Handhabung sowohl beim Kuppeln als auch Entkuppeln und schließlich bei der Schlüsselbetätigung erleichtert. Dies gilt insbesondere wenn man den Schlüsselkopf und das Gehäuse plattenartig ausbildet, die in der Haltelage einen bündigen Übergang der Außenflächen dieser Bauteile gewährleisten. Störende Kanten oder Vorsprünge liegen nicht vor. Daher ist die Aufbewahrung des Schlüssels in der Hosentasche der Bedienungsperson besonders angenehm.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in einem Ausführungsbeispiel dargestellt. Es zeigen:

Fig. 1 eine Draufsicht auf das Gehäuse des elektronischen Schlüssels mit eingestecktem Notschlüssel,

Fig. 2, schematisch, einen Längsschnitt durch das Gehäuse von Fig. 1,

Fig. 3 + 4 zwei Querschnitte durch das Gehäuse von Fig. 1 und 2 längs der Schnittlinien III - III bzw. IV - IV,

Fig. 5, in einer der Fig. 4 entsprechenden Darstellung, die Lage der Bauteile von Fig. 4 in einer anderen, drehversetzten Lage,

Fig. 6, in einer der Fig. 2 entsprechenden Darstellung, nachdem der Notschlüssel aus dem Gehäuse entnommen worden ist,

Fig. 7, in Draufsicht, den aus dem Gehäuse entnommenen Notschlüssel und

Fig. 8, in perspektivischer, gestreckter Position eine flexible Leiterplatte zur Aufnahme elektronischer Bauteile, die in gefaltetem Zustand im Gehäuse untergebracht wird.

Der erfindungsgemäße Schlüssel umfasst eine Kombination aus dem eigentlichen elektronischen Schlüssel 10 und einem mechanischen Notschlüssel 30. Der elektronische Schlüssel 10 kann über eine größere Entfernung auf ein nicht näher gezeigtes, an ein Kraftfahrzeug angeordnetes Schloss durch codierte Signale 15 wirken. Dazu besitzt das Gehäuse 20, das aus mehreren Gehäuseteilen 21 bis 24 zusammengesetzt sein kann, geeignete elektronische Bauteile 11 und

Betätigungsstellen 13, 14, die dieses Signal 15 generieren und, gegebenenfalls im Dialog, an die entsprechende komplementäre Sende- und Empfangseinrichtung im Fahrzeug weiterleiten. Im Erfolgsfall, wenn die Codierung der Signale 15 akzeptiert wird, wird ein nicht näher gezeigtes elektronisches oder elektromechanisches Schloss wirksam gesetzt. Im Bereich dieser Betätigungsstellen 11 bis 14 sind Mikroschalter 17 angeordnet, die aus Fig. 8 erkennbare Schaltglieder 62 aufweisen. Diese sitzen, zusammen mit den Bauteilen 11 auf einer vorzugsweise auch elektrische Leiterbahnen aufweisende Folie 60, die in Fig. 8 gezeigt ist. Diese Folie 60 kann stellenweise Dellen 61 aufweisen, in welchen manche der Elemente 11 bzw. Glieder 62 versenkt angeordnet sind. Die Folie 60 lässt sich falten und in einen mehr oder weniger zylindrischen Raum im Inneren des Gehäuses 20 unterbringen. Das Gehäuse 20 ist längssymmetrisch aufgebaut bezüglich seiner in Fig. 1 dargestellten Längsmitte 16. Das Gehäuse 20 ist plattenförmig gestaltet, wie aus 63 in Fig. 4 zu ersehen ist und bestimmt eine in Fig. 4 strichpunktiert angedeutete Mittenebene 18.

Der grundsätzliche Aufbau des Notschlüssels 30 ergibt sich aus Fig. 7. Diese umfasst den Schlüsselschaft 31 mit nicht näher gezeigten profilierten Einschnitten bzw. Bahnen für entsprechende Steuermittel im Schloss. An seinem äußeren Ende befindet sich eine Verbreiterung, die einstückig oder mehrstückig gegenüber dem Schlüsselschaft 31 sein kann. Im vorliegenden Fall besteht sie aus einem Schlüsselkopf 32 aus Kunststoff. Der Schlüsselschaft 31 besitzt ein Flachprofil 50, das vorzugsweise aus Metall besteht. Auch der Schlüsselkopf 32 bestimmt eine durch die Punktlinie 38 in Fig. 4 verdeutlichte Mittenebene 38. Das Flachprofil 50 des Schlüsselschafts 31 ist, wie aus Fig. 4 hervorgeht, gegenüber dem vorzugsweise symmetrischen Querschnittsprofil des Schlüsselkopfs 32, ausweislich der strichpunktiert eingezeichneten Querschnittsebene 50 um einen Winkel 39 bezüglich dieser Mittenebene 38 verkippt. Sowohl der Umriss des Gehäuses 20 als auch der des Schlüsselkopfes 32 sind zwar plattenartig 63, 64, gemäß Fig. 4, ausgebildet, können aber in sich profiliert sein. Normalerweise befindet sich der Notschlüssel 30 in seiner aus Fig. 1 bis 4 gezeigten Ruheposition, die nachfolgend kurz „Haltelage“ des Notschlüssels bezeichnet werden soll. In diesem Fall liegt die Mittenebene 18 des

Gehäuses 20 im wesentlichen höhengleich mit der Mittenebene 38 des Schlüsselkopfs 32.

Wie am besten aus Fig. 6 zu entnehmen ist, besitzt das hintere Gehäuseende 28 einen Ausbruch 40, der hier als Gabelöffnung ausgebildet ist. Dadurch entstehen den Ausbruch 40 begrenzende Gabelschenkel 41, 42. Die den Ausbruch 40 nach innen begrenzende Endwand 26 ist mit einer Aufnahme 27 für den bereits beschriebenen Schlüsselschaft 31 des Notschlüssels 30 versehen, wenn die Haltelage 30 gemäß Fig. 1 bis 4 vorliegt. Die Aufnahme 27 entsteht hier durch einen mit der Endwand 26 einstückigen Köcher 25, der einen Innengehäuse bildet und sich in diesem Ausführungsbeispiel in der bereits genannten Längsmitte 16 des Gehäuses 20 befindet. In der Haltelage gemäß Fig. 1 bis 4 ist der Notschlüssel 30 in seiner Einstecklage in der Aufnahme 27 zunächst gesichert und lässt sich nicht ohne weiteres im Sinne des Pfeils 47 von Fig. 2 herausziehen. Dazu werden folgende besondere Maßnahmen vorgeschlagen.

Der Ausbruch 40 ist wenigstens stellenweise bei 43, 44 hinterschnitten. Im vorliegenden Fall wird dies an den beiden Schenkeln 41, 42 durch mehr oder weniger konvergent aufeinander zu laufende Innenflächen 43, 44 der beiden Schenkel 41, 42 erreicht. Dadurch kommt es wenigstens punktuell zu einem Formschluss zwischen den einen Hinterschnitt 45, 46 gemäß Fig. 6 erzeugenden Schenkeln 41, 42 einerseits und dem Schlüsselkopf 32 andererseits. In dieser Haltelage befindet sich der Schlüsselkopf 32 in einer möglichst bündigen Position zum Gehäuse 20, wie durch die bereits erwähnte übereinstimmende Höhenlage der Mittenebene 18, 38 der beiden Plattenformen 63, 64 von Fig. 4 zu entnehmen ist. Zur zusätzlichen Sicherung der Haltelage von Fig. 1 bis 4 können an den Berührungsstellen der Schenkel 41, 42 und im Umfangsbereich zusammenwirkende Rastelemente 51, 52 vorgesehen sein, z.B. ein Vorsprung 51 und eine Vertiefung 52, wie aus Fig. 3 und 5 zu entnehmen ist. Es ist eine Art Einrenkverbindung erforderlich, um den Notschlüssel 30 aus dem Gehäuse 20 im Sinne des Pfeils 47 herausziehen zu können. Dies soll anhand der Fig. 5 näher erläutert werden.

Die Aussparung 40 im Gehäuse 20 ist nach oben bzw. unten offen, weshalb eine Drehung des Schlüsselkopfes aus seiner Haltelage im Sinne des Pfeils 49 der Fig. 3 bis 5 möglich ist. Diese Drehung erfolgt um eine Drehachse 19, die im vorliegenden Fall mit der erwähnten Gehäuselängsmitte 16 zusammenfällt. Man erreicht so die aus Fig. 5 erkennbare andere Lage der Bauteile 20, 30', die aus guten Gründen nachfolgend als „Löselage" des Notschlüssels bezeichnet werden soll. In dieser Löselage 30' liegt nicht mehr der vorgeschriebene Formschluss vor. Jetzt lässt sich der Notschlüssel 30' im Sinne der bereits mehrfach erwähnten Pfeile 47 herausziehen. Eine Kollision der Bauteile 20, 30' findet dann nicht mehr statt. Die vorerwähnte Drehung 49 kann durch Endanschläge 53, 54 im Inneren der Aufnahme 27 begrenzt sein. Im vorliegenden Fall ist der Kippwinkel 39 von Fig. 4 etwa nur halb so groß wie der Drehwinkel 48, bezogen auf die Mittenebene 16 vom Gehäuse 20.

Gemäß Fig. 1 ist der Notschlüssel 30 mit einem überraschend großen Schlüsselkopf 32 versehen, der, zwecks besserer Deutlichkeit, in Punktschraffur dargestellt ist. Das lässt eine bequeme Handhabung sowohl bei der vorbeschriebenen Entnahme 47 als auch bei der späteren Drehbetätigung des Notschlüssels 30 im Schloss zu. Der Schlüsselkopf 32 kann sogar mit einem Reststück 59 über die äußerste Begrenzung des Gehäuses 10 an den Enden der beiden Schenkel 41, 42 in der Haltelage herausragen.

Der Formschluss zwischen der Aussparung 40 und dem Notschlüssel 40 kommt also bei der Erfindung durch axiale Abstützung und gegebenenfalls durch radiale Drehanschläge im Bereich des Schlüsselkopfs 32 zustande. Statt des Schlüsselkopfs 32 könnten auch Verbreiterungen im Schlüsselschaft 31 od. dgl. genutzt werden. Günstig ist es hier für eine Flächenberührung zu sorgen, weshalb die vorbeschriebenen Innenflächen 43, 44 der beiden Schenkel 41, 42 der Drehung 49 entsprechende Rundungen aufweisen und mit möglichst engen Fugen mit einem entsprechenden Gegenprofil bei 33, 34 des Schlüsselkopfs 32 zu liegen kommen. Im

vorliegenden Fall sind die beiden einander gegenüberliegenden Kopfseitenflächen 33, 34 im Sinne der Hilfslinien 35, 36 von Fig. 7 in Richtung auf das freie Kopfende 37 sich im wesentlichen linear verjüngt. Dazu ergibt sich ein Formschluss durch Flächenberührung zwischen 33, 43 einerseits und 34, 44 andererseits. Wegen der Drehung 49 zum Entkuppeln und, wie sich zeigen wird, auch beim Kuppeln, könnte aber der Hintergriff der Bauteile 20, 30 in der Haltelage auch an anderen Stellen wirksam werden, z.B. am freien Kopfende 37. Wegen des guten Hintergriffs lässt sich der in der Haltelage befindliche Notschlüssel 30 auch durch große axiale Kräfte im Sinne der Herausziehpfeils 47 nicht entfernen. Der Notschlüssel ist in seiner Haltelage 30 so zuverlässig in seinem Ausbruch 40 gegenüber im Herausziehsinne wirkende Kräfte positioniert, dass sein Schlüsselkopf 32 ohne weiteres mit einem Aufhängeloch 56 für Schlüsselanhänger od. dgl. versehen sein kann.

Die vorbeschriebene Einrenkbewegung findet im umgekehrten Sinne statt, wenn man, ausgehend von einem entnommenen Notschlüssel wieder in die Aussparung des Gehäuses 20 von Fig. 6 im Sinne des Pfeils 58 von Fig. 6 in das Gehäuse 20 einstecken will. In diesem Fall befindet sich der Notschlüssel zunächst in seiner Löselage 30' außerhalb des Gehäuses 20 und wird dann, im Sinne des Pfeils 58 von Fig. 6, in die Aufnahme 27 hineingeschoben, bis durch axiale Anschläge die Endposition erreicht ist. Dann wird der Notschlüssel in Gegenrichtung zum Drehpfeil 49 in seine Haltelage 30 von Fig. 3 bzw. 4 zurückgeführt.

Das Gehäuse 20 besteht, wie bereits erwähnt wurde, aus mehreren Gehäuseteilen 21 bis 24. Sie umfassen eine im mittleren Bereich angeordnete Oberschale 21 und Unterschale 22 und zwei Seitenteile 23, 24. Die Seitenteile werden von Nocken 57 od. dgl. durchgriffen, die an der Ober- bzw. Unterschale 21, 22 sitzen und für einen Zusammenhalt dieser Gehäuseteile sorgen. Der Ausbruch 40 erfolgt durch Verlängerungen der Gehäuseseitenteile 23, 24 über das Ende der Ober- und Unterschale 21, 22 hinaus, wodurch die bereits erwähnten Gabelschenkel 41, 42 entstehen. Das vordere Gehäuseende 29 wird von der zusammengefügten Ober- und Unterschale 21, 22 gebildet und weist bei 65 von Fig. 2 eine stumpfe Form auf. An

diesem vorderen Gehäuseende 29 beginnen die beiden Seitenteile 23, 24 in einem Axialabstand 66 gegenüber der stumpfen Front 65.

Bezugszeichenliste :

10	elektronischer Schlüssel
11	elektronische Bauteile
12	erste Betätigungsstelle von 10
13	zweite Betätigungsstelle von 10
14	dritte Betätigungsstelle von 10
15	Signal von 10
16	Gehäuselängsrichtung, Längsmitte
17	Mikroschalter
18	Mittelebene von 20, Gehäuseebene
19	Drehachse für 30 in 30‘
20	Gehäuse, Gesamtgehäuse
21	Oberschale von 20
22	Unterschale von 20
23	erster Seitenteil von 20
24	zweiter Seitenteil von 20
25	Köcher für 31 in 20
26	Endwand von 25 zwischen 21, 22
27	Aufnahme in 25 für 31
28	hinteres Gehäuseende von 20
29	vorderes Gehäuseende von 20
30	Notschlüssel (Haltelage; gesichert)
30‘	Löselage von 30
31	Schlüsselschaft von 30 (Haltelage)
31‘	Löselage von 31 bei 30‘
32	Schlüsselkopf von 30 (Haltelage)
32‘	Löselage von 32
33	Gegenprofil für 43 an 32 (Fig. 7), erste Kopfseitenfläche von 32
34	Gegenprofil für 44 an 32 (Fig. 7), zweite Kopfseitenfläche von 32

35 Verjüngung von 33
36 Verjüngung von 34
37 freies Kopfende von 32
38 Ebene des Schlüsselkopfs, Mittenebene von 32 (in Haltelage, Fig. 4)
38‘ Löselage von 38 (Fig. 5)
39 Kippwinkel zwischen 31, 38
40 Ausbruch in 28, Gabelöffnung
41 erster Schenkel von 23, Gabelschenkel
42 zweiter Schenkel von 24, Gabelschenkel
43 Innenfläche von 41
44 Innenfläche von 42
45 Winkel des Hinterschnitts von 43
46 Winkel des Hinterschnitts von 44
47 translatorischer Herauszieh-Pfeil von 30‘
48 Drehwinkel zwischen 30, 30‘
49 Drehpfeil von 30
50 Flachprofil von 31
51 erstes Rastelement an 33, 34, Vorsprung
52 zweites Rastelement an 43, 44, Vertiefung
53 erster Drehanschlag in 27 für 31
54 zweiter Drehanschlag in 27 für 31‘
55 Ebene von 50
56 Aufhängeloch in 32 (Fig. 7)
57 seitlicher Nocken an 22 bzw. 21 für 23 bzw. 24
58 translatorischer Pfeil der Einsteckbewegung von 30‘ (Fig. 6)
59 herausragendes Reststück von 32 (Fig. 1)
60 Folie in 12 und 17
61 Delle in 60 für 17
62 Schaltglied an 17 (Fig. 8)
63 Plattenform von 20 (Fig. 4)
64 plattenartige Form von 32 (Fig. 4)

65 stumpfe Front von 29

66 Axialabstand von 23, 24 gegenüber 29 (Fig. 1)

P a t e n t a n s p r ü c h e :

1.) Elektronischer Schlüssel (10), insbesondere für Kraftfahrzeuge, mit einem Gehäuse (20), das elektronische Bauteile (11) aufnimmt und zum Aussenden bzw. Empfangen von Signalen (15) zum Wirksamsetzen eines zugehörigen elektronischen oder elektromechanischen Schlosses beinhaltet,

mit einem mechanischen Notschlüssel (30), der mit seinem Schlüsselschaft (31) in eine Aufnahme (27) des Gehäuses (20) einsteckbar und im Einsteckfall im Gehäuse gesichert ist, wobei der Notschlüssel (30) mit einer Verbreiterung (32) versehen ist,

d a d u r c h g e k e n n z e i c h n e t ,

dass das eine Gehäuseende (28) einen Ausbruch (40) aufweist, der wenigstens bereichsweise hinterschnitten (45, 46) ist und normalerweise, bei eingestecktem Notschlüssel (30) seine Herausziehbewegung (47) verhindert,

wobei der Schlüsselkopf sich in einer im wesentlichen formschlüssigen Haltelage (30) im Gehäuse (20) befindet

und dass der Notschlüssel in der Aufnahme (27) des Gehäuses (20) aus dieser Haltelage (30) in eine Löselage (30') verdrehbar ist, in welcher der Formschluss zwischen der Verbreiterung (32') und dem Ausbruch (40) in Richtung der Herausziehbewegung (47) des Notschlüssels beseitigt ist.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die Verbreiterung im Notschlüssel (30) aus der zur Schlüsselbetätigung dienenden Handhabe, wie einem Schlüsselkopf (32), besteht.

3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Ausbruch (40) wenigstens auf seiner einen Seite von einem Schenkel (41; 42) begrenzt ist und der Schenkel (41; 42) auf der dem Ausbruch (40) zugekehrten Innenflanke (43; 44) den Hinterschnitt (45; 46) aufweist

und dass der Schlüsselkopf (32) mit seiner der Innenflanke (43; 44) vom Gehäuseschenkel (41, 42) zugekehrten Kopfseitenfläche (33; 34) sich zum freien Kopfende (37) hin mindestens bereichsweise verjüngt und in der Haltelage (30) des Notschlüssels sich mindestens stellenweise am Gehäuseschenkel (41; 42) abstützt.

4.) Schlüssel nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Schlüsselkopf (32) und das Gehäuse (20) plattenartig (63; 64) ausgebildet sind, wobei die Plattenform jeweils zwei Mittenebenen (18, 38) bestimmt,

und dass die Mittenebene (18, 38) in der Haltelage zwar im wesentlichen miteinander fluchten, aber in der Löselage die beiden Ebenen (18, 38') zueinander drehversetzt (48) sind.

5.) Schlüssel nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass zwischen dem Schlüsselkopf (32) und dem Ausbruch (40) im Gehäuse (30) Rastelemente angeordnet sind, welche die Haltelage (30) gegenüber Drehungen (49) sichern.

6.) Schlüssel nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass in der Aufnahme des Gehäuses Drehanschläge (53; 54) vorgesehen sind, welche

die Position des Schlüsselschafts in der Haltelage (31) und/oder der Löselage (31') bestimmen und die Drehung (49) des Schlüsselschafts zwischen diesen beiden Lagen (31; 31') begrenzen.

7.) Schlüssel nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der Schlüsselschaft (31) ein Flachprofil (50) aufweist,

dass der Schlüsselkopf (32) des Notschlüssels (30) ein vorzugsweise symmetrisches Querschnittsprofil besitzt, welches die Mittenebene (38) im Schlüsselkopf (32) bestimmt,

und dass die Ebene (55) vom Flachprofil (50) des Schlüsselschafts (31) gegenüber der Mittenebene (38) im Schlüsselkopf (32) gegenüber jener Drehachse (19) verkippt (39) ist, welche die Drehung (49) des Notschlüssels zwischen der Haltelage (30) und der Löselage (30') bestimmt.

8.) Schlüssel nach Anspruch 7, dadurch gekennzeichnet, dass der Kippwinkel (39) zwischen der Flachprofilebene (55) des Schlüsselschafts (31) und der Mittenebene (38) vom Schlüsselkopf (32) annähernd gleich dem halben Drehwinkel (48) des Schlüsselschafts zwischen dessen Ruhelage (31) und Löselage (31') ist.

9.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Aufnahme (27) für den Schlüsselschaft (31) im Gehäuse aus einem Köcher (25) eines Innengehäuses besteht.

10.) Schlüssel nach Anspruch 9, dadurch gekennzeichnet, dass das Innengehäuse zwischen einer Oberschale (21) und einer Unterschale (22) eines mehrteiligen Gesamtgehäuses (20) angeordnet ist.

11.) Schlüssel nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass der Schenkel (41, 42) des Ausbruches (40) aus dem Endstück eines den Längsrand des Gesamtgehäuses (20) erzeugenden Gehäuseseitenteils (23) bzw. (24) gebildet wird.

12.) Schlüssel nach Anspruch 11, dadurch gekennzeichnet, dass seitliche Nocken (57) od. dgl. die Ober- und Unterschale (21, 22) des Gesamtgehäuses (20) mit dem bzw. den Gehäuseseitenteilen (43; 24) verbinden.

13.) Schlüssel nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass die Aufnahme (27) im wesentlichen in der Längsmitte (16) des Gehäuses (20) angeordnet ist

und dass die Längsmitte (16) eine Symmetrieachse des Gehäuses (20) bestimmt.

14.) Schlüssel nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, dass das hintere Gehäuseende (28) gegabelt (40) ist und

dass der Ausbruch im Gehäuse (20) aus einer Gabelöffnung (40) besteht, die beidseitig von zwei sie begrenzenden Gabelschenkeln (41; 42) eingefasst ist.

15.) Schlüssel nach Anspruch 14, dadurch gekennzeichnet, dass die beiden Gabelschenkeln (41; 42) an ihren einander zugekehrten Innenflanken (43; 44) jeweils einen zueinander gegensinnigen Hinterschnitt (45; 46) für den Schlüsselkopf (32) des Notschlüssels (30) aufweisen.

16.) Schlüssel nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass die elektronischen Bauteile (11) auf einer als flexibe Leiterplatte dienenden Folie (60) sitzen

und dass, - im Querschnitt gesehen -, diese Folie (60) in einer C-artigen Krümmung um die in Gehäuselängsrichtung (16) sich erstreckende Aufnahme (27) verläuft.

17.) Schlüssel nach Anspruch 16, dadurch gekennzeichnet, dass die Folie (60) stellenweise Dellen (61) aufweist, in denen Mikroschalter (17) positioniert sind,

und dass die Schaltglieder (62) an den Mikroschaltern (17) bei gekrümmter Folie (60) mit den Betätigungsstellen (12, 13, 14) auf der Außenseite des Gehäuses (20) ausgerichtet sind.

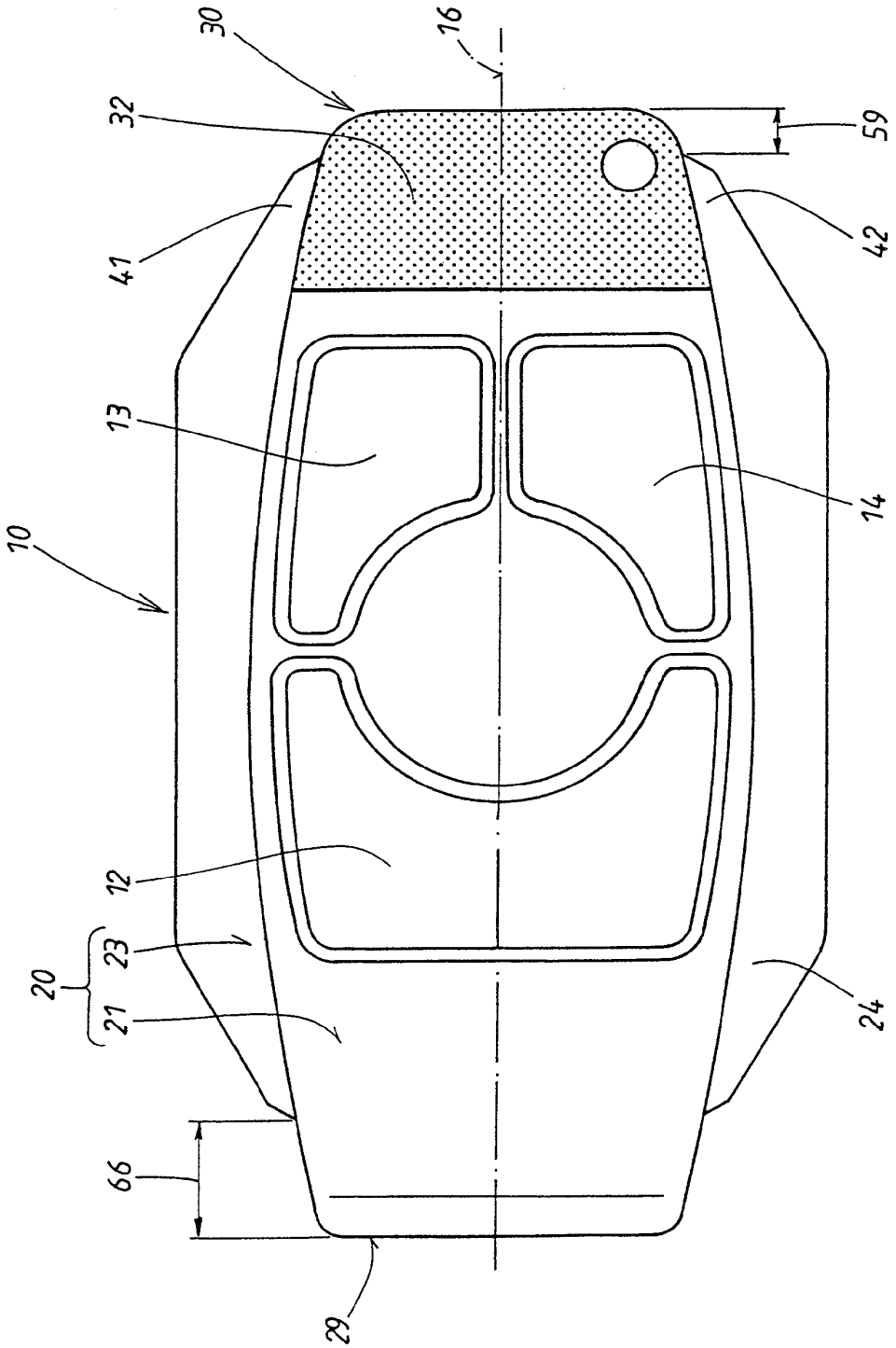


FIG. 1

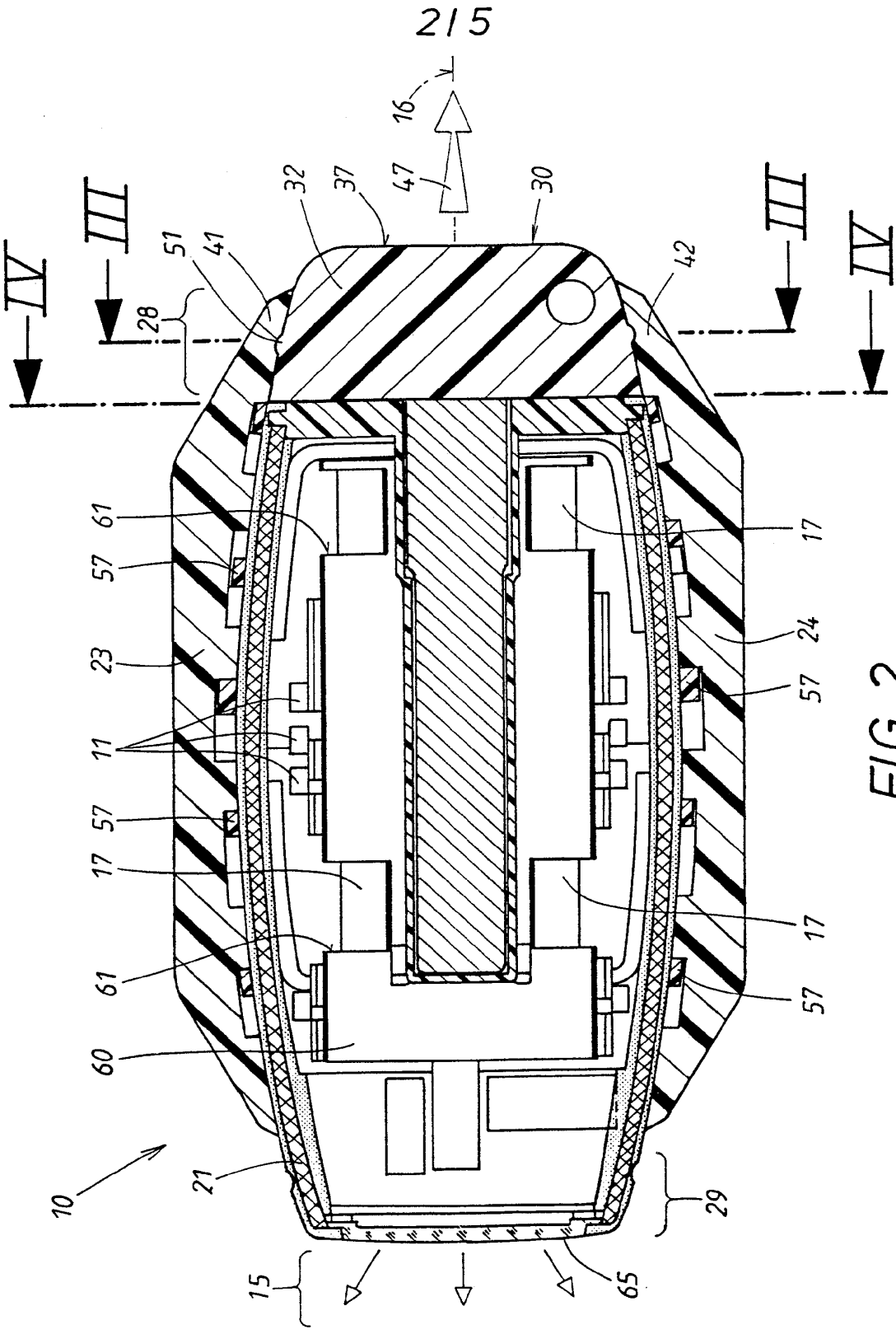

215
16
32
37
47
30
III
III
IV
IV
51
41
28
42
61
57
23
11
57
17
61
60
21
10
17
24
57
17
57
29
15
65

FIG. 2

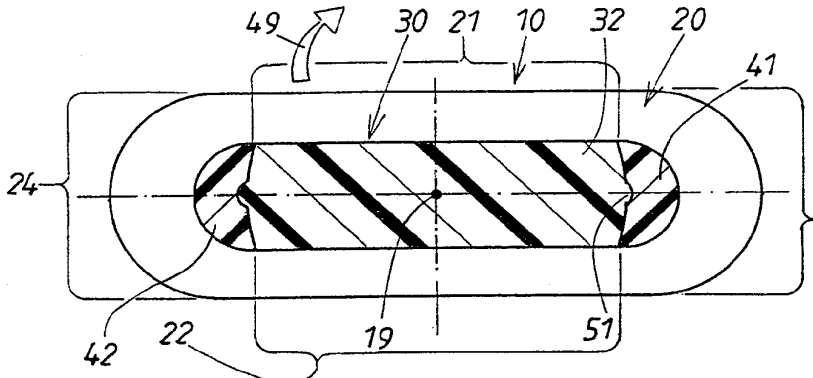


FIG. 3

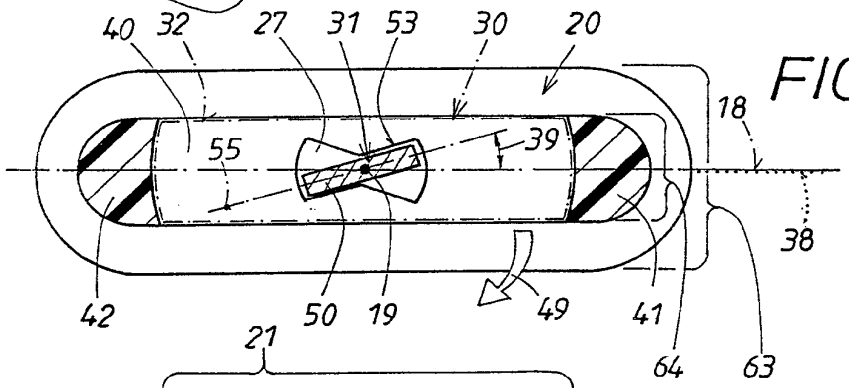


FIG. 4

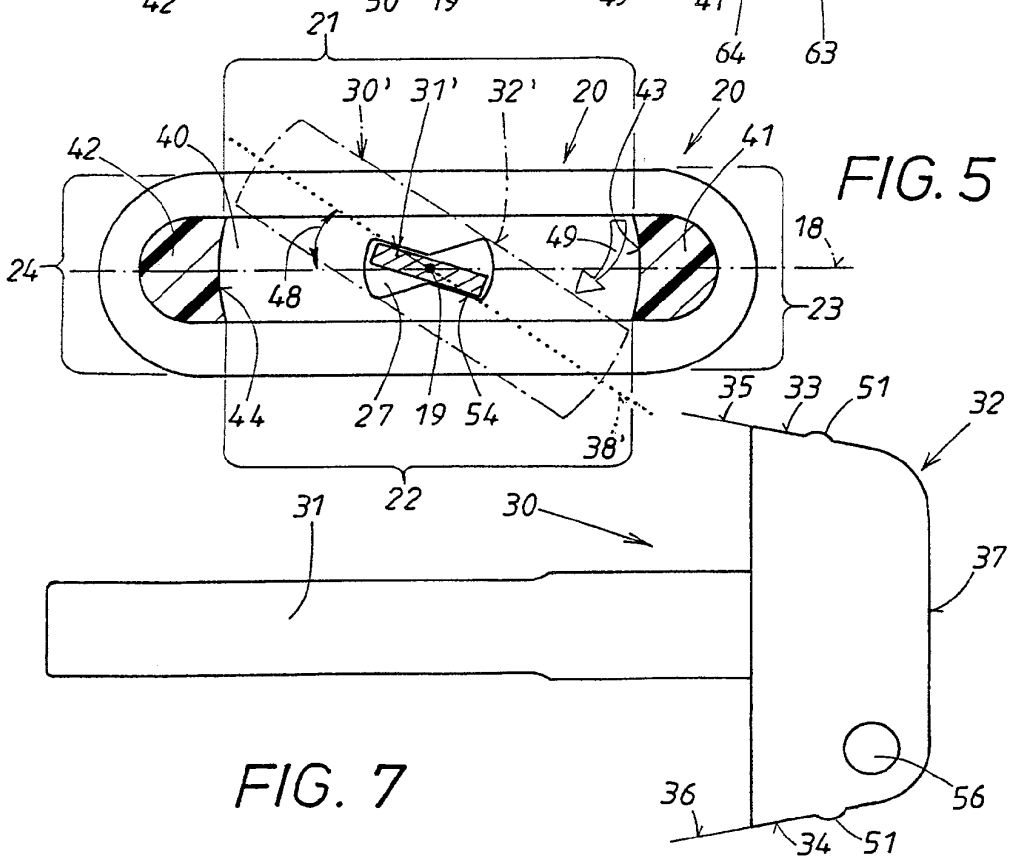


FIG. 5

FIG. 7

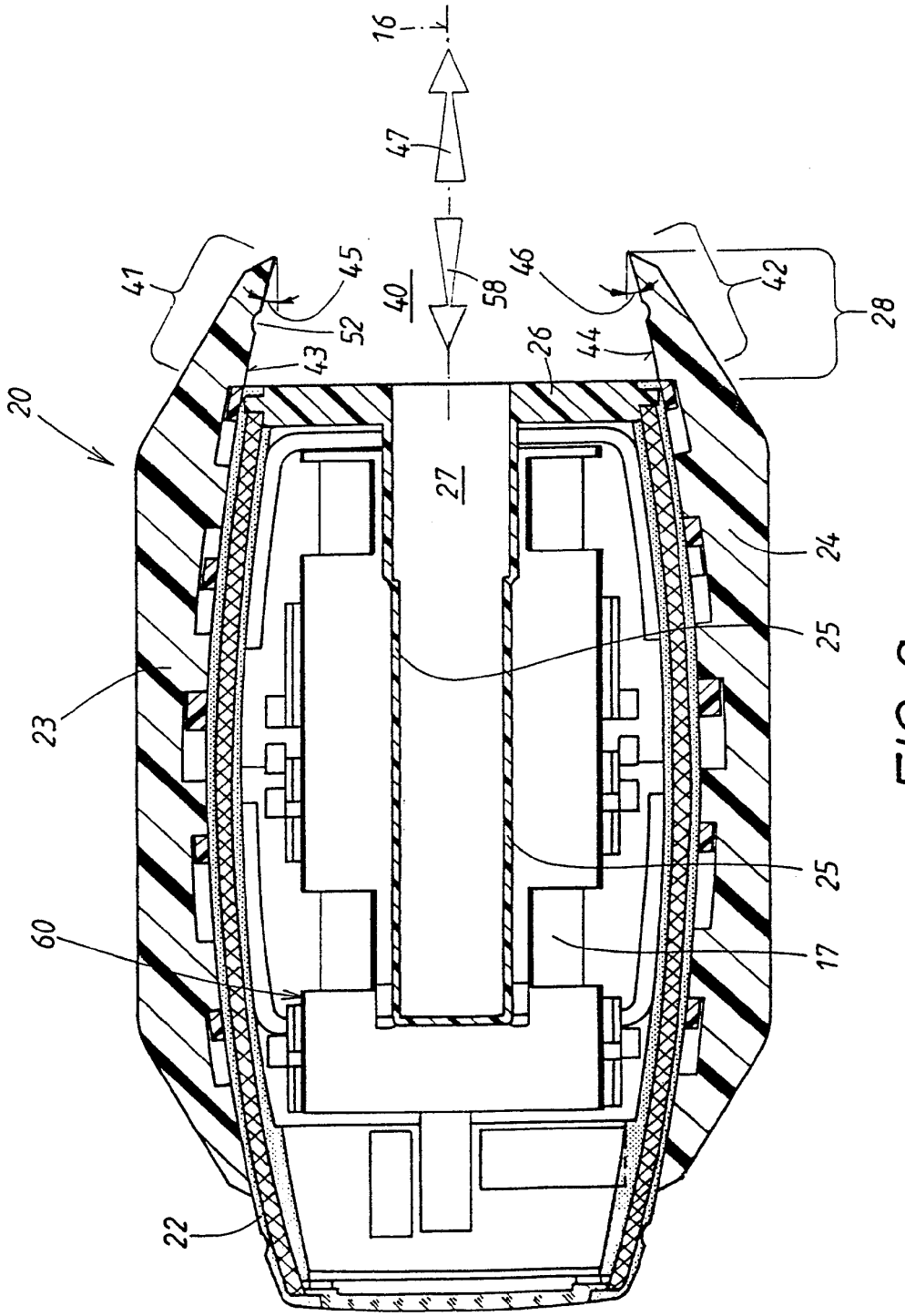


FIG. 6

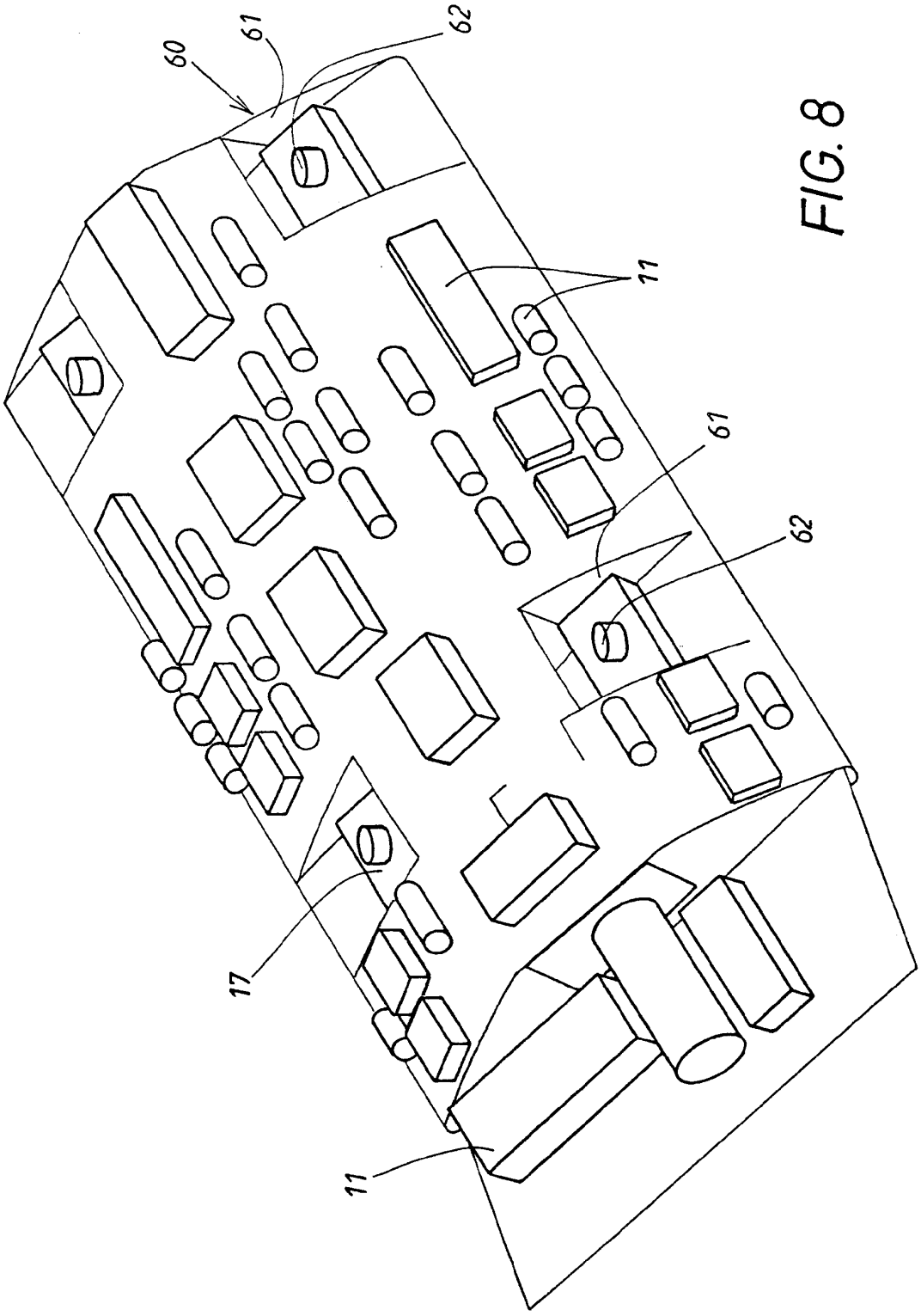


FIG. 8

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/EP 99/09251

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00 E05B19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 297 22 484 U (HUF HUELSBECK & FUERST GMBH &) 26 February 1998 (1998-02-26) figures page 2, last paragraph -page 3, paragraph 1 page 4, paragraph 1 - paragraph 2	1,2
A	DE 44 44 913 A (MARQUARDT GMBH) 22 June 1995 (1995-06-22) abstract; figures 1,3,5,7,8	1,2
A	DE 197 23 039 A (WISUSCHIL ANDREAS) 3 December 1998 (1998-12-03) abstract; figure 3 column 3, line 29 - line 37	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 February 2000	24/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Buron, E

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte. onal Application No
PCT/EP 99/09251

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 29722484 U	26-02-1998	NONE	
DE 4444913 A	22-06-1995	NONE	
DE 19723039 A	03-12-1998	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Int. ...ionales Aktenzeichen
PCT/EP 99/09251

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00 E05B19/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 297 22 484 U (HUF HUELSBECK & FUERST GMBH &) 26. Februar 1998 (1998-02-26) Abbildungen Seite 2, letzter Absatz -Seite 3, Absatz 1 Seite 4, Absatz 1 - Absatz 2	1,2
A	DE 44 44 913 A (MARQUARDT GMBH) 22. Juni 1995 (1995-06-22) Zusammenfassung; Abbildungen 1,3,5,7,8	1,2
A	DE 197 23 039 A (WISUSCHIL ANDREAS) 3. Dezember 1998 (1998-12-03) Zusammenfassung; Abbildung 3 Spalte 3, Zeile 29 - Zeile 37	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
16. Februar 2000	24/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Buron, E

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inte ...nales Aktenzeichen
PCT/EP 99/09251

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 29722484	U	26-02-1998	KEINE	
DE 4444913	A	22-06-1995	KEINE	
DE 19723039	A	03-12-1998	KEINE	

Formblatt PCT/ISA/210 (Anhang Patentfamilie)(Juli 1992)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00 — A1

(11) International Publication Number: **WO 00/42491**

(43) International Publication Date: 20 July 2000 (20.07.00)

(21) International Application Number: PCT/US00/00711

(22) International Filing Date: 12 January 2000 (12.01.00)

(30) Priority Data:

60/116,006	15 January 1999 (15.01.99)	US
09/281,017	30 March 1999 (30.03.99)	US
09/449,159	24 November 1999 (24.11.99)	US

(71) Applicant: RAINBOW TECHNOLOGIES, INC. [US/US]; 50 Technology Drive, Irvine, CA 92618 (US).

(72) Inventors: ABBOTT, Shawn, D.; 305 Pinnacle Ridge Place, RR12, Calgary, Alberta T3E 6W3 (CA). AFGHANI, Bahram; 891 Tia Juana Street, Laguna Beach, CA 92651 (US). SOTOODEH, Mehdi; 17 Paloma Drive, Mission Viejo, CA 92692 (US). DENTON, Norman, L., III; 34052 Capo–by–the–Sea, Dana Point, CA 92629 (US). LONG, Calvin, W.; 1260 Oakhaven Lane, Arcadia, CA 91006 (US). PUNT, Maarten, G.; 24942 Paseo Arboleda, Lake Forest, CA 92630 (US). ANDERSON, Allan, D.; 11158 Bertha Place, Cerritos, CA 90703 (US). GODDING, Patrick, N.; 22665 Shady Grove Circle, Lake Forest, CA 92630 (US).

(74) Agent: COOPER, Victor, G.; Gates & Cooper, Suite 1050, 6701 Center Drive, West, Los Angeles, CA 90025 (US).

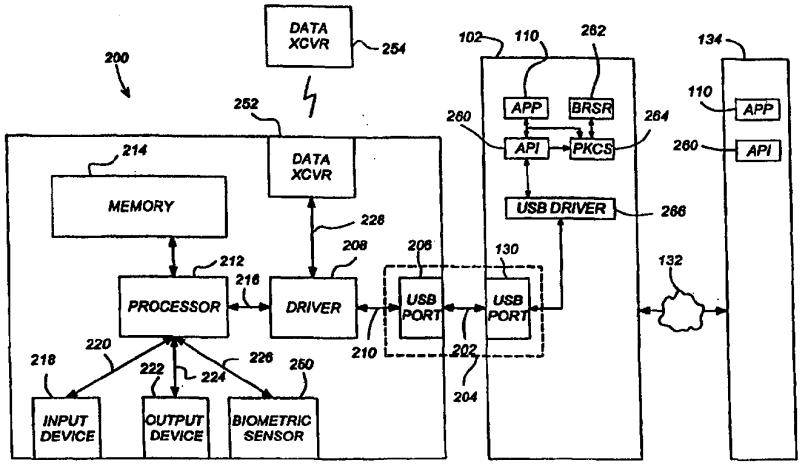
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, 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, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: USB–COMPLIANT PERSONAL KEY WITH INTEGRAL INPUT AND OUTPUT DEVICES



(57) Abstract

A compact, self–contained, personal key is disclosed. The personal key comprises a USB–compliant interface (206) releasably coupl eable to a host processing device (102); a memory (214); and a processor (212). The processor (212) provides the host processing device (102) conditional access to data storable in the memory (214) as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device (218) and an integral user output device (222). The input and output devices (218, 222) communicate with the processor (212) by communication paths (220, 222) which are independent from the USB–compliant interface (206), and thus allow the user to communicate with the processor (212) without manifesting any private information external to the personal key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

USB-COMPLIANT PERSONAL KEY WITH INTEGRAL INPUT AND OUTPUT DEVICES

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computer peripherals, and in particular to a personal key having input and output devices integrated therewith to provide for increased security.

2. Description of the Related Art

In the last decade, the use of personal computers in both the home and in the office have become widespread. These computers provide a high level of functionality to many people at a moderate price, substantially surpassing the performance of the large mainframe computers of only a few decades ago. The trend is further evidenced by the increasing popularity of laptop and notebook computers, which provide high-performance computing power on a mobile basis.

The widespread availability of personal computers has had a profound impact on interpersonal communications as well. Only a decade ago, telephones or fax machines offered virtually the only media for rapid business communications. Today, a growing number of businesses and individuals communicate via electronic mail

(e-mail). Personal computers have also been instrumental in the emergence of the Internet and its growing use as a medium of commerce.

While certainly beneficial, the growing use of computers in personal communications, commerce, and business has also given rise to a number of unique challenges.

First, the growing use of computers has resulted in extensive unauthorized use and copying of computer software, costing software developers substantial revenue. Although unauthorized copying or use of software is a violation of the law, the widespread availability of pirated software and enforcement difficulties have limited the effectiveness of this means of preventing software piracy.

Software developers and computer designers alike have sought technical solutions to attack the problem of software piracy. One solution uses an external device known as a hardware key, or "dongle" coupled to an input/output (I/O) port of the host computer.

While the use of such hardware keys is an effective way to reduce software piracy, to date, their use has been substantially limited to high value software products. Hardware keys have not been widely applied to popular software packages, in part, because the hardware keys are too expensive, and in part, because there is a reluctance on the part of the application program user to bother with a hardware key whenever use of the protected program is desired. Also, in many cases, the hardware keys are designed for use with only one application. Hence, where the use of multiple applications on the same computer is desired, multiple hardware keys must be operated at the same time.

While it reflects a tremendous advance over telephones and facsimile machines, e-mail also has its problems. One of these problems involves security. Telephone lines are relatively secure and a legally sanctioned way to engage in the private transmission of information, however, e-mails are generally sent over the Internet with no security whatsoever. Persons transmitting electronic messages must be assured that their messages are not opened or disclosed to unauthorized persons.

Further, the addressee of the electronic message should be certain of the identity of the sender and that the message was not tampered with at some point during transmission.

Although the packet-switching nature of Internet communications helps to minimize the risk of intercepted communications, it would not be difficult for a determined interloper to obtain access to an unprotected e-mail message.

Many methods have been developed to secure the integrity of electronic messages during transmission. Simple encryption is the most common method of securing data. Both secret key encryption such as DES (Data Encryption Standard) and public key encryption methods that use both a public and a private key are implemented. Public and private key encryption methods allow users to send Internet and e-mail messages without concern that the message will be read by unauthorized persons or that its contents will be tampered with. However, key cryptographic methods do not protect the receiver of the message, because they do not allow the recipient to authenticate the validity of the public key or to validate the identity of the sender of the electronic message.

The use of digital certificates presents one solution to this problem. A digital certificate is a signed document attesting to the identity and public key of the person signing the message. Digital certificates allow the recipient to validate the authenticity of a public key. However, the typical user may use e-mail to communicate with hundreds of persons, and may use any one of several computers to do so. Hence, a means for managing a number of digital certificates across several computer platforms is needed.

Internet commerce raises other challenges. Users seeking to purchase goods or services using the Internet must be assured that their credit card numbers and the like are safe from compromise. At the same time, vendors must be assured that services and goods are delivered only to those who have paid for them. In many cases, these goals are accomplished with the use of passwords. However, as Internet commerce becomes more commonplace, customers are finding themselves in a position where they must either decide to use a small number of passwords for all transactions, or face the daunting task of remembering multiple passwords. Using a small number of passwords for all transactions inherently compromises security, since the disclosure of any of the

passwords may lead to a disclosure of the others. Even the use of a large number of passwords can lead to compromised security. Because customers commonly forget their password, many Internet vendors provide an option whereby the user can be reminded of their password by providing other personal information such as their birthplace, mother's maiden name, and/or social security number. This feature, while often necessary to promote Internet commerce, severely compromises the password by relying on "secret" information that is in fact, publicly available.

Even in cases where the user is willing and able to keep track of a large number of passwords, the password security technique is often compromised by the fact that the user is inclined to select a password that is relatively easy to remember. It is indeed rare that a user selects a truly random password. What is needed is a means for generating and managing random passwords that can be stored and recalled for use on a wide variety of computer platforms.

Internet communications have also seen the increased use of "cookies." Cookies comprise data and programs that keep track of a user's patterns and preferences that can be downloaded from the Internet server for storage on the user's computer. Typically, cookies contain a range of addresses. When the browser encounters those addresses again, the cookies associated with the addresses are provided to the Internet server. For example, if a user's password were stored as a cookie, the use of the cookie would allow the user to request services or goods without requiring that the user enter the password again when accessing that service for the second and subsequent time.

However beneficial, cookies can also have their dark side. Many users object to storage of cookies on their computer's hard drive. In response to these concerns, Internet browser software allows the user to select an option so that they are notified before cookies are stored or used. The trouble with this solution is that this usually results in an excessive number of messages prompting the user to accept cookies. A better solution than this all-or-nothing approach would be to allow the storage and/or use of cookies, but to isolate and control that storage and use to comply with user-specified criteria.

Smartcard provide some of the above mentioned functionality, but smartcards do not present an ideal solution. First, personal keys are only valuable to the user if they offer a single, widely accepted secure repository for digital certificates and passwords. Smartcard readers are relatively expensive, and are not in wide use, at least in the United States, and are therefore unsuited to the task.

Second, smartcards do not provide for entering data directly into the card. This opens the smartcard to possible sniffer modules in malicious software, which can monitor the smartcard-reader interface to determine the user's personal identification or password information. This problem is especially problematic in situations where the user is using an unknown or untrusted smartcard reader. The lack of any direct input device also prevents the user from performing any smartcard-related functions in the relatively common situation where no smartcard reader is available.

Third, data cannot be accessed from the smartcard unless the smartcard is in the reader. This prevents the user from viewing data stored in the smartcard (i.e. a stored password) until a smartcard reader can be located. Given that smartcard readers (especially trusted ones) can be difficult to find, this substantially limits the usefulness of the card. Of course, the user may simply write the password down on paper, but this may compromise the security of all of the data in the card, and is inconsistent with the goal of providing a central, secure, portable repository for private data.

From the foregoing, it can be seen that there is a need for a personal key that allows the user to store and retrieve passwords and digital certificates without requiring the use of vulnerable external interfaces.

SUMMARY OF THE INVENTION

The present invention satisfies all of these needs with a personal key in a form factor that is compliant with a commonly available I/O interface such as the Universal Serial Bus (USB). The personal key includes a processor and a memory which implement software protection schemes to prevent copying and unauthorized use.

The personal key provides for the storage and management of digital certificates, allowing the user to store all of his digital certificates in one media that is portable from platform to platform. The personal key provides for the generation, storage, and management of many passwords, providing additional security and relieving the user from the task of remembering multiple passwords. The personal key provides a means to store cookies and other Java-implemented software programs, allowing the user to accept cookies in a removable and secure form-factor. These features are especially useful when the present invention is used in a virtual private network (VPN). The present invention can also be used for several applications

Because the personal key is capable of storing virtually all of the user's sensitive information, it is important that the personal key be as secure as possible. Hence, one embodiment of the personal key also comprises a biometric sensor disposed to measure biometrics such as fingerprint data. The biometric sensor measures characteristics of the person holding the key (such as fingerprints) to confirm that the person possessing the key is the actual owner of the key.

Since the personal key represents a single, secure repository for a great deal of the data the user will need to use and interact with a variety of computer platforms, it is also important that the personal key be able to interface (i.e., transmit and receive data) with a large variety of computers and computer peripherals. Hence, one embodiment of the personal key includes an electromagnetic wave transception device such as an infrared (IR) transceiver. This transceiver allows the personal key to exchange information with a wide variety of computers and peripherals without physical coupling.

The present invention is well suited for controlling access to network services, or anywhere a password, cookie, digital certificate, or smartcard might otherwise be used, including:

- Remote access servers, including Internet protocol security (IPSec), point to point tunneling protocol (PPTP), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), remote

access dial-in user service (RADIUS), terminal access controller access control system (TACACS);

- Providing Extranet and subscription-based web access control, including hypertext transport protocol (HTTP), secure sockets layer (SSL);
- Supporting secure online banking, benefits administration, account management;
- Supporting secure workflow and supply chain integration (form signing);
- Preventing laptop computer theft (requiring personal key for laptop operation);
- Workstation logon authorization;
- Preventing the modification or copying of software;
- Encrypting files;
- Supporting secure e-mail, for example, with secure multipurpose Internet mail extensions (S/MIME), and open pretty good privacy (OpenPGP)
- Administering network equipment administration; and
- Electronic wallets, with, for example, secure electronic transaction (SET, MilliCent, eWallet)

In one embodiment, the present invention comprises a compact, self-contained, personal token or key. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device; a memory; and a processor. The processor provides the host processing device conditional access to data storable in the memory as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device and an integral user output device. The input and output devices communicate with the processor by communication paths which are independent from the USB-compliant interface, and thus allow the user to communicate with the processor without manifesting any private information external to the personal key.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an exemplary hardware environment for practicing the present invention;

FIG. 2 is a block diagram illustrating selected modules of one embodiment of the present invention;

FIG. 3 is a diagram of the memory resources provided by the memory of the personal key;

FIG. 4 is a diagram showing one embodiment of how an encryption engine is used to authenticate the identity of the personal key or the application data stored therein;

FIG. 5 is a diagram illustrating the data contents of a file system memory resource of an active personal key that provides authentication and specific configuration data for several application;

FIG. 6 is a diagram presenting an illustration of one embodiment of the personal key;

FIGs. 7A-7C are diagrams showing one embodiment of the personal key having an input device including a first pressure sensitive device and a second pressure sensitive device, each communicatively coupled the processor by a communication path distinct from the USB-compliant interface;

FIGs. 8A-8C are diagrams presenting an illustration of another embodiment of the present invention;

FIG. 9 is a flow chart illustrating an embodiment of the present invention in which processor operations are subject to user authorization; and

FIG. 10 is a flow chart illustrating an embodiment of the present invention in which the PIN is entered directly into the personal key.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which is shown, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

Hardware Environment

FIG. 1 illustrates an exemplary computer system 100 that could be used to implement the present invention. The computer 102 comprises a processor 104 and a memory, such as random access memory (RAM) 106. The computer 102 is operatively coupled to a display 122, which presents images such as windows to the user on a graphical user interface 118B. The computer 102 may be coupled to other devices, such as a keyboard 114, a mouse device 116, a printer 128, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the computer 102.

Generally, the computer 102 operates under control of an operating system 108 stored in the memory 106, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module 118A. Although the GUI module 118A is depicted as a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system 108, the computer program 110, or implemented with special purpose memory and processors. The computer 102 also implements a compiler 112 which allows an application program 110 written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor 104 readable code. After completion, the application 110 accesses and manipulates data stored in the memory 106 of the computer 102 using the relationships and logic that are generated using the compiler 112. The computer 102 also comprises an input/output (I/O) port 130 for a personal token 200 (hereinafter alternatively referred to also as a personal

key 200). In one embodiment, the I/O port 130 is a USB-compliant port implementing a USB-compliant interface.

In one embodiment, instructions implementing the operating system 108, the computer program 110, and the compiler 112 are tangibly embodied in a computer-readable medium, e.g., data storage device 120, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive 124, hard drive, CD-ROM drive, tape drive, etc. Further, the operating system 108 and the computer program 110 are comprised of instructions which, when read and executed by the computer 102, causes the computer 102 to perform the steps necessary to implement and/or use the present invention. Computer program 110 and/or operating instructions may also be tangibly embodied in memory 106 and/or data communications devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

The computer 102 may be communicatively coupled to a remote computer or server 134 via communication medium 132 such as a dial-up network, a wide area network (WAN), local area network (LAN), virtual private network (VPN) or the Internet. Program instructions for computer operation, including additional or alternative application programs can be loaded from the remote computer/server 134. In one embodiment, the computer 102 implements an Internet browser, allowing the user to access the world wide web (WWW) and other internet resources.

Those skilled in the art will recognize that many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the present invention.

Architectural Overview

FIG. 2 is a block diagram illustrating selected modules of the present invention. The personal key 200 communicates with and obtains power from the host

computer through a USB-compliant communication path 202 in the USB-compliant interface 204 which includes the input/output port 130 of the host computer 102 and a matching input/output (I/O) port 206 on the personal key 200. Signals received at the personal key I/O port 206 are passed to and from the processor 212 by a driver/buffer 208 via communication paths 210 and 216. The processor 212 is communicatively coupled to a memory 214, which may store data and instructions to implement the above-described features of the invention. In one embodiment, the memory 214 is a non-volatile random-access memory that can retain factory-supplied data as well as customer-supplied application related data. The processor 212 may also include some internal memory for performing some of these functions.

The processor 212 is optionally communicatively coupled to an input device 218 via an input device communication path 220 and to an output device 222 via an output device communication path 224, both of which are distinct from the USB-compliant interface 204 and communication path 202. These separate communication paths 220 and 224 allow the user to view information about processor 212 operations and provide input related to processor 212 operations without allowing a process or other entity with visibility to the USB-compliant interface 204 to eavesdrop or intercede. This permits secure communications between the key processor 212 and the user. In one embodiment of the invention set forth more fully below, the user communicates directly with the processor 212 by physical manipulation of mechanical switches or devices actuatable from the external side of the key (for example, by pressure-sensitive devices such as buttons and mechanical switches). In another embodiment of the invention set forth more fully below, the input device includes a wheel with tactile detents indicating the selection of characters.

The input device and output devices 218, 222 may cooperatively interact with one another to enhance the functionality of the personal key 200. For example, the output device 222 may provide information prompting the user to enter information into the input device 218. For example, the output device 222 may comprise a visual display such as an alphanumeric LED or LCD display (which can display Arabic numbers and or letters) and/or an aural device. The user may be prompted to enter

information by a beeping of the aural device, by a flashing pattern of the LED, or by both. The output device 222 may also optionally be used to confirm entry of information by the input device 218. For example, an aural output device may beep when the user enters information into the input device 218 or when the user input is invalid. The input device 218 may take one of many forms, including different combinations of input devices.

Although the input device communication path 220 and the output device communication path 224 are illustrated in FIG. 2 as separate paths, the present invention can be implemented by combining the paths 220 and 224 while still retaining a communication path distinct from the USB-compliant interface 204. For example, the input device 218 and output device 222 may be packaged in a single device and communications with the processor 212 multiplexed over a single communication path.

In one embodiment of the invention, the present invention further comprises a second output device 222 that may be coupled to the USB-compliant interface 204 instead of being coupled to the processor via a communication path distinct from the USB-compliant interface 204. This embodiment may be used, for example, to indicate to the user that the personal key 200 has been correctly inserted into the host computer's USB port (for example, by providing an indication of a power signal of the USB-compliant interface). The second output device may also be used to show that data is passing to and from the host computer and the personal key 200 (for example, by providing an indication of a data signal from the USB-compliant interface).

The personal key has an interface including a USB driver module 266 communicatively coupled to an application program interface (API) 260 having a plurality of API library routines. The API 260 provides an interface with the application 110 to issue commands and accept results from the personal key 200. In one embodiment, a browser 262, such as the browser available from NETSCAPE, Inc. operates with the API 260 and the public key cryptographic standard (PKCS) module 264 to implement a token-based user authentication system.

While the portability and utility of the personal key has many advantages, it also has one important disadvantage...it can be lost or stolen. This is especially troublesome because the personal key 200 represents a secure repository for so much of the user's private data. For these reasons, the ultimate security of the information contained in the personal key 200 (but not necessarily the personal key 200 itself) is highly important.

Ultimately, the personal key 200 identifies the possessor to the outside world through the host computer 102, but there is no guarantee that the person in possession of the personal key 200 is the actual owner, because the personal key may have been lost or stolen. Security can be increased with the use of personal passwords and the like, but this solution is not ideal. First, the use of a single password raises the very real possibility that the password may have been compromised (after all, the thief may know the user, and hence, the user's password). Also, requiring the entry of a password multiple times increases the chance that malicious software executing in the host computer 102 or the remote computer 134 may eavesdrop on the password or personal identification. The use of multiple passwords is no solution because one of the reasons for using the personal key 200 is to relieve the user of the need to remember a number of passwords. Another problem with passwords is that hacking methods can be employed to circumvent the password protection or to discover the password itself. This is especially problematic in context of a personal key 200 which in most cases, depends on data entered in a host computer 120 peripheral such as the keyboard 114 and transmitted via the input/output port 130, rendering the personal key 200 vulnerable to hacking.

In one embodiment of the present invention, a biometric sensing device 250 is mounted on or in the personal key 200 to collect biometric data from the user when the user is holding the personal key 200. In one embodiment, the biometric sensing device 250 comprises a fingerprint sensor, which is capable of reading the user's fingerprints. The biometric sensor 250 may also include built-in processing to reduce the biometric data to data suitable for use by the processor 212. If necessary for the collection of biometric data, a light emitting or heat-emitting device can be placed

proximate to the biometric sensor to provide an active data measurement using light or heat.

The biometric sensor 250 is nominally placed where it can best measure the biometric data of interest. In the illustrated embodiment, the biometric sensor 250 is sized and disposed to collect data from the user's thumbprint when the user grips the personal key 200 to insert it into the host computer 102 I/O port 130. To facilitate measurement of the holder's fingerprint, the exterior surface of the personal key 200 can be designed to cradle the user's thumb in a particular place. Alternatively, to increase security, the exterior appearance of the personal key 200 may be designed to mask the presence of the biometric sensor 250 entirely.

The biometric sensor 250 can be advantageously placed in a position where it can be expected to collect known data of a predictable type, at a known time (for example, obtaining a thumbprint when the personal key 200 is plugged into the host computer I/O port 130). The personal key 200 accepts data from the biometric sensor 250 via biometric sensor communication path 226 to verify the identity of the person holding the key with no passwords to remember or compromise, or any other input. Thus, the biometric sensor 250 provides a personal key 200 with a heightened level of security which is greater than that which can be obtained with a biometric sensor or passwords alone. If necessary, the personal key 200 can be configured to recognize the host computer 102 it is plugged into, and using data thus obtained, further increase the security of the key.

The biometric sensor can also be used to increase the security of the personal key in other ways as well. For example, if the personal key were to be stolen, the biometric sensor can be used to measure the fingerprint of the thief. This data can be stored and retained until such time as the thief attempts to use the personal key to make a purchase, for example on the Internet. At this time, the personal key 200 can be programmed to contact (with or without visibility to the thief) a particular entity (such as an Internet site), where the fingerprint information (and any other relevant information) can be transferred to the appropriate authority. The personal key 200

may also perform this dial up and report function if a number of incorrect passwords have been supplied.

In one embodiment of the present invention, the personal key 200 also comprises a data transceiver 252 for communicating data with an external data transceiver 254. The data transceiver 252 is communicatively coupled to the processor 212, via the driver 208 and communication paths 216 and 228, and allows the personal key 200 to transmit and receive data via the transmission and reception of electromagnetic waves without exposing the data to the USB-compliant interface 204. Alternatively, the data transceiver 252 may be communicatively coupled directly to the processor 212.

In one embodiment, the data transceiver 252 comprises an infrared (IR) transceiver that can communicate with a number of commercially available peripherals with similar capability. This feature provides the personal key 200 another means for communicating with external peripherals and devices, even when the personal key 200 is already coupled to the I/O port 130 of the host computer 102.

In one embodiment, the personal key 200 also comprises a power source such as a battery or capacitive device. The power source supplies power to the components of the personal key to allow the data to be retained and to allow personal key functions and operations to be performed, even when disconnected from the host computer 102.

FIG. 3 is a diagram of the memory resources provided by the memory 214 of the personal key 200. The memory resources include a master key memory resource 312, a personal identification number (PIN) memory resource 314, an associated PIN counter register 316 and PIN reset register resource 318, a serial number memory resource 310, a global access control register memory resource 320, a file system space 324, auxiliary program instruction space 322, and a processor operation program instruction space 326. The processor operation program instruction space 326 stores instructions that the personal key 200 executes to perform the nominal operations described herein, including those supporting functions called by the application program interface 260 associated with the applications 110 executing in either the host computer 102 or the remote server 134. The auxiliary program

instruction space provides the personal key 200 with space to store processor 212 instructions for implementing additional functionality, if desired.

The master key is an administrative password that must be known by the trusted entity or program that will initialize and configure the personal key 200. For example, if the personal key 200 is to be supplied to a number of remotely located employees to enable access to private documents stored in a remote server through a VPN, the system administrator for the remote server may enter the master key (or change the key from the factory settings) before providing the key to the remotely located employees. The system administrator also stores the master key in a secure place, and uses this master key to perform the required secure operations (including, for example, authorization and authentication of the remote users).

In one embodiment, the master key can not be configured, reset, or initialized if the MKEY can not be verified first. Hence, if the master key is unknown the personal key 200 would have to be destroyed/thrown away or returned to the factory to be reset to the factory settings.

The PIN is an optional value that can be used to authenticate the user of the personal key 200. The PIN is initialized by the trusted administrator. Depending on how the personal key 200 initialization program is implemented and deployed, it is possible for the end user to set and/or update their PIN. The PIN may comprise alphanumeric characters or simply numbers.

The PIN can also be checked using an application program interface (API) call that transparently uses the two associated registers 316 and 318. The PIN counter resource 316 is a decrementing counter, while the PIN reset register resource 318 is used to store a limit that is used to reset the PIN counter 316 memory resource. The PIN count and limit registers 316 and 318 are used to prevent a rogue application or user from rapidly testing thousands of random PINs in an attempt to discover the PIN.

When the PIN is initialized, the decrementing counter register 316 is set to the value in the PIN reset register resource 318. Whenever a PIN verification fails the counter register 316 is decremented. When a PIN verification succeeds then the counter register is set to the limit value. When the decrementing counter register 316

reaches 0, no more PIN verifications are permitted until a trusted administrator resets the PIN counter register 316 to the limit value. For example if the PIN reset register resource 318 limit has been set to 3, then a user could fail PIN verification 3 times whereupon the PIN would be rendered useless until it is reset. The counter register 316 would be reset to 3 when a correct PIN was successfully verified.

The serial number is a unique factory installed serial number (SN). The serial number can be used to differentiate a single user from all other personal key 200 users.

The memory 214 of the personal key 200 also includes built in algorithm memory resources 302, including a MD-5 hash engine memory 304 for storing related processing instructions, an HMAC-MD5 authorization memory resource 306 for storing related processing instructions, and a random number generator memory resource 308 for storing processing instructions for generating random numbers. The random number generator can be used to generate challenges to be used when generating authentication digest results as well as to provide seeds to other cryptographic procedures. The MD-5 algorithm accepts as an input a message of arbitrary length, and produces a 128-bit "fingerprint" or "message digest" of the input as an output. In doing so, the algorithm scrambles or hashes the input data into a reproducible product using a high speed algorithm such as RFC-1321. The hashed message authentication codes (HMAC) can be used in combination with any iterated cryptographic hash function (e.g. MD-5) along with a secret key, to authenticate a message or collection of data. The personal key 200 integrates this method to provide a way for the end user or application data to be authenticated without exposing the secret key.

The present invention allows end user authorization using two security mechanisms. The first mechanism, which is discussed below, allows software running on the host computer 102 or the remote computer/server 134 to authenticate the personal key 200. This first mechanism uses a hashing algorithm and a mutually agreed upon secret value known to both the personal key 200 and the entity attempting to authenticate the personal key. The second mechanism, which is discussed later in

this disclosure, allows the personal key 200 to authenticate the user who is trying to use the personal key 200. This second mechanism uses a personal identification number (PIN) to help prevent unauthorized use or access in situations where the key has been lost or stolen. As set forth more fully below, the PIN can be entered directly in the personal key 200, thus increasing security by assuring that the PIN is never exposed external to the personal key 200.

FIG. 4 is a diagram showing one embodiment of how the HMAC-MD5 engine is used to authenticate the identity of the personal key 200 or the application data stored therein. Associated with the personal key 200 and executing either in the host computer 102 or the remote computer/server 134 is a personal key library of functions which are linked with an application executing in the host computer (e.g. application program 110) or in the remote computer/server 134. A hash algorithm 410 is implemented in both the application 110 and the personal key 200. Both the application 110 and the personal key 200 have access to a secret 406. The secret 406B is retained within the memory 214 of the personal key 200 in a location where it cannot be accessed without suitable permission. Typically, secret 406B is stored in the personal key 200 by the system administrator or some other trusted source. Hence, if the user of the personal key 200 is the entity that the application 110 thinks it is, the application's secret 406A and the personal key's secret 406B are the same. This can be verified by a hashing algorithm without exposing the secret. Similarly, if the user of the personal key 200 is not the entity that the application expects, secrets 406A and 406B will be different. This too can be verified by a hashing algorithm without exposing the secret.

A challenge is generated by the application 110, and provided to the hash algorithms 410 accessible to the application 110 and the hash algorithm implemented in the personal key 200. Each hash algorithm applies the challenge and the resident secret to generate a hashed output 412. If the hash algorithms were equivalent and each of the secrets 406A and 406B were the same, the resulting hashed output 412 or digest string in each case should be the same. If the digest strings 412A and 412B compare equal using logic 414 in the application, the personal key 200 is trusted.

Further, if the user authentication was verified, the user is trusted as well. One advantage in this authentication system is that the challenge 408 can be transmitted over untrusted media such as the Internet. The secret 406 remains coded in the application 110 or remote server 134 program and in the personal key 200 where it remains without being exposed to network sniffers/snoopers or potentially compromised user interfaces.

The file system memory resource 324 is fully managed within the application program interface library 260 in either the host computer 102 or the remote server 134. It provides a flexible system for storing, protecting, and retrieving personal key 200 data.

FIG. 5 is a diagram illustrating the data contents of a file system memory resource 324 of an active personal key 200 that provides authentication and specific configuration data for several applications. The master file (MF) 502 is the root directory and uses an identification (ID) of zero (0). The MF 502 may contain pointers 504A and 504B or other designations to data files 506A and 506B, as well as pointers 508A and 508B to directories 510 and 516. Directories and files are defined by an identification (1 → 0xFFFFFFFF for the directories, and 0 → 0xFFFFFFFF for files). The directories 510 and 516 also contain pointers (512A-512B and 518A-518B, respectively) to data files (514A-514B and 520A-520C, respectively).

Three file types are implemented, as shown in Table 1 below:

Type	Access
DATA	Any variable length string of unsigned characters
KEY	Strings that are used as input to cryptographic operations
CTR	Data files that have a decrementing counter (e.g. a counter of 16 bits). The counters range from 0 to XFF and are used to limit the number of times a data file can be read.

Table 1

These file types can be controlled on a per-file basis, according to Table 2 below:

Access Types	File Types		
	DATA	KEY	CTR
Read	Control	Never - no control	Control
Write	Control	Control	Control
Crypt	Always - no control	Control	Always - no control

Table 2

The read and write access type controls govern the transfer of files in the personal key 200 to and from the application 110. The crypt access type is used with KEY file types for performing cryptographic operations including the computation of hash values, encrypting, or decrypting data. When set, the controls defined in Table 2 can have one of four attributes listed in Table 3 below:

Attribute	Access
ALWAYS	Always granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
NEVER	Never granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
PIN	Access is granted if and only if the proper PIN has been supplied to the personal key 200, and PIN verification is successful (user authentication).
MKEY	Access is granted if and only if the proper master key (MKEY) has been provided to the personal key 200, and master key verification is successful (super user or security officer authentication).

Table 3

A global access control register 320 applies to the entire scope of the personal key 200 file system. Nominally, the global access control register 320 is an 8-bit value that is divided into two global access controls as shown in Table 4 below:

Global Access Type	Global File System Access
Create	Control
Delete	Control

Table 4

The create and delete global access types can have one of the four attribute values shown in Table 5 below. The create and delete global controls are enforced by the CreateDir, CreateFile, DeleteDir, DeleteFile, and DeleteAllFiles API calls described in Table 5 below.

Attribute	Access
ALWAYS	Always granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
NEVER	Never granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
PIN	Access is granted if and only if the proper PIN has been supplied to the personal key 200, and PIN verification is successful (user authentication).
MKEY	Access is granted if and only if the proper MKEY has been supplied to the personal key 200, and PIN verification is successful (super user or security officer authentication).

Table 5

Table 6 is an alphabetical listing of personal key 200 APIs 260 in the library. In Table 6, "D" indicates a device-related function, "F" denotes a file system related

function, "A" denotes an administrative function, and "C" denotes a cryptographic function.

Name	Description	D	F	A	C
CloseDevice	Close access to the personal key	√			
CloseFile	Close selected file		√		
CreateDir	Create a directory in the personal key memory		√	√	
CreateFile	Create a file in the personal key memory		√	√	
Decrement	Decrement a CTR type file		√		
DeleteAllFiles	Reformat file space		√	√	
DeleteDir	Delete directory		√	√	
DeleteFile	Delete file		√	√	
Dir	Return directory and file information		√		
GetAccessSettings	Return current global create/delete			√	
GetChallenge	Returns a 64-bit random number			√	√
GetSerialNumber	Read unique serial number	√		√	
HashToken	MD5 hash the selected file or currently open file - two modes are supported (1) XOR hash and HMAC hash		√		√
HMAC_MD5	This function is a wrapper for performing HMAC-MD5 using the HashToken function in the HMAC mode. It computes MD5 without exposing the key.		√		√

Name	Description	D	F	A	C
LedControl	Control the output device, including turning an LED or other output device on or off	√			
ModifyMasterKey	Update/Modify master key			√	
ModifyPIN	Update/Modify PIN			√	
OpenDevice	Open one of 32 potential personal keys	√			
ReadFile	Return contents of selected file		√		
ResetDevice	Reset to power-on state	√		√	
SelectFile	Open a file		√		
SetAccessSettings	Update global create/delete access settings			√	
VerifyMasterKey	Verify the master key provided as an argument is the master key stored in the personal key			√	
VerifyPIN	Verify that the PIN provided as an argument is the PIN stored in the personal key (user authentication)			√	
VerifyPIN2	An alternative command used to verify the user PIN without exposing the PIN externally to the personal key 200. This command is issued without the PIN as an argument, and the personal key 200 returns a response indicating whether the PIN entered by the user on the				√

Name	Description	D	F	A	C
	input device 218 matches that of the stored PIN in the memory 214.				
WriteFile	Write contents to the selected file	√			
MD5_Hash	Hash routine: wrapper (provided in API library and not implemented in personal key)				√
MD5Final	Finish computation and return digest (provided in API library and not implemented in personal key)				√
MD5Init	Initialize message digest context (provided in API library and not implemented in personal key)				√
MD5Update	Update message digest context (provided in API library and not implemented in personal key)				√

Table 6

Exemplary Application to a Virtual Private Network

Using the foregoing, the personal key 200 and related APIs 260 can be used to implement a secure document access system. This secure document access system provides remote users access to secret encrypted documents over the Internet to company employees. The system also limits the circulation of secret encrypted documents so that specified documents can be read only a limited number of times.

The application program 110 used for reading documents is linked with the personal key API 260 library to allow document viewing based on the information in the personal key 200. A trusted administrative program controlled by the master key

can be used to set up the personal key 200 (by storing the appropriate information with the associated security control settings) for a wide range of employees.

The personal key 200 and the API 260 library can be used to authenticate document viewers and administrators, to supply keys for decryption and encryption of documents, to provide a list of viewable documents, and to enforce document access rights and counters.

The foregoing can be implemented in a number of programs, including an administrative initialization program to set up the personal keys 200 before delivery to the employees (hereinafter referred to as SETKEY), a document encryption and library update program (hereinafter referred to as BUILDDOC), a viewer application that authenticates the user and the personal key 200 (hereinafter referred to as VIEWDOC), and a library application which authenticates the user and updates the personal key (hereinafter referred to as LIBDOC).

The SETKEY program is used to setup personal keys received from the factory for individual users. Document names, access counters, a PIN, and a hash secret are loaded into the personal key 200. Depending on the employee's security clearance, specific documents can be configured for viewing. For sake of clarification the following symbolic names are used in the discussion below:

DOCFilename -iKey data file that holds the document file name

DOCSecret -iKey data file that holds a secret used to make encryption/decryption keys

First, the SETKEY program gains access to the personal key 200 by issuing an OpenDevice command. The VerifyMasterKey command is then issued to open the personal key 200 to master access. A Dir command is used in a loop to obtain and verify the status of the personal key 200. The comments are compared to the contents of a factory-fresh key, and one of several states is determined. If the key is factory fresh, the personal key is initialized. A VIEWDOC directory and file set is then created. An employee database can then be accessed and used to determine the type and extent of the access that is to be granted to each employee. Depending on the security clearance of each employee, one of several types of directory and file sets can

be created. The global create and delete access types are then set to the master key using the SetAccessSettings command. The DOCFilename database is then loaded in the personal key 200, and the CreateDir and CreateFile APIs 260 are used as required to create and allocate directories and files. The SelectFile, WriteFile, and CloseFile API commands are used to load the files and the secret. Depending on whether access is to be limited to a particular number of occasions, the DATA or CTR file types are used.

The BUILDOC program is used to accept new documents into the secure access library. Using information from the personal key 200, encryption keys are generated that are used by a document encryption engine in the personal key 200.

The BUILDOC program is a stand-alone application that runs on trusted systems within the secure walls of the organization. It requires validation of the master key. It uses the personal key 200 to create an encryption key for each document file name.

First, the HashToken API 260 with the XOR option is used to hash together the DOCFilename, block number (computed by the BUILDOC program as it reads and encrypts the document), DOCSecret. The block number is calculated by the BUILDOC program as it reads and encrypts the document. The resulting MD5-XOR digest is used as the encryption key that is used by the encryption engine in the BUILDOC application. Then, the CreateFile, SelectFile, WriteFile, and CloseFile APIs 260 along with the HashToken in XOR mode are used on each document that is to be added to the secure document library.

The VIEWDOC program is a web browser 262 plug-in application allows the user to open, decrypt, an view the document based on his/her personal key 200 based document access codes. If desired, the view counters for some types of documents can also be decremented in the VIEWDOC program. The VIEWDOC program does not require file saving or forwarding, screen scraping, and printing.

The VIEWDOC program validates the user and uploads and decrypts the documents. It uses the VerifyPIN command API 260 to authenticate the user. The

user can then view the documents listed in the personal key 200 directory as long as the personal key 200 remains communicatively coupled to the USB port 130.

A message facility, such as the message facility used in the WINDOWS operating system (WM_DEVICECHANGE) can be used to determine if the key has been removed. The Dir, SelectFile, ReadFile, and CloseFile command APIs 260 are used to determine which documents can be read. The HashToken with the XOR mode API 260 along with DOCSecret, DOCFilename, and the document block numbers are used to create the decryption key on a per block basis. When the DOCfilename is of file type CTR, the CTR is decremented using the Decrement command API 260. In one embodiment, to reduce complexity, the CTR field is not hashed, but merely managed by VIEWDOC.

The LIBDOC program provides an administrative function that is a subset of SETKEY. It allows a secure document librarian to grant access to documents based upon information stored in the personal key 200. The net effect is that the trusted librarian can update the personal key 200 based list of documents that can be viewed.

The LIBDOC program updates the list of DOCFilenames on a per-personal key 200 basis. After verifying the master key with VerifyMasterKey command API 260 and looking the user name up in the employee data base, the current set of DOCFilenames are updated using the SelectFile, WriteFile, and CloseFile command APIs 260.

Using the foregoing, employees worldwide can carry a personal key 200 loaded with their local database of file names. Individual departments do not have to rely on MIS procedures to restrict who has access to documents. The personal keys 200 of department members can be updated using the LIBDOC program as required. Documents can be decrypted and viewed by the employees only if the personal key 200 secret is correct. The personal secret remains secure because it is never revealed outside of the personal key 200. A simple form of metering can also be used to reduce the number of copies of documents that can be used to reduce the number of copies of documents that can be viewed.

FIG. 6 is a diagram presenting an illustration of one embodiment of the personal key 200. The personal key 200 comprises a first housing member 602 and a second housing member 604. The first housing member 602 is sized and shaped so as to accept a circuit board 606 therein.

The first housing member 602 comprises a plurality of bosses 624, which, when inserted into each respective hole 640 in the second housing member 604, secures the first housing member 602 to the second housing member 604. The first housing member 602 and the second housing member 604 also each comprise an aperture 628, which allows the personal key 200 to be affixed to a key chain.

The circuit board 606 is held in position by a plurality of circuit board supports 608. The circuit board 606 comprises a substantially flat circuit connection surface 610 on the periphery of the circuit board 606 for communicative coupling with the host processing device or computer 102 via conductive pins. Circuit connection surface 610 allows communication with a processor 212 mounted on the circuit board 606. The processor 212 comprises memory and instructions for performing the operations required to implement the functionality of the personal key 200 as disclosed herein. The processor is communicatively coupled with a memory 214 on the circuit board to store and retrieve data as required by processor 212 instructions. In the illustrated embodiment, the circuit board 606 also comprises an output device 222 such as a light emitting device 616, e.g. light emitting diode (LED), which provides the user of the personal key 200 a visual indication of the operations being performed by the personal key 200. This is accomplished, for example, by emitting light according to a signal passing from the host computer 102 to the personal key 200. The light emitting device could also comprise a liquid crystal display (LCD) or other device providing a visual indication of the functions being performed in the personal key or data passing to or from the personal key 200.

The energy from the light emitting device 616 is presented to the user in one of two ways. In the embodiment illustrated in FIG. 2, the light emitting device 616 is disposed through a light emitting device orifice 644 in the second housing member 604. In this design, the personal key 200 can be sealed with the addition of a small

amount of epoxy or other suitable material placed in the light emitting device orifice 644 after assembly.

In another embodiment, the light emitting device 616 does not extend beyond the interior of the housing 602, 604, and remains internal to the personal key 200. In this embodiment, at least a portion of the first housing 602 or the second housing 604 is at least partially translucent to the energy being emitted by the light emitting device 616 at the bandwidths of interest. For example, if the light emitting device 616 were a simple LED, the second housing 604 can be selected of a material that is translucent at visual wavelengths. One advantage of the foregoing embodiment is that the LED can be placed where it does not allow electromagnetic discharges and other undesirable energy to the circuit board 606 or any of the components disposed thereon. This is because no part of the LED, even the surface, is in contact with the user's hand at any time.

While the foregoing has been described with a single light emitting device 646, the present invention can also advantageously embody two or more light emitting devices, or devices emitting energy in other wavelengths. For example, the foregoing can be implemented with a three color LED (red, yellow and green), or three one-color LEDs to transfer personal key 200 information to the user.

In addition to or as an alternative to the foregoing, information regarding the operation of the personal key 200 is provided by an aural transducer such as a miniaturized loudspeaker or piezoelectric transducer. Such aural information would be particularly beneficial to users with limited or no vision. For example, the aural transducer can be used to indicate that the personal key 200 has been inserted properly into the host computer 120 I/O port 130.

An aural transducer may also be used to provide alert information to the user. This is particularly useful in situations where the user is not expecting any input or information from the key. For example, if the personal key 200 or related device is engaged in lengthy computations, the aural transducer can indicate when the process is complete. Also, the aural transducer can indicate when there has been an internal fault, when there has been an attempt to compromise the security of the key with

infected or otherwise harmful software instructions, or to prompt the user to take an action such as providing an input to the key 200.

Further, it is envisioned that as the use of personal keys 200 will become widespread, it will be beneficial to incorporate the functions of other devices within the personal key. For example, a device such as a paging transceiver can be incorporated into the personal key to allow the user to be summoned or contacted remotely. Or, the personal key 200 may be used to store programs and instructions such as the user's calendar. In this application, the personal key 200 can be used to remind the user of events on the calendar, especially in conjunction with the LCD display discussed above. The aural transducer can be operated at a wide variety of frequencies, including minimally audible vibrational frequencies. This design is particularly beneficial, since the personal key is small enough to be placed on the user's key ring, where it will be in pocket or purse for lengthy periods of time where it cannot be seen or easily heard.

FIGs. 7A-7C are diagrams showing one embodiment of the personal key 200 having an input device 218 including a first pressure sensitive device 702 and a second pressure sensitive device 704, each communicatively coupled the processor 212 by a communication path distinct from the USB-compliant interface 204.

FIG. 7A illustrates an embodiment of the personal key 200 in which an output device 222 such as an LED or LCD display 706 is communicatively coupled to the processor 212 by a second communication path distinct from the USB-compliant interface 204. In this embodiment, input to the personal key processor 212 may be supplied by depressing a combination of the pressure sensitive devices 702, 704, optionally as directed by the output device 222.

In an embodiment illustrated in FIGs. 7B and 7C, the pressure sensitive devices 702 and 704 are simple mechanical push switches communicatively coupled to the processor 212 via traces on the circuit board 606. In this case, the switches 702 and 704 may be actuated by depressing a button surface that extends through apertures 708 and 710 in the second housing member 604. FIG. 7B also shows a window 712 permitting viewing of the output device 706 display.

FIG. 7C shows the exterior appearance of this embodiment of the personal key 200 when the first housing member 602 and the second housing member 604 are assembled.

In another embodiment of the present invention, the pressure switches 702 and 704 do not extend to the exterior of the personal key 200. Instead, the personal key 200 is configured so that pressure may be exerted on the pressure sensitive switches 702 and 704 without requiring any portion of the switches to extend to the exterior of the personal key 200. For example, in one embodiment, at least a portion of the exterior surface of the personal key 200 is sufficiently flexible to permit pressure exerted on the outside surface of the key 200 to actuate the switches therein. Alternatively, the first housing member 602 and the second housing member 604 may be hinged to allow pressure to be applied to the switch. In another embodiment, the thresholded output of a pressure sensitive device such as a strain gauge is used to indicate user input to the personal key.

The foregoing pressure sensitive devices 702 and 704 may be used as follows. In one embodiment, the two pressure sensitive devices 702 and 704 is used to enter alphanumeric information. Here, pressure can be applied to the first pressure sensitive device 702 to select the desired character. To assist the user, the currently selected character can be displayed on the output device 222. When the user is satisfied with the selected character, applying pressure to the second pressure sensitive device may indicate that the currently displayed character should be entered (thus providing an "enter" function). This process may be repeated until all of the characters of the user input (e.g. a user password or personal identification number (PIN) has been entered. The end of the user input can be signified by repeated application of pressure to the second pressure sensitive device 702, and confirmed by the output device 222. An aural transducer can be used alone or in combination with a visual display to indicate the character, to indicate an error, or to indicate when the user input process has been completed.

The foregoing pressure sensitive devices may also be used to provide a binary input to the personal key 200. For example, the user's PIN or password can be

entered by applying pressure to the first pressure sensitive device 702 and the second pressure sensitive device 704 in the proper order in rapid succession. In this way, a user password or PIN defined as "10100010111" may be entered by depressing the first pressure sensitive device 502 to indicate a "0" and the second pressure sensitive device 704 to indicate a "1."

FIGs. 8A-8C are diagrams presenting an illustration of another embodiment of the present invention. In this embodiment, the input device 218 comprises an edge exposed wheel 802 coupled to the processor by the input device communication path 808. In this embodiment, the user provides an input by urging the wheel 802 through a series of tactile positions identifying input characters. When the desired input character is either shown on the output device 222 or on the wheel 802 itself, the user can indicate the character as a user input by urging the wheel 802 toward the centerline of the personal key 200. This process can be repeated for a series of input characters, until all of the desired characters are provided. The user can also indicate that no more input will be provided by urging the wheel 802 toward the center of the personal key multiple times in rapid succession, or by selecting an input tactile position on the wheel 802 and depressing the wheel 802.

Security Features Using the Input and Output Devices

The input device 218 and output device 222 of the present invention can be advantageously used to enhance the security of the personal key 200. For example, when connected to the host computer 102, the personal key 200 can be used to authorize transactions with a remote computer/server 134 communicatively coupled to the host computer 102 via a communication medium 132 such as a dial-up network, the Internet, LAN, or WAN. Malicious software, which can be executing in the remote computer/server 134 or the host computer 102, can send anything it wants to the personal key 200 for authorization without the knowledge or permission of the user. Without some sort of user input device 218, the personal key 200 can authorize transactions without the user's knowledge that the holder cannot repudiate. Such transactions may include, for example, payment and legally binding signatures.

Although a personal identification such as the personal identification number (PIN) is required to log on and activate the personal key 200, the personal key 200 ordinarily remains active once the PIN has been entered. Hence, the personal key 200 will perform any action for any application, without notice to, or authorization by the user.

To ameliorate this problem, one embodiment of the present invention utilizes a "squeeze to sign" authorization technique, in which some direct user action is required to authorize the use of identified secret values stored in the personal key 200. For instance, if a private key (such as the secret 406) or PIN stored in the memory 214 of the personal key 200 is identified as requiring a "squeeze to sign" authorization, firmware executing in the processor 212 of the personal key 200 requires direct user input via the input device 410 or the data transceiver 252 before honoring any request from the host computer 102 or the remote computer/server 134 that involves the use of the private key or personal information. Ordinarily, the private key and/or other personal information is designated as requiring direct authorization by an associated value or flag in the memory 214. Such data may also be designated as "use-only" indicting that the data cannot be read directly from the key under any circumstances. The data may be shared with no other entity (as would often be the case with a PIN), or may be a value shared with the trusted entity and used for authorization, such as the secret 406. For example, private keys can be used as the secret 406 to perform authorization via hash functions. In such cases, the secret value 406 is typically a shared secret such as a DES key or a password. Since secret values 406 can be stored in the memory 214 of the personal key 200, before distributing the personal key 200 to the user, the secret value 406 need not be made available in plaintext form at any time.

Typically, each time a user connects to an SSL secured web site that supports client authentication, a browser 262 calls middleware such as one of the APIs 260 or the PKCS 264, which commands the personal key 200 to encrypt a challenge value with the user's secret private key 406B (stored in the personal key memory 214). Assuming the user's PIN is already stored in the personal key 200, thus authenticating the user to the personal key 200, it still remains to authenticate the key to the secure

web site. In this case, access to the user's secret private key is required, and the output device 222 integrated with the personal key 200 may activate to indicate that a command that requires access to the private key has been invoked, and that the user needs to authorize this access. In one embodiment of the present invention this is accomplished by blinking a visual output device (such as an LED or LCD display), or by beeping an aural device. In another embodiment of the present invention, the middleware (either the API 260 or the PKCS 264) activates the display 122 attached to the computer 102, indicating that the user must authorize access to the private key before processing can proceed. An input device 218 in the personal key 200 such as the wheel 802 or one of the pressure sensitive devices 702 and 704 can then be actuated by the user to indicate that the user has authorized access to the private key. No authorization is granted if the personal key 200 is removed from the I/O port 130, or a "cancel" button presented on the display 122 is selected to refuse the on-screen dialogue. Access to the private key (in the example above, to perform the hash function) is granted if the user authorizes as such. The "squeeze to sign" concept thus makes it less likely that malicious software will be able to use the secret 406B without the user's consent or knowledge.

Malicious software may monitor the interface between the personal key 200 and the host computer 102 to capture the value of user's PIN. Although the PIN cannot be read directly, it is possible for the malicious software to examine both the VerifyPIN command described in Table 6 (and it's argument) and the response from the personal key 200. If the response indicates that the proper PIN was provided as an argument to the VerifyPIN command, the malicious software can determine the PIN itself. The foregoing can also be applied to further safeguard the user's PIN instead of the secret 406B. For example, if a sniffer module in malicious software in the host computer has been able to access the user's PIN, when it attempted to use that PIN in a context the user did not expect, the user would be alerted to the fact that the PIN had been compromised.

FIG. 9 is a flow chart illustrating an embodiment of the present invention in which processor 212 operations are subject to user authorization. First, the API 260

issues 902 a command that invokes a processor 212 operation. The command is transmitted via the USB-interface 204 to the personal key 200. The processor 212 accepts the command, as shown in block 904. The personal key 200 then determines whether the invoked processor command is one that requires authorization. This can be accomplished by storing information in the memory 214 of the personal key indicating which processor commands require authorization. For example, this can be implemented in a map stored in the memory 214, a plurality of flags, where it may be customized for each user, or the information can be stored in the processor 212 firmware or similar location so that the mapping cannot be altered. In one embodiment, different levels of authorization are implemented for different processor commands (e.g. a write command may require authorization, whereas a read command may not).

In another embodiment, authorization may be premised on data instead of the invoked command, or on a combination of the invoked command and data. For example, the present invention may be configured to require authorization any time the PIN is accessed in any way, or when the PIN is read from the memory 214 of the personal key 200, but not when other data is read, or when the PIN is written to the personal key 200. This may be accomplished, for example, by determining which data stored in the memory 214 is affected by the processor operation, and determining whether the data affected by the processor operation is associated with an identification designating the data as private information.

Using one of the output devices 222, the data transceiver 252, or the display 122 coupled to the host computer, the personal key 200 may then prompt the user to authorize the processor operation, as shown in block 906. This may be accomplished by flashing a display device such as an LED or LCD, by activating an aural transducer, or by performing both operations. If desired, the user may be prompted first with a display device, and if the authorization is not forthcoming within a specified period of time, the aural transducer may be activated.

To expose the prompting operation as little as possible to malicious software or other intrusive activity, the prompt is preferably performed using a communication

path entirely distinct from the communication path between the personal key 200 and the host computer 102 (in the illustrated example) the USB-interface 204. To further increase security, the illustrated embodiment prompts the user with the output device 222 via a communication path which not manifested externally from the personal key in any way that is visible to the malicious software, and is hence not subject to tampering.

Next, the user provides an input signaling authorization of the operation 910. This can be performed using a variety of input devices, such as the mouse 116, or keyboard 114, but is preferably performed using an input device 218 or the data transceiver 252 in the personal key 200. This information is communicated to the personal key 200 via a communication path that is entirely distinct from the communication path between the personal key 200 and the host computer 102, and preferably entirely internal to the personal key 200 (not manifested externally to the personal key 200 by a means visible to malicious software). This prevents malicious software interfering with or emulating the user authorization.

Another embodiment of the present invention provides additional PIN security. In this embodiment, the VerifyPIN command is altered from that which is described in Table 6. Ordinarily, the VerifyPIN command accepts what the host computer 102 or remote computer/server 134 believes is the user's PIN as an argument. The personal key 200 accepts this command and returns a status indicating whether the proper PIN was provided. In this alternative embodiment however, the VerifyPIN command is altered so that it does not include the PIN as an argument. The VerifyPIN command is provided to the personal key 200, and the user is prompted to enter his or her PIN. After the PIN is entered, it is communicated to the processor 212 via a communication path 220 which is distinct from the host computer 102 - personal key 200 interface, and not externally manifested anywhere where it can be detected by malicious software. It is then internally verified, and a message providing the result of that manifestation is transmitted from the personal key 200 to the host computer 200 or remote computer/server 134. This prevents any external manifestation of the PIN.

When combined with the hashing technique using the secret 406 above, the foregoing provides a highly secure technique for user authorization. The secure hashing technique authenticates the key, and protects the secret 406 from external exposure. However, the hashing technique does not authenticate the person possessing the key (since it may have been lost or stolen). The ability to enter the PIN directly into the processor 212 of the personal key allows the personal key to authenticate the user, and since the PIN is never manifested externally from the key, exposure to malicious software is prevented. Since the third party can authenticate the personal key and the personal key can authenticate the user, the third party can perform user authentication with a high degree of confidence.

FIG. 10 is a flow chart illustrating an embodiment of the present invention in which the PIN is entered directly into the personal key 200. In block 1002, a command is issued which requires access to the user's PIN, such as the VerifyPIN and ModifyPIN commands listed in Table 6. The personal key 200 accepts 1004 the command, and if necessary, prompts the user for the PIN, as shown in block 1006. This may be accomplished with the display 122, one of the output devices 222, or any combination thereof. Preferably, this is accomplished via a communication path distinct and inaccessible from the USB interface 204. Using one of the input device 218 embodiments described above, the user provides the PIN to the personal key 200. Using a value stored in the memory 214, the processor 212 in the personal key 200 validates the user-entered PIN. In one embodiment, this is accomplished by comparing the user-provided value directly with a value stored in the memory 214. The personal key then provides 1014 a response indicating the validity of the PIN, which is accepted by the API 260. The response indicates whether the user supplied PIN was valid.

In one embodiment, a biometric sensor 250 is also communicatively coupled to the processor 212. The biometric sensor 250 provides data to the processor 212 and receives commands from the processor 212, as described earlier in this disclosure.

The processor is also optionally communicatively coupled to one or more light emitting devices 216 or other visual display device to provide a visual indication of

the activities or status of the personal key 200. The processor 212 may also be communicatively coupled with an aural device to provide a vibrational or audio data to the user of the status or activities of the personal key 200.

Conclusion

This concludes the description of the preferred embodiments of the present invention. In summary, the present invention describes a compact, self-contained, personal token. The token comprises a USB-compliant interface releaseably coupleable to a host processing device; a memory; and a processor. The processor provides the host processing device conditional access to data storable in the memory as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device and an integral user output device. The input and output devices communicate with the processor by communication paths which are independent from the USB-compliant interface, and thus allow the user to communicate with the processor without manifesting any private information external to the personal key.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. For example, while the foregoing personal key has been described as providing for electrical communication with the host communication, it is envisioned that such electrical communication includes the optical transfer of data such as is implemented by fiber optics and the like.

It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made

without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

WHAT IS CLAIMED IS:

1. A compact personal token (200), comprising:

a USB-compliant interface (206) releaseably coupleable to a host processing device (102);

a memory (214);

a processor (212), communicatively coupled to the memory (214) and communicatively coupleable to the host processing device (102) via the USB-compliant interface (130), the proccssor (212) for providing the host processing device (102) conditional access to data storable in the memory (214); and

a user input device (218), communicatively coupled to the processor (212) by a path (220) distinct from the USB-compliant interface (206).

2. The apparatus of claim 1, wherein the user input device (218) is configured to control an operation of the processor (212).

3. The apparatus of claim 1, wherein the operation comprises an operation selected from the group comprising:

an encryption operation; and

a decryption operation.

4. The apparatus of claim 1, wherein the operation comprises a digital signature operation using a private key stored in the memory (214).

5. The apparatus of claim 1, wherein the input device (218) comprises at least one pressure-sensitive device actuatable from an exterior surface of the token (200).

6. The apparatus of claim 1, wherein the input device (218) comprises at least one push-button switch (702).

7. The apparatus of claim 1, further comprising an output device (222), communicatively coupled to the processor (212) by path (224) distinct from the USB-compliant interface (206), for providing information regarding the operation of the processor (212).

8. The apparatus of claim 7, wherein the output device (212) comprises at least one light emitting device (616).

9. The apparatus of claim 7, wherein the output device comprises at least one liquid crystal display (706).

10. The apparatus of claim 7, wherein the output device comprises at least one aural output device.

11. A compact personal token (200), comprising:

a USB-compliant interface (206) releaseably coupleable to a host processing device (102);

a memory (214);

a processor (212), communicatively coupled to the memory (214) and communicatively coupleable to the host processing device (102) via the USB-compliant interface (206), the processor (212) for providing the host processing device (102) conditional access to data storable in the memory (214); and

a user output device (222), communicatively coupled to the processor (212).

12. The apparatus of claim 11, wherein the user output device (212) is coupled to the processor (212) by a path (224) distinct from the USB-compliant interface (206).

13. The apparatus of claim 11, wherein the user output device (212) is configured to indicate the operation of the processor (212).

14. The apparatus of claim 11, wherein the operation comprises an operation selected from the group comprising:

an encryption operation;

a decryption operation; and

a digital signature operation using a private key.

15. The apparatus of claim 11, wherein the user output device (212) is selected from a group comprising:

at least one light emitting device (616);

at least one liquid crystal display (706); and

at least one aural device.

16. The apparatus of claim 11, further comprising an input device (218), communicatively coupled to the processor (212) by path (220) distinct from the USB-compliant interface (206), for providing information for the operation of the processor (212).

17. The apparatus of claim 11, wherein the processor (212) and memory (214) are disposed on a circuit board (606) having at least one circuit connection surface (610) providing electrical communication with the processor (212), and the USB-compliant interface (206) comprises:

at least one conductive pin for providing electrical communication between the circuit connecting surface (610) and the host processing device (102), wherein the conductive pin comprises a pin securing portion and is releasably coupleable to the circuit connection surface (610); and

a housing (602) for substantially enclosing at least some of the circuit board(606), the housing (602) comprising a pin interfacing portion mateable with the pin securing portion for securing the pin member along a longitudinal axis of the conductive pin.

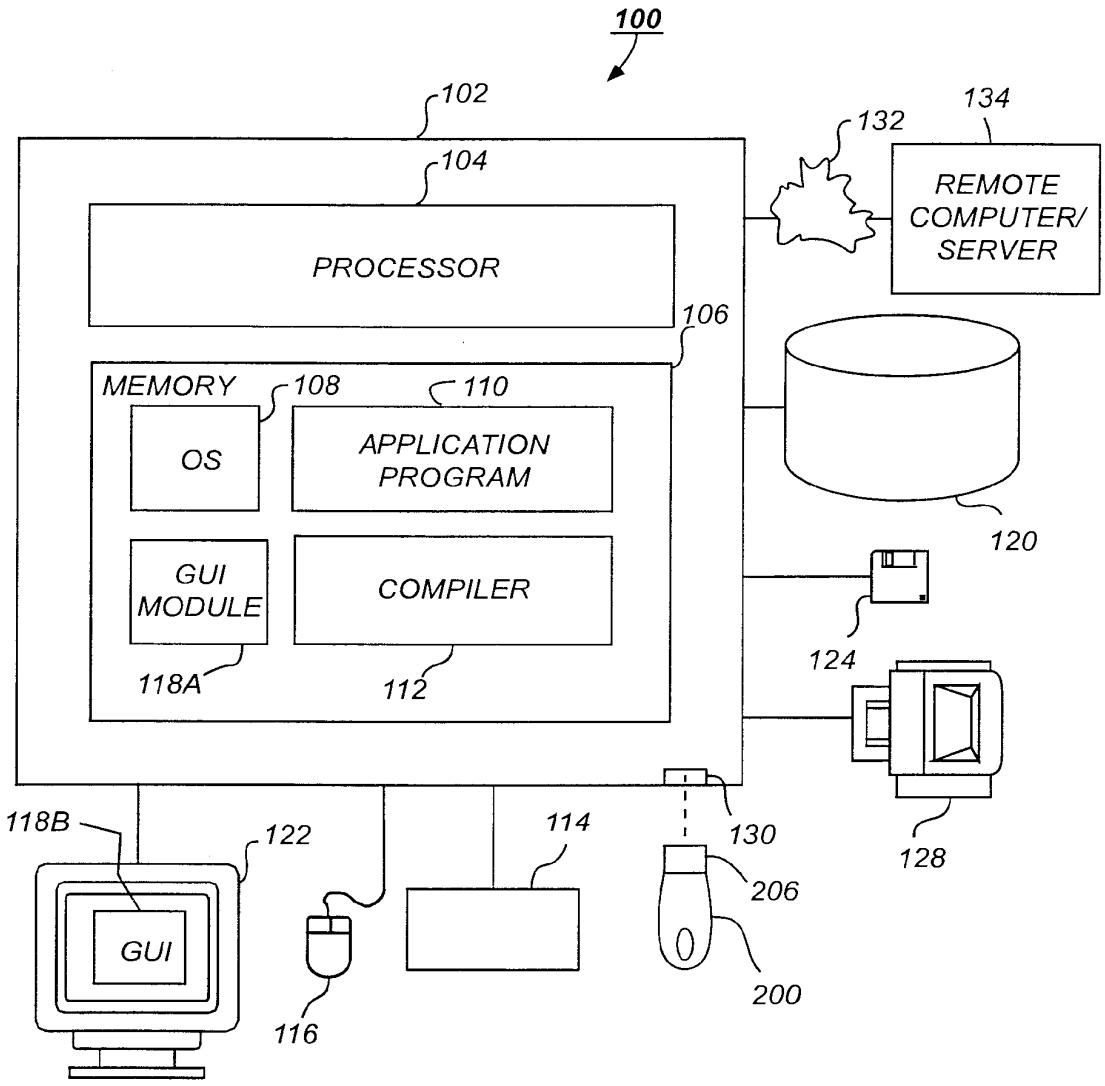

100
102
104
PROCESSOR
106
MEMORY
108
110
OS
APPLICATION PROGRAM
GUI MODULE
COMPILER
118A
112
132
134
REMOTE COMPUTER/ SERVER
120
124
128
130
206
200
114
118B
122
GUI
116

FIG. 1

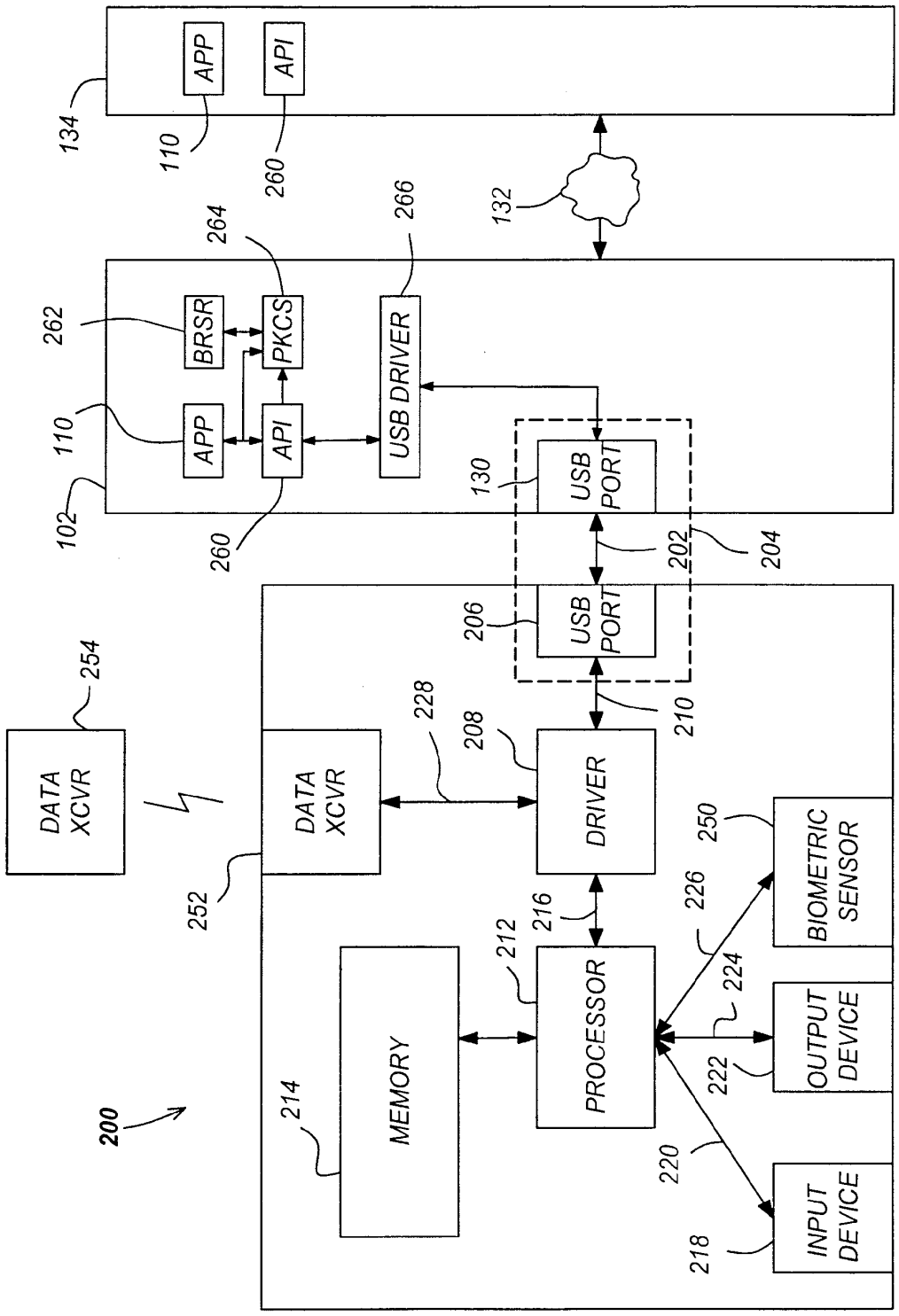

134
APP
API
110
260
132
264
266
262
BRSR
PKCS
USB DRIVER
110
APP
API
USB PORT
130
102
260
202
204
206
USB PORT
254
228
208
210
DATA XCVR
DATA XCVR
DRIVER
250
252
216
226
BIOMETRIC SENSOR
212
224
MEMORY
PROCESSOR
OUTPUT DEVICE
222
214
220
200
INPUT DEVICE
218

FIG. 2

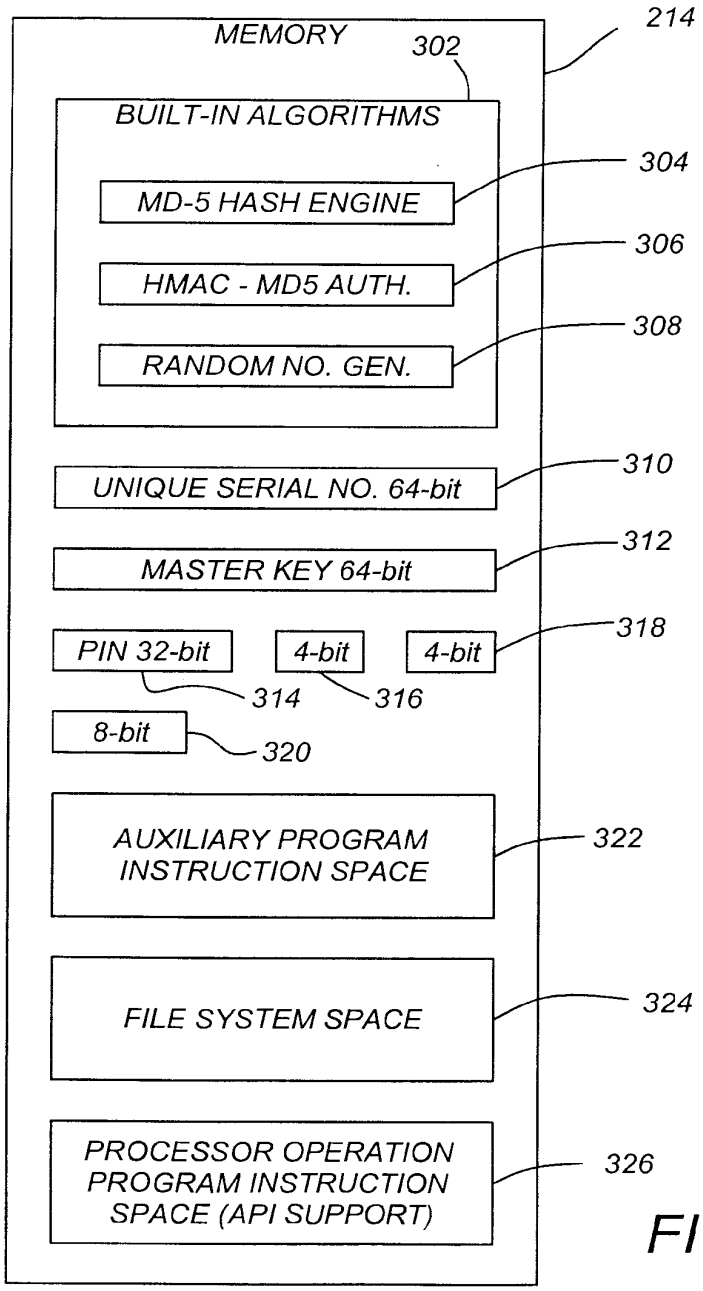

MEMORY
214
302
BUILT-IN ALGORITHMS
304
MD-5 HASH ENGINE
306
HMAC - MD5 AUTH.
308
RANDOM NO. GEN.
310
UNIQUE SERIAL NO. 64-bit
312
MASTER KEY 64-bit
318
PIN 32-bit
4-bit
4-bit
314
316
8-bit
320
AUXILIARY PROGRAM INSTRUCTION SPACE
322
FILE SYSTEM SPACE
324
PROCESSOR OPERATION PROGRAM INSTRUCTION SPACE (API SUPPORT)
326

FIG. 3

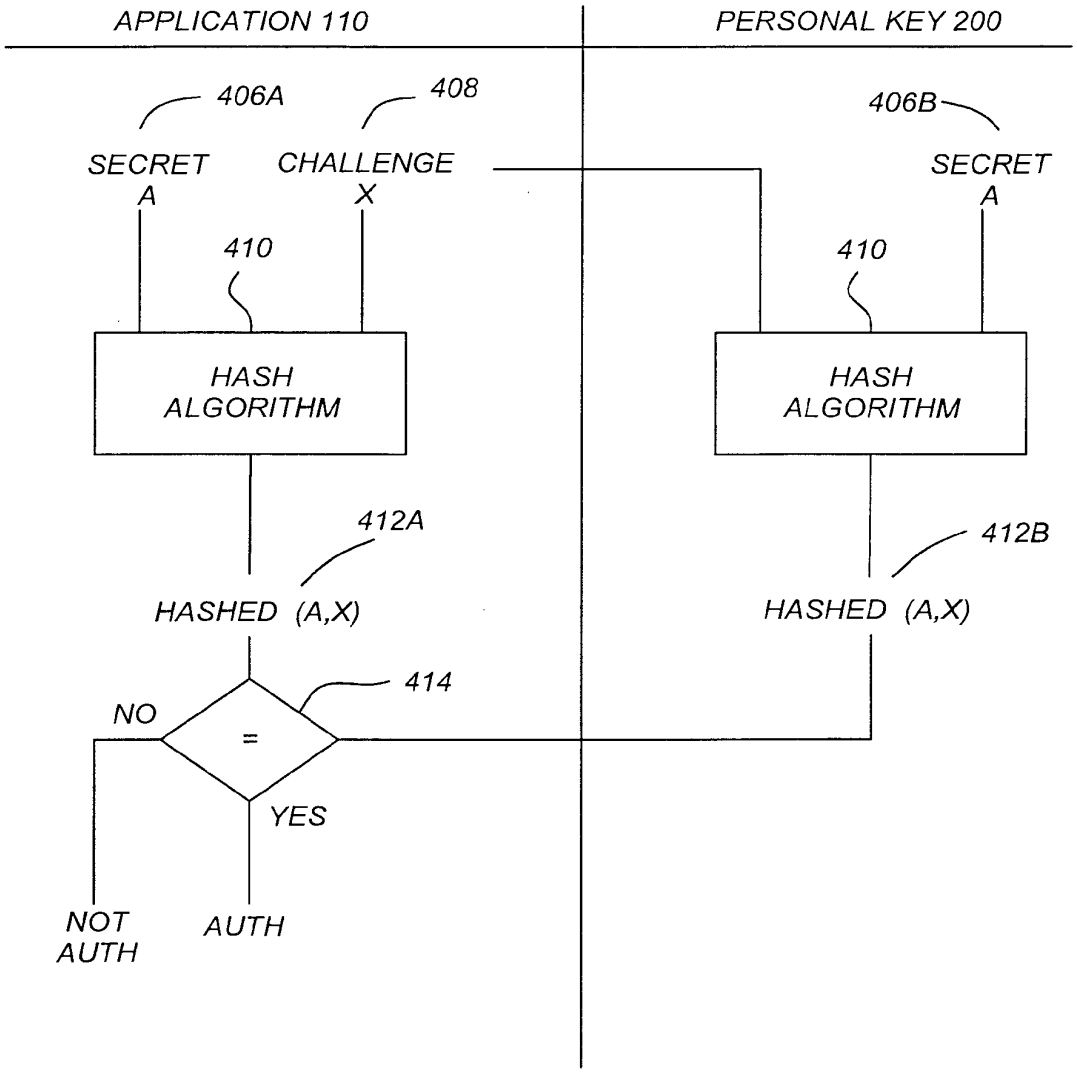

APPLICATION 110
PERSONAL KEY 200
406A
408
406B
SECRET A
CHALLENGE X
SECRET A
410
410
HASH ALGORITHM
HASH ALGORITHM
412A
412B
HASHED (A,X)
HASHED (A,X)
414
NO
=
YES
NOT AUTH
AUTH

FIG. 4

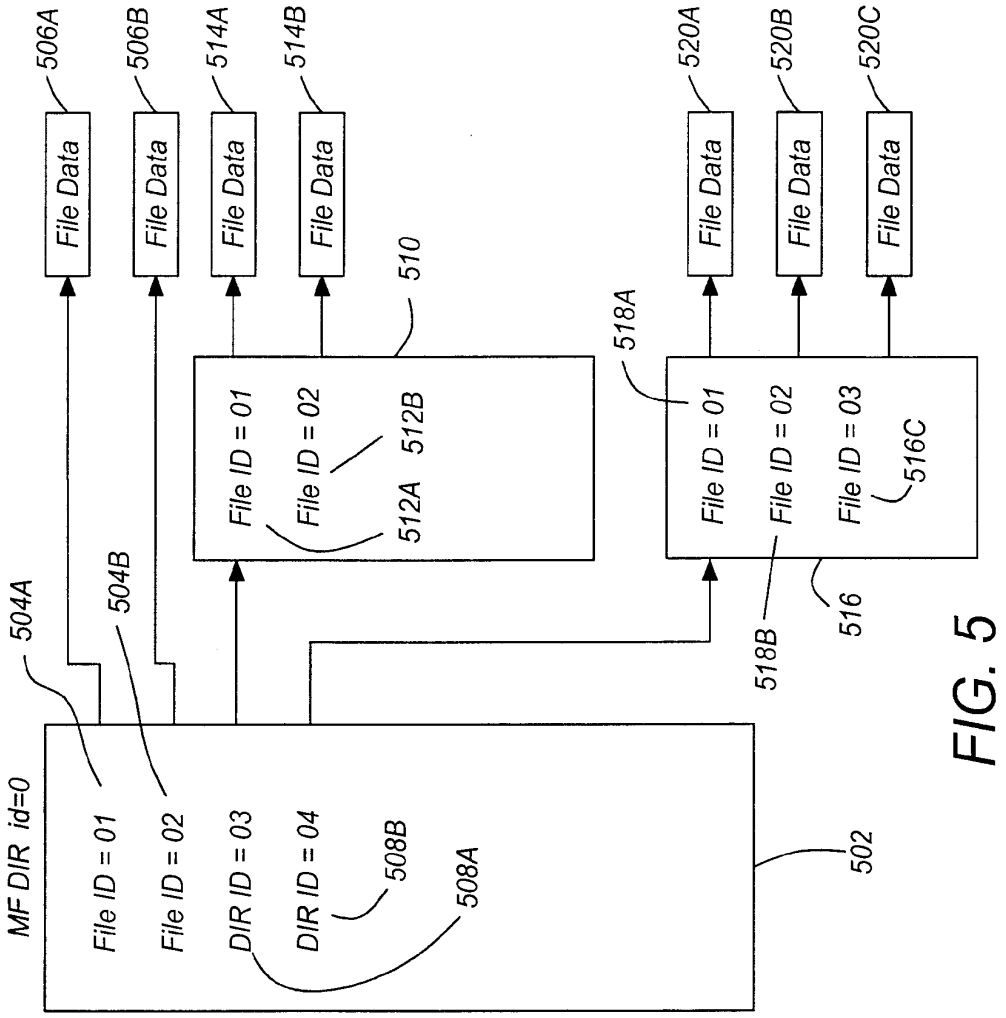

506A
506B
514A
514B
520A
520B
520C
File Data
510
518A
File ID = 01
File ID = 02
512B
512A
File ID = 03
516C
504A
504B
518B
516
MF DIR id=0
DIR ID = 03
DIR ID = 04
508B
508A
502

FIG. 5

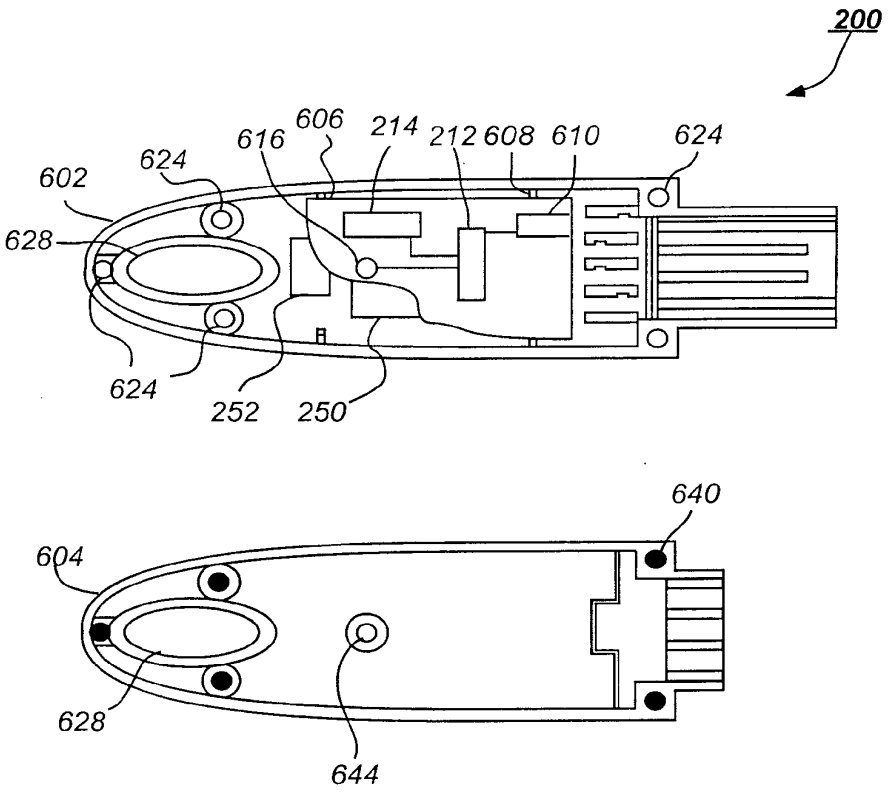

200
606
214
212
608
610
624
616
624
602
628
624
252
250
640
604
628
644

FIG. 6

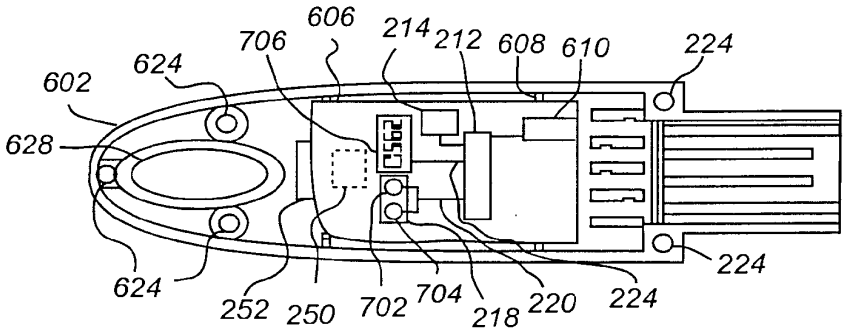


FIG. 7A

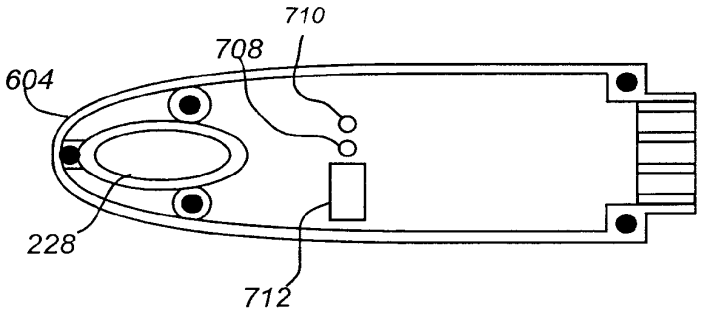


FIG. 7B

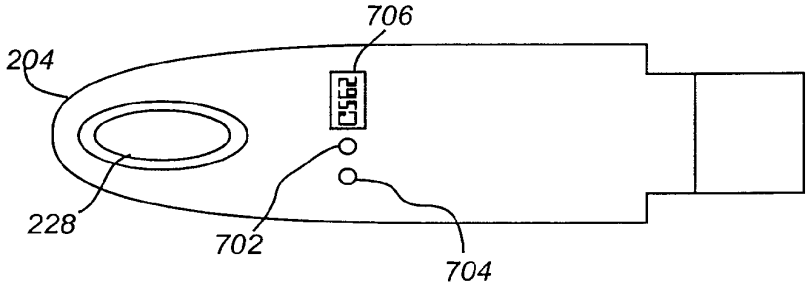


FIG. 7C

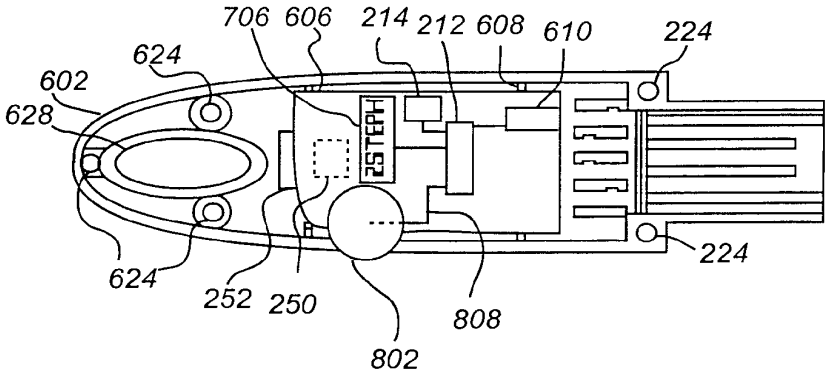


FIG. 8A

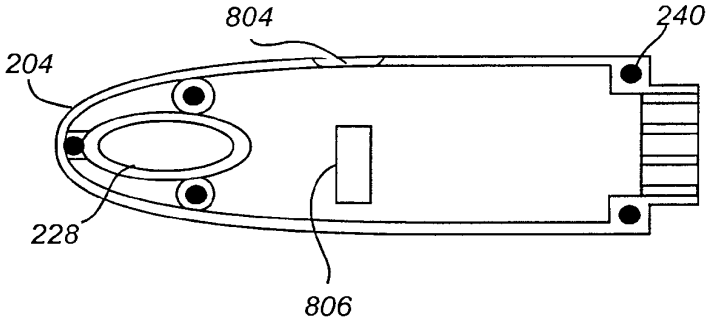


FIG. 8B

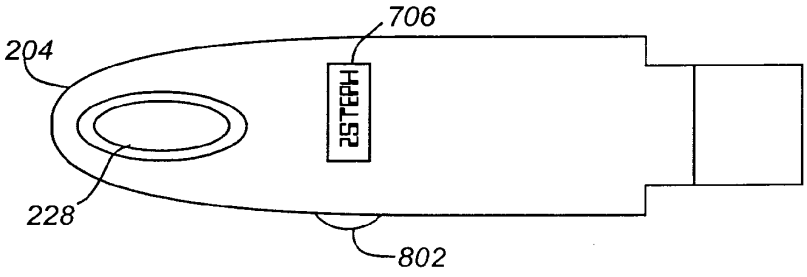


FIG. 8C

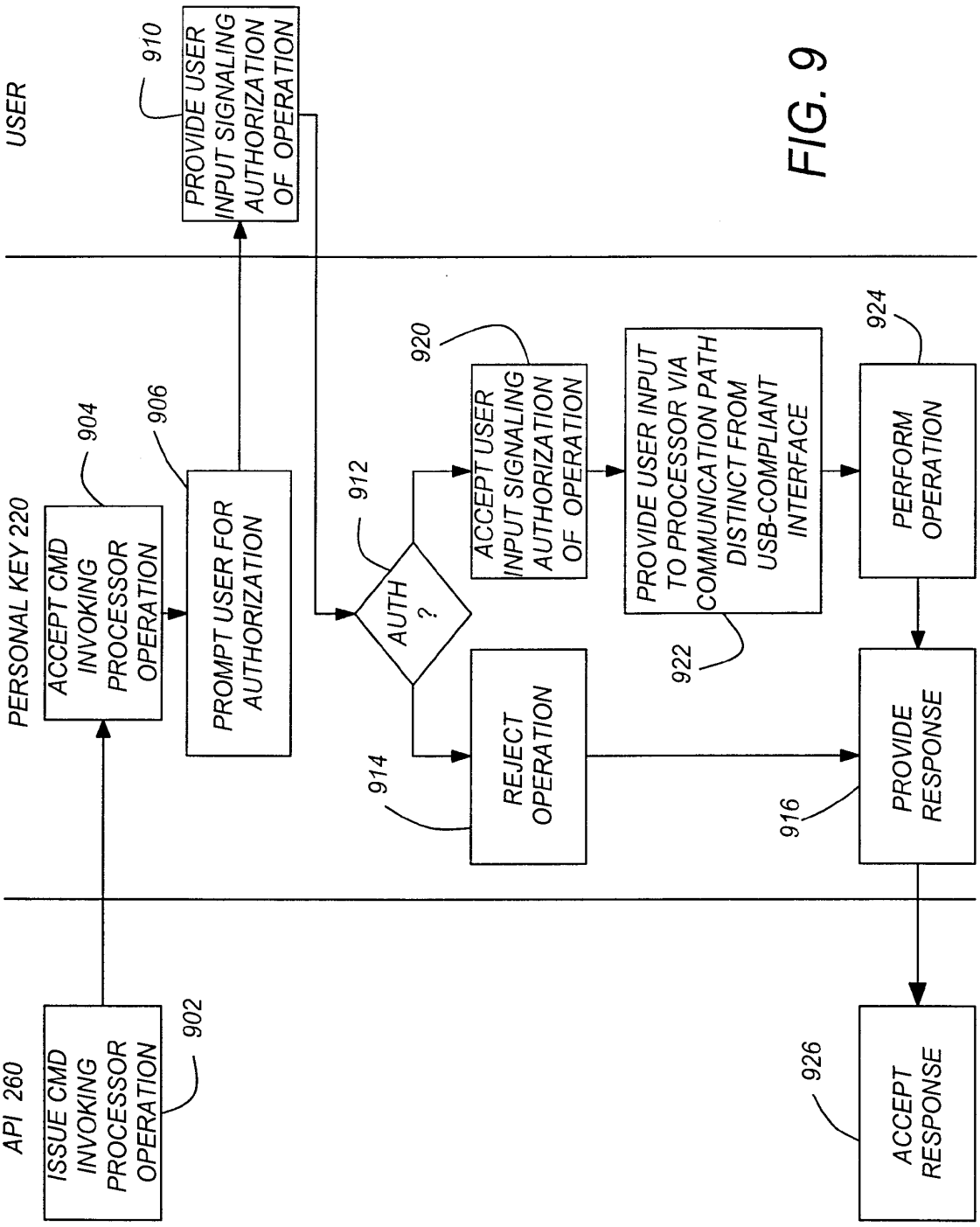

USER
PERSONAL KEY 220
API 260
ISSUE CMD INVOKING PROCESSOR OPERATION
902
ACCEPT CMD INVOKING PROCESSOR OPERATION
904
PROMPT USER FOR AUTHORIZATION
906
PROVIDE USER INPUT SIGNALING AUTHORIZATION OF OPERATION
910
AUTH ?
912
ACCEPT USER INPUT SIGNALING AUTHORIZATION OF OPERATION
920
PROVIDE USER INPUT TO PROCESSOR VIA COMMUNICATION PATH DISTINCT FROM USB-COMPLIANT INTERFACE
922
PERFORM OPERATION
924
REJECT OPERATION
914
PROVIDE RESPONSE
916
ACCEPT RESPONSE
926

FIG. 9

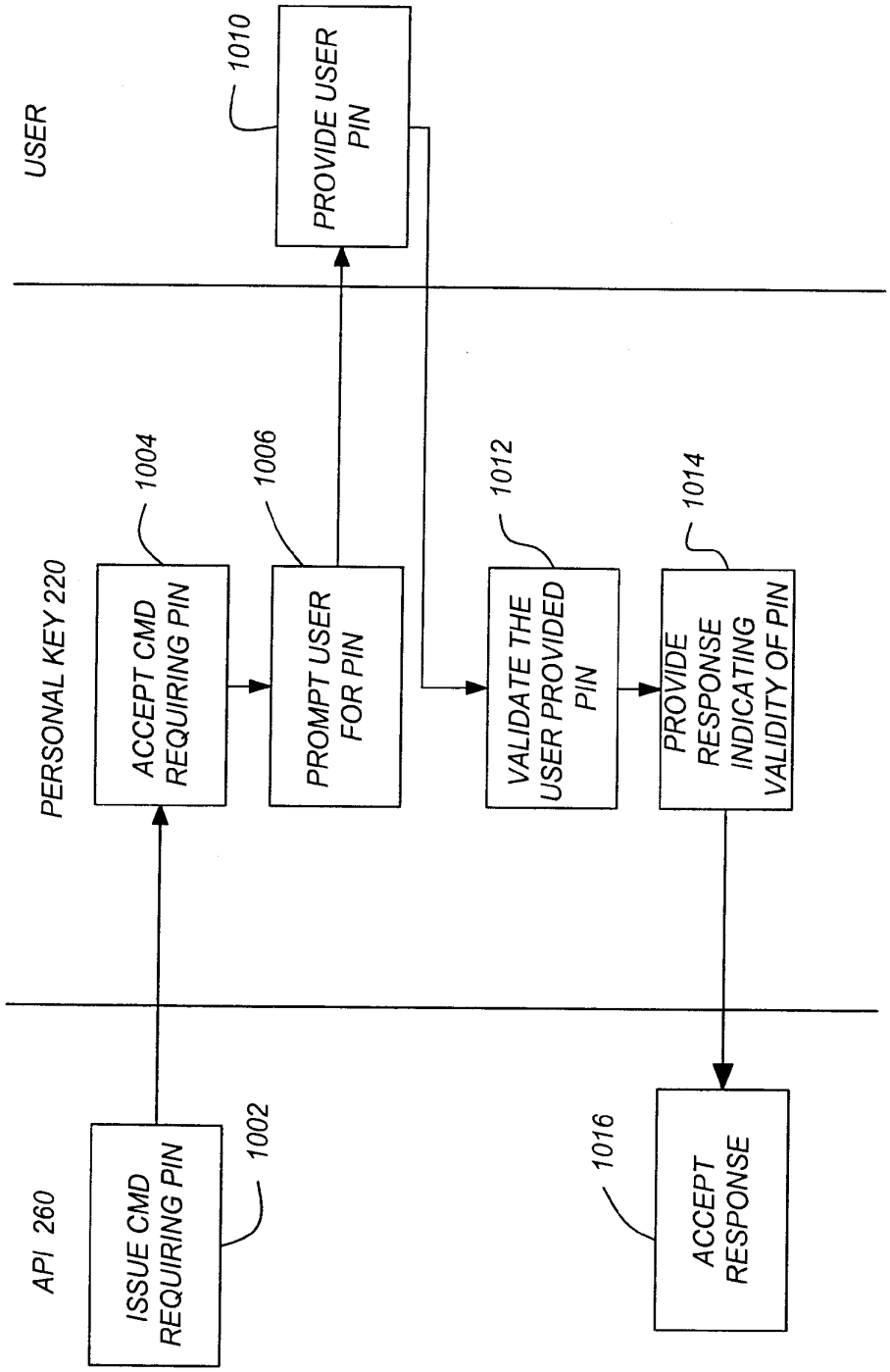

USER
PROVIDE USER PIN
1010
PERSONAL KEY 220
ACCEPT CMD REQUIRING PIN
1004
PROMPT USER FOR PIN
1006
VALIDATE THE USER PROVIDED PIN
1012
PROVIDE RESPONSE INDICATING VALIDITY OF PIN
1014
API 260
ISSUE CMD REQUIRING PIN
1002
ACCEPT RESPONSE
1016

FIG. 10

INTERNATIONAL SEARCH REPORT

Internatio. ...pplication No
PCT/US 00/00711

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"WIBU-KEY, User's Guide Version 2.50" 'Online! July 1998 (1998-07) , WIBU-SYSTEMS AG , KARLSRUHE, GERMANY XP002139265 Retrieved from the Internet: <URL: ftp://www2.wibu.de/pub/download/us/UG250US .pdf> 'retrieved on 2000-05-25!	1-5,7,9, 11,12, 14-16
A	page 12, paragraph 1 -page 14, paragraph 1 page 164 ---	17
Y	GB 2 154 344 A (NAT RES DEV) 4 September 1985 (1985-09-04) page 3, line 7 - line 62; figures 1-3 --- -/--	1-5,7,9, 11,12, 14-16

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2000	20/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internatic Application No
PCT/US 00/00711

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 791 877 A (FRANCE TELECOM) 27 August 1997 (1997-08-27) column 3, line 43 -column 4, line 8; figures ---	1,3,4, 11,12,14
A	US 5 857 024 A (NISHINO KIYOSHI ET AL) 5 January 1999 (1999-01-05) column 4, line 6 - line 64; figures 1,7 ---	1,5-9, 11-13, 15-17
A	"Rainbow Technologies Adds USB Support For PC And Macintosh Software Developers To Sentinel Line" NEWS RELEASE, 'Online! 17 November 1998 (1998-11-17), XP002139273 Retrieved from the Internet: <URL:http://www.rainbow.com/invest/PR98111 7b.html> 'retrieved on 2000-05-28! the whole document -----	1,3,4, 11,12,14

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatio application No
PCT/US 00/00711

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2154344 A	04-09-1985	US 4799258 A	17-01-1989
EP 0791877 A	27-08-1997	FR 2745399 A	29-08-1997
US 5857024 A	05-01-1999	JP 9114946 A	02-05-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

Electronic Acknowledgement Receipt

EFS ID:	2038725
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	02-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	09:02:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	DE_19631050.pdf	185970 99e9f9dcd6bf0b365d511dc226fe742b3aa13ccf	no	4
Warnings:					

Information:					
2	Foreign Reference	HK1063994.pdf	885012 d69cda2d664de6d1701b0470e3f1691f0b35ae1d	no	14
Warnings:					
Information:					
3	Foreign Reference	HK1063995.pdf	518447 7b835a22d2528236346337ec0006fe5cea86c1be	no	11
Warnings:					
Information:					
4	Foreign Reference	JP2004246720.pdf	907344 9159c08903f05d6a0e2bf39fb16607ba50cea65b	no	23
Warnings:					
Information:					
5	Foreign Reference	WO199952051.pdf	951330 ec4c57ba5b6100fcb5a986a3c5033b44f4c4e732	no	26
Warnings:					
Information:					
6	Foreign Reference	WO199938062.pdf	604741 20884711b7378788a042dacdd1bf523bc13a0f6a	no	16
Warnings:					
Information:					
7	Foreign Reference	WO200036252.pdf	965881 d5e717a68ba4acc00a6e42670eb814b1cea38ec4	no	27
Warnings:					
Information:					
8	Foreign Reference	WO200042491.pdf	2287491 e8f85924fba4d53d07ad7cfc609857cc040c315f	no	57
Warnings:					
Information:					
			Total Files Size (in bytes):	7306216	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 :		(11) Internationale Veröffentlichungsnummer: WO 00/65180
E05B 49/00	A1	(43) Internationales Veröffentlichungsdatum: 2. November 2000 (02.11.00)

(21) Internationales Aktenzeichen: PCT/EP00/02949

(22) Internationales Anmeldedatum: 3. April 2000 (03.04.00)

(30) Prioritätsdaten:
199 18 817.3 26. April 1999 (26.04.99) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, D–42551 Velbert (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MÜLLER, Ulrich [DE/DE]; Schneegelskothen 7C, D–42549 Velbert (DE). VAN DEN BOOM, Andreas [DE/DE]; Mühlenkamp 35, D–45309 Essen (DE). KLEIN, Helmut [DE/DE]; Heidekamp 51, D–42549 Velbert (DE).

(74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, D–42275 Wuppertal (DE).

(81) Bestimmungsstaaten: AU, BR, CN, IN, JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

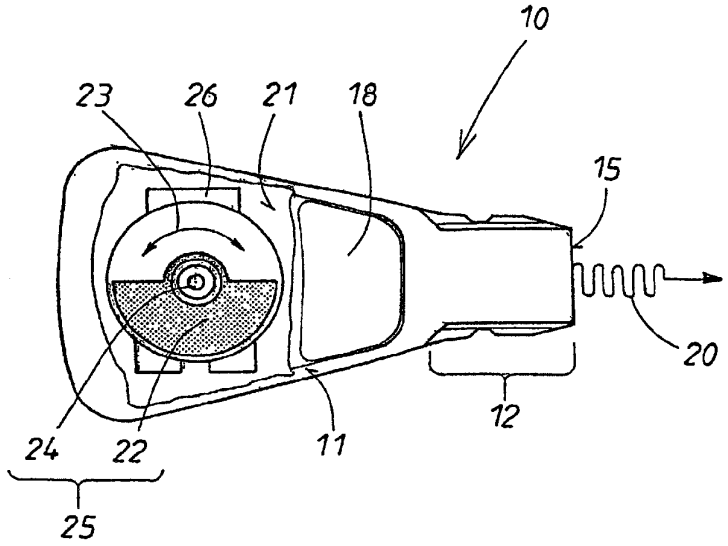
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: ELECTRONIC KEY, IN PARTICULAR, FOR VEHICLES

(54) Bezeichnung: ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR FAHRZEUGE

(57) Abstract

The invention relates to an electronic key (10), in which coded signals (20) are transmitted and optionally received. In order to achieve this, it is necessary to provide suitable electronic components which are supplied with electric energy by a current reservoir in the housing interior (21). A mass (22) is kinetically mounted (24) in the housing interior (21), in order to ensure that the electronic key (10) is continuously operational. The kinetic energy (23) of said mass (22) which is generated when the key is moved, is converted into electric energy by an electric generator (26), provided in the housing interior (21). The electric energy is subsequently used to continuously recharge the current reservoir.



(57) Zusammenfassung

Bei einem elektronischen Schlüssel (10) werden codierte Signale (20) gesendet und gegebenenfalls empfangen. Dazu sind geeignete elektronische Bauteile im Gehäuseinneren (21) notwendig, die von einem Stromspeicher mit elektrischer Energie versorgt werden. Um einen stets betriebsbereiten elektronischen Schlüssel (10) zu gewährleisten, wird vorgeschlagen, eine Masse (22) im Gehäuseinneren (21) beweglich zu lagern (24). Die beim Bewegen des Schlüssels anfallende Bewegungsenergie (23) dieser Masse (22) wird in einem im Gehäuseinneren (21) vorgesehenen elektrischen Generator (26) in elektrische Energie gewandelt, die dann zum dauernden Nachladen des Stromspeichers genutzt wird.

Elektronischer Schlüssel, insbesondere für Fahrzeuge

Die Erfindung richtet sich auf einen elektronischen Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Zum Betrieb der elektronischen Bauteile verwendet man in der Regel elektrische Batterien in Form von sogenannten Knopfzellen. Nach einiger Gebrauchszeit entleeren sich die Batterien. Es müssen daher Vorkehrungen getroffen werden, um die Batterien bequem ausbauen, neue Batterien wieder einbauen und zuverlässig kontaktieren zu können. Dafür muss ein geeigneter Platz im Schlüsselgehäuse reserviert sein. Das ist aufwendig. Das Auswechseln der Batterie ist mühevoll und erfordert eine eingehende Belehrung des Schlüsselbesitzers, der dazu nicht immer bereit ist.

Man kann anstelle von solchen Einweg-Batterien auch Akkumulatoren als Stromspeicher für die elektrische Energie im Schlüsselgehäuse verwenden. Es sind aber zum regelmäßigen Aufladen eines solchen Stromspeichers Anschlüsse im Schlüsselgehäuse erforderlich, deren Anordnung wegen der sehr begrenzten Gehäuseoberfläche problematisch ist. Außerdem sind Anzeigemittel für den Ladezustand des Stromspeichers erforderlich, wenn man von einer plötzlichen Entleerung des Stromspeichers nicht überrascht werden will. Auch das erfordert an der Gehäuseoberfläche Platz. Vor allem ist aber während des Ladevorgangs der Schlüssel nicht nutzbar. Der Schlüsselinhaber muss daher die Pausen zwischen der Benutzung des Schlüssels nutzen und die Ladetätigkeit gut einplanen. Das wird als störend empfunden.

Für den Betrieb elektrischer Kleingeräte (DE 196 20 880 A1) ist es bekannt, die zum bestimmungsgemäßen Gebrauch des Geräts erforderliche manuelle Betätigung eines Funktionsauslöseelements dazu zu verwenden, um daraus eine elektrische Energie zu gewinnen. Als Kleingerät verwendete man dabei auch einen mechanischen Schlüssel mit integrierter Infrarot-Sendeeinrichtung. Weil zur Gewinnung der elektrischen Energie ein entsprechendes, mechanisches Energieäquivalent aufgebracht werden muss, ist der Betätiger bei diesem Kleingerät schwergängig. Dies wirkt sich unangenehm bei der Handhabung aus.

Bei einem Türschloss mit einem manuell mittels eines Schlüssels schließbaren Schlossriegel (DE 32 08 818 C2) verwendete man einen elektrischen Antrieb für den Schlossriegel. Der elektrische Antrieb war an einen netzunabhängigen Speicher oder Generator angeschlossen. Die bestimmungsgemäße Betätigung des Schlosses beim Öffnen und Schließen wurde dazu genutzt, um den Generator anzutreiben. Die Betätigung zur Gewinnung elektrischer Energie konnte in einem Fall vom Türgriff ausgehen, der mit dem Generator gekuppelt war. In einem anderen Fall war das Antriebsritzel des dynamischen Generators mit einer Zahnstange eines im Schloss längsverschieblichen Schlüssels verbunden, der beim Ein- bzw. Ausstecken über den Generator elektrische Energie erzeugte.

Schließlich ist es bekannt (DE 197 21 001 C1) bei einem elektronischen Gerät einen längsverschieblichen Schieber oder einen drehbaren Rotationskörper vorzusehen, der, um elektrische Energie für das Gerät zu gewinnen, mit der Hand oder mit den Fingern bewegt werden musste. Die elektrische Energie wurde hier zwar auf mechanischem Wege erzeugt, doch musste dazu der Schieber bzw. der Rotationskörper gezielt manuell angetrieben werden. Das war mühsam und zeitaufwendig. Wurde es vergessen lag keine nutzbare elektrische Energie vor, weshalb der Betrieb des elektronischen Geräts ausfiel. Der Schieber bzw. der Rotationskörper erfordert einen großen Flächenbereich auf der Gehäuseaußenseite, um für die Hand zu Antriebszwecken gut zugänglich zu sein. Die Anwendung auf elektronische Schlösser war zwar vorgesehen, ist aber für elektronische Schlüssel ungeeignet.

Es ist bei Armbanduhren bekannt, dreh- oder schwenkbewegliche Pendel im Uhrengehäuse vorzusehen, welche für die mechanische Energieversorgung des Uhrwerks sorgen. Es liegt aber nicht nahe diese Uhrenmechanik auf elektronische Schlüssel zu übertragen, die, abgesehen von einem eventuellen mechanischen Notschlüssel, keine mechanische Funktionen haben und auf einen elektrischen Stromspeicher angewiesen sind.

Der Erfindung liegt die Aufgabe zugrunde einen preiswerten elektronischen Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, dessen Betriebsbereitschaft sich durch einen besonders bequemen Service auszeichnet. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Erfindung hat erkannt, dass der elektronische Schlüssel normalerweise Bewegungen ausgesetzt ist, die sich in Beschleunigungen und Verzögerungen des Schlüssels auswirken. Dadurch werden unvermeidlich dauernd mechanische Kräfte auf den Schlüssel ausgeübt, die zur Gewinnung von mechanischer Energie genutzt werden können. Dies tritt nicht nur in einer Ruhephase des Schlüssels ein, wenn der Schlüssel vom Besitzer in der Hosentasche od. dgl. getragen wird und der Schlüsselbesitzer sich bewegt, sondern auch während der Arbeitsphase des Schlüssels, wenn der Schlüssel im Schloss steckt und das Fahrzeug sich beschleunigend oder verzögernd bewegt.

Ordnet man nun eine Masse im Schlüsselgehäuse beweglich an, so kann die dort anfallende mechanische Energie von einem elektrischen Generator in elektrische Energie gewandelt werden. Diese elektrische Energie kann dann zum Aufladen des im Schlossgehäuse befindlichen Stromspeichers genutzt werden.

Bei der Erfindung ist nicht nur der Stromspeicher sondern auch die Aufladeeinrichtung und die Energieerzeugung im Inneren des Schlüsselgehäuses integriert. Es brauchen daher an der Gehäuseoberfläche keinen besonderen Maßnahmen zur Zugänglichkeit ins Schlüsselinnere oder zur Energieversorgung von

außen erfolgen. Der Schlüsselinhaber braucht sich um die Energieversorgung des elektronischen Schlüssels überhaupt nicht mehr zu kümmern; das Aufladen des Schlüssels erfolgt automatisch bei jeder Schlüsselbewegung, also sowohl in der Ruhe- als auch in der Gebrauchsphase des Schlüssels. Der erfindungsgemäße Schlüssel ist stets betriebsbereit.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus dem Unteranspruch, der nachfolgenden Beschreibung und der Zeichnung. In der Zeichnung ist die Erfindung schematisch in einem Ausführungsbeispiel dargestellt. Es zeigen:

Fig. 1 die Seitenansicht eines elektronischen Schlüssels mit einem Gehäuseausbruch und

Fig. 2 ein Blockschaltbild zur Verdeutlichung des inneren Aufbaus und der Wirkungsweise des erfindungsgemäßen Schlüssels.

Der elektronische Schlüssel 10 umfasst ein Schlüsselgehäuse 11 dessen eines Ende 12 mit einem geeigneten Einsteckprofil 12 versehen ist. Diesem elektronischen Schlüssel ist ein komplementäres elektronisches Schloss zugeordnet, das eine geeignete Aufnahme für das Einsteckprofil 12 aufweist. Im Schlüsselinneren sind verschiedenste elektronische Bauteile 13 vorgesehen, die in definierter Weise miteinander geschaltet sind, z.B. über Leiterbahnen einer sogenannten elektrischen Leiterplatte. Die elektronischen Bauteile 13 haben verschiedene Funktionen zu erfüllen. Außer der Kommunikation mit dem zugehörigen Schloss gehört dazu auch das Aussenden oder Empfangen von codierten Signalen 20, z.B. in Form einer elektromagnetischen hochfrequenten Strahlung. Dazu ist ein geeigneter Sender 14 im Schlüsselgehäuse integriert, zweckmäßigerweise am Stirnende 15 des Einsteckabschnitts 12.

Zur Energieversorgung der Schaltung und ihrer Bauteile 13 dient ein elektrischer Stromspeicher 16. Die elektrischen Bauteile 13 können durch einen Schalter 17

wirksam gesetzt werden. Der Schalter 17 wird von einem Betätiger 18, z.B. einem Taster, ein- und/oder ausgeschaltet. Das ist durch einen Betätigungspfeil 19 im Schema von Fig. 2 veranschaulicht. Dieser Betätiger 18 ist durch eine geeignete Profilierung eines Gehäusebereichs in die Gehäuseschale integriert.

Im Gehäuseinneren 21 ist eine Masse 22 beweglich gelagert, wie durch den Bewegungspfeil 23 veranschaulicht ist. Im vorliegenden Fall ist diese Masse 22 an einem Lagerzapfen 24 frei drehgelagert, weshalb hier ein Pendel 25 vorliegt. Diese Pendelbewegung 25 wird als mechanische Energie einem zugeordneten Generator 26 zugeführt, der elektrische Energie erzeugt und diese über die in Fig. 2 verdeutlichte elektrische Verbindung 27 zum Aufladen des Stromspeichers 16 nutzt.

Die rotatorische Energie eines Pendels 25 ist zwar besonders geeignet, doch wäre es auch möglich, die mechanische Energie durch eine translatorische Bewegung einer Masse 22 zu erzeugen. Die mechanische Energie kann in beliebiger Weise durch bewegliche Massen oder Flüssigkeiten im Inneren des Schlüsselgehäuses erzeugt werden. Entscheidend ist, dass die bei der Benutzung und Nichtbenutzung des Schlüssels anfallenden mechanischen Bewegungen in elektrische Energie umgewandelt werden, die zur Versorgung der elektronischen Bauteile beim bestimmungsgemäßen Gebrauch des elektronischen Schlüssels dient.

Bezugszeichenliste :

10	elektronischer Schlüssel
11	Schlüsselgehäuse von 10
12	Einsteckprofil von 11, Einsteckbereich
13	elektronische Bauteile in 11
14	Sender in 11
15	Stirnende von 12
16	Stromspeicher in 11
17	Schalter
18	Betätiger, Taster
19	Betätigungspfeil von 18
20	codiertes Signal von 14
21	Gehäuseinneres von 11
22	freibewegliche Masse
23	Bewegungspfeil von 22, Pendelbewegung
24	Lagerzapfen von 22
25	Pendel aus 22, 24
26	Generator
27	elektrische Verbindung zwischen 26, 16

Patentansprüche :

1.) Elektronischer Schlüssel (10), insbesondere für Fahrzeuge, mit einem Schlüsselgehäuse (11), beinhaltend

einen Sender (14) und gegebenenfalls einen Empfänger für codierte Signale (20) zwecks Kommunikation mit einem zugehörigen elektronischen Schloss,

eine elektrische Schaltung mit elektronischen Bauteilen (13) zur Generierung, zur Codierung und gegebenenfalls zur Decodierung der Signale (20)

und einen Stromspeicher (16) für die zum Betrieb der elektronischen Bauteile (13) benötigte elektrische Energie,

dadurch gekennzeichnet ,

dass eine bewegliche (23) Masse (22) im Schlüsselgehäuse (11) angeordnet ist und beim Bewegen des Schlüssels mechanische Energie erzeugt,

dass im Schlüsselgehäuse (11) ein Wandler, wie ein elektrischer Generator (26), angeordnet ist, der die mechanische Energie in elektrische Energie wandelt,

und dass die elektrische Energie zum Aufladen des Stromspeichers (16) im Schlüsselgehäuse (11) dient.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die bewegliche Masse (22) aus einem schwenk- bzw. drehgelagerten (24) Pendel (25) besteht.

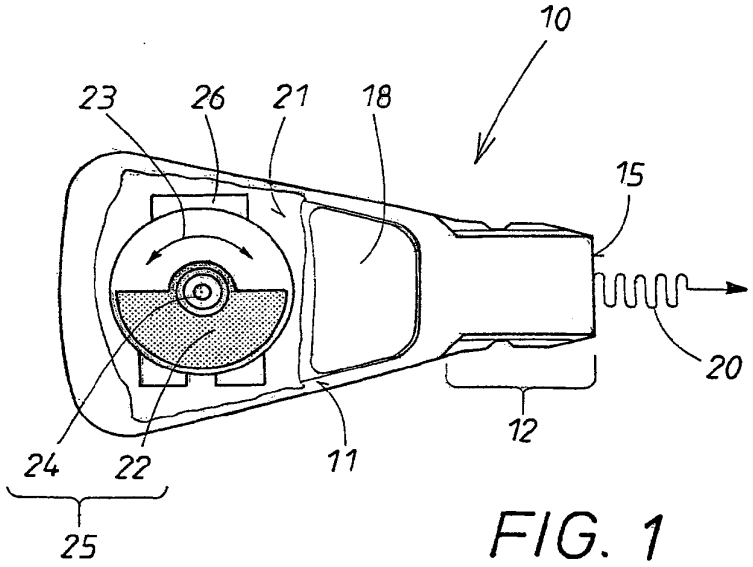

10
23
26
21
18
15
20
12
11
24
22
25

FIG. 1

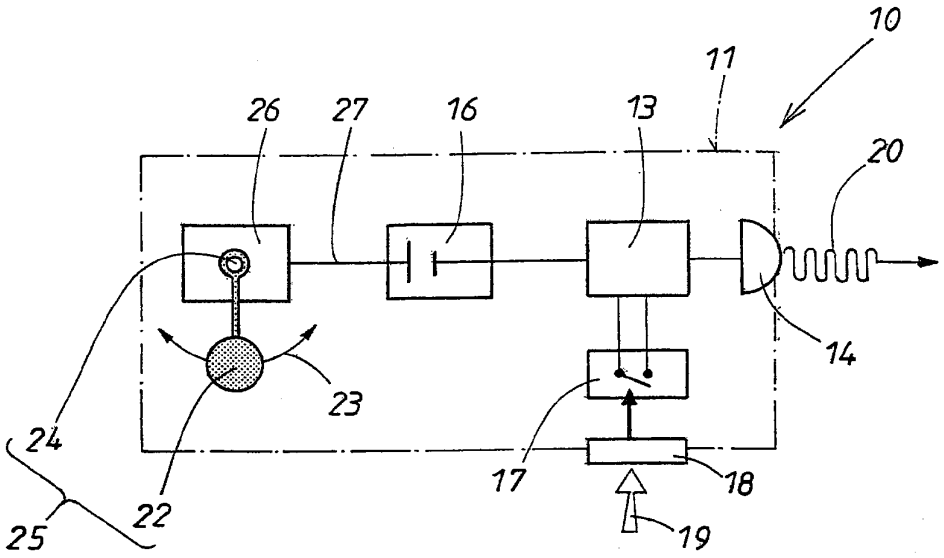

10
11
26
27
16
13
20
14
23
24
22
25
17
18
19

FIG. 2

INTERNATIONAL SEARCH REPORT

Inte. ..ional Application No
PCT/EP 00/02949

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B G04C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 196 20 880 A (BRANDESTINI) 27 November 1997 (1997-11-27) cited in the application the whole document	1,2
Y	WO 84 01041 A (KNAPEN) 15 March 1984 (1984-03-15) abstract	1,2
A	EP 0 170 303 A (KINETRON BV) 5 February 1986 (1986-02-05) abstract	1,2
A	FR 2 407 599 A (JUILLET) 25 May 1979 (1979-05-25) the whole document	1,2

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2000	24/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van Beurden, J

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/EP 00/02949

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19620880 A	27-11-1997	CN 1219298 A	09-06-1999
		WO 9744883 A	27-11-1997
		EP 0900467 A	10-03-1999
WO 8401041 A	15-03-1984	NL 8203443 A	02-04-1984
		AU 1944983 A	29-03-1984
		EP 0119223 A	26-09-1984
EP 0170303 A	05-02-1986	NL 8402113 A	03-02-1986
		AT 40223 T	15-02-1989
		DE 3567750 D	23-02-1989
		JP 1612218 C	30-07-1991
		JP 2035547 B	10-08-1990
		JP 61018326 A	27-01-1986
		KR 9005809 B	11-08-1990
		US 4644246 A	17-02-1987
FR 2407599 A	25-05-1979	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Inte. ionales Aktenzeichen
PCT/EP 00/02949

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B G04C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	DE 196 20 880 A (BRANDESTINI) 27. November 1997 (1997-11-27) in der Anmeldung erwähnt das ganze Dokument	1,2
Y	WO 84 01041 A (KNAPEN) 15. März 1984 (1984-03-15) Zusammenfassung	1,2
A	EP 0 170 303 A (KINETRON BV) 5. Februar 1986 (1986-02-05) Zusammenfassung	1,2
A	FR 2 407 599 A (JUILLET) 25. Mai 1979 (1979-05-25) das ganze Dokument	1,2

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. August 2000	24/08/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van Beurden, J

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/02949

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19620880 A	27-11-1997	CN 1219298 A	09-06-1999
		WO 9744883 A	27-11-1997
		EP 0900467 A	10-03-1999
WO 8401041 A	15-03-1984	NL 8203443 A	02-04-1984
		AU 1944983 A	29-03-1984
		EP 0119223 A	26-09-1984
EP 0170303 A	05-02-1986	NL 8402113 A	03-02-1986
		AT 40223 T	15-02-1989
		DE 3567750 D	23-02-1989
		JP 1612218 C	30-07-1991
		JP 2035547 B	10-08-1990
		JP 61018326 A	27-01-1986
		KR 9005809 B	11-08-1990
		US 4644246 A	17-02-1987
FR 2407599 A	25-05-1979	KEINE	

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75755 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IT00/00216

(22) International Filing Date: 25 May 2000 (25.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
TO99A000480 8 June 1999 (08.06.1999) IT

(71) Applicant *(for all designated States except US)*: **EUTRON INFOSECURITY S.R.L.** [IT/IT]; Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LEIDI, Michele** [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT). **CASSIA, Lucio** [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(74) Agent: **GARAVELLI, Paolo**; A.Bre.Mar. S.r.l., Via Servais, 27, I-10146 Torino (IT).

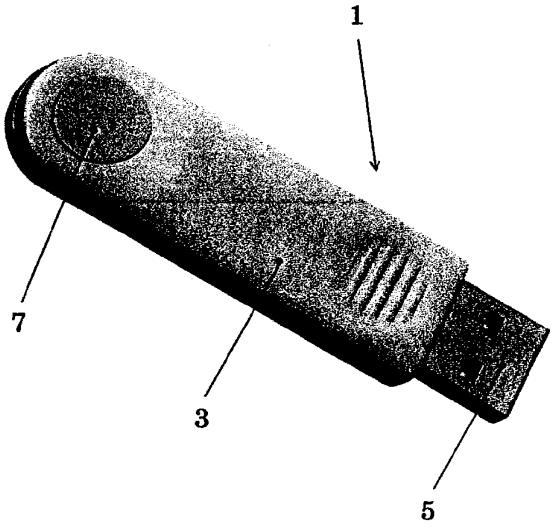
(81) Designated States *(national)*: AE, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, YU, ZA.

(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, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

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.

(54) Title: IDENTIFICATION DEVICE FOR AUTHENTICATING A USER



(57) Abstract: A device (1) is described to authenticate a user in an Internet environment, comprising: a support structure (3); a terminal (5) for the connection to a processor port; a microprocessor circuitry to perform safety functions and cryptography algorithms; and activation means (7) to allow enabling an authentication code. A system and a process are further described to input a PIN inside the device (1) and a system and a process to authenticate a user based on such device (1).

WO 00/75755 A1

IDENTIFICATION DEVICE FOR AUTHENTICATING A USER

The present invention refers to a user authentication system within an Internet architecture based on an hardware device connected to the Universal Serial Bus (USB) port of a client processor through a cryptographic procedure of the "Challenge Response" type. Moreover, the invention refers to a hardware and software system to input a Personal Identification Number (PIN) inside the above-said identification device based on USB port in order to prevent the interception thereof.

With the always wider spreading of the Internet network and other networks of this type, a particular and major importance has been given to problems about the controlled distribution of information on the network, in order to guarantee that these information cannot be attacked and guarantee their privacy as well, in addition to

providing access to particular transactions or information only to authorised users. Several arrangements have so far been proposed, starting from the so-called protecting "hardware keys" to be connected to processors, up to more or less complex cryptographic systems with different types of software keys. The proposed solutions either are very costly to be implemented in terms of several types of resources, or do not guarantee a complete safety of the information to be protected.

Object of the present invention is solving the above prior-art problems, by providing an hardware and software system that is of a reduced cost, easily implemented and absolutely efficient in terms of protection. In particular, the hardware device of the invention is of a simple configuration, has the sizes of a key and, once being inserted into the USB port of a computer, allows univocally recognising and authenticating the user of a network-based application and to start therewith protected and encrypted transactions on the Internet network itself. Authentication uniqueness and transaction safety are based on the features of the device, that is equipped with a microprocessor implemented for

safety functions, and on private-key time-varying cryptographic algorithms.

The above and other objects and advantages of the invention, as will appear from the following description, are obtained by a user authentication device and process as claimed in Claims 1 and 6, respectively, and by a system and process that use the above device as claimed in Claims 15 and 17, respectively. Preferred embodiments and non-trivial variations of the present invention are claimed in the dependent Claims.

The present invention will be better described by some preferred embodiments thereof, given as a non-limiting example, with reference to the enclosed drawings, in which:

- Figure 1 is a perspective view of an embodiment of the device according to the present invention;
- Figure 2 is a block diagram of the architecture of the code-inputting system of the device of the invention;
- Figure 3 is a block diagram of the process realised by the architecture in Fig. 2;
- Figure 4 is a block diagram detailing a step of the process in Fig. 3;

- Figure 5 is a block diagram detailing a step of the process in Fig. 3;
- Figure 6 is a block diagram of the operating process of the device in Fig. 1;
- Figure 7 is a block diagram detailing a step of the process in Fig. 6;
- Figure 8 is a block diagram detailing a step of the process in Fig. 6;
- Figure 9 is a block diagram summarising the steps of the processes in Fig.s 7 and 8; and
- Figure 10 is a block diagram detailing a step of the process in Fig. 6.

With reference to Fig. 1, the device 1 for authenticating a user in an Internet architecture environment substantially comprises an elongated support structure 3, preferably made of plastic material and adapted to be grasped by a user and inserted into a port of a client processor (not shown), for example the Universal Serial Bus (USB) port of a personal computer. For such purpose, the device 1 is equipped with a terminal 5 for the connection to the port and with a microprocessor circuitry contained inside the support structure 3; the circuitry is adapted to perform safety

functions and to operate on cryptographic algorithms. Finally, the device 1 of the invention comprises activation means 7 (commonly realised in the shape of a push-button) supported by the structure 3 and adapted to control the microprocessor circuitry to allow enabling therein an authentication code, as will be described hereinbelow.

In the current and preferred embodiment, the device 1 operates on cryptographic algorithms that are of the private-key time-varying type. Due to the standard interface and "plug&play" USB and to a set of interfacing libraries of the ActiveX and Plug-In type on server and client sides, the device 1 is efficient in terms not only of safety, but also of simplicity and transparency. Its features make it an efficient tool to store keywords, electronic certificates, digital signatures, electronic purse functions or to store and protect therein other interesting information related to user or used services.

With the device 1 of the invention, those who need protecting and checking the access to pages, services, data bases or more generally to areas of Internet sites, will simply have to supply

authorised users of their one Internet service with a suitably initialised device 1. The users will then have to simply insert the device 1 into the USB port of the computer without performing any installation operation. The server application will take care of setting a safe communication with the device 1 in order to authenticate the user. User recognition in fact occurs depending on reserved information inside the device linked with a user keyword. Once having recognised the client and having checked affected user authorisations, the device 1 takes care of sending customised and reserved information to the user, encrypting the contents with an algorithm of the 256-bit Blowfish type, for example, with a time-varying key linked to the secret value contained into the device 1. Information can be indifferently, but not in a limiting way, HTML pages, data bases information with "web" interface, forms, download areas, and the like. The information transaction of the network is performed encrypted both from server to client, and vice versa.

In order to be able to use the above-described device 1, it is necessary to equip it with a univocal Personal Identification Number (PIN) per

user. For such purpose, a system has been implemented whose architecture is shown in Fig. 2, such system being adapted to perform a process as detailed in Figures 3 to 5.

With reference first of all to Fig. 2, the system architecture that allows using the device 1 substantially comprises a processor equipped with a graphic window 10 that displays a digit from 0 to 9. Such window cooperates with a user library 12 (arrow A in Fig. 2), that is a proprietary library that deals with managing the device 1 and, through an identification process 14 contained therein, with checking the enabling of the device 1 itself.

The user library 12 is connected (arrow B in Fig. 2) with a device driver 16, that is also a proprietary library that deals with managing the device 1 at USB level. The device driver 16 is connected (arrow C in Fig. 2) with the device 1 that receives commands (arrow D in Fig. 2) from the push-button 7. According to the flow defined by arrows A to D, in the user library 12 an internal tick pulse is generated so that, upon every tick, a digit is sent both to the window 10 for being displayed, and to the device 1 through the device driver 16; the device driver 16 queries the device

1 whether there are other digits and, if the response is affirmative, goes on with the processing, while otherwise it warns the user library 12 to stop the process. Upon every pressure of the push-button 7, the device 1 stores the currently supplied digit that is also displayed by the window 10.

The general operation of the above-described system is shown as a block diagram in Fig.s 3 to 5. Such process guarantees the maximum safety when inputting the PIN to use the device 1. The process first of all comprises, upon request of the PIN code, the activation (301) of the graphic window 10 to display a current digit from 0 to 9.

Then the PIN code is sent (303) for every digit, through a process inserted into the libraries, both to the displaying window 10 and to the device 1.

Upon pressing the push-button 7, therefore, every digit is stored (305) as belonging to the PIN code; then, the process that sends the digit both to the graphic window 10 and to the device 1, queries (307) every time the device 1 to check whether there are other digits: if the response is affirmative, the process goes on by timely sending

(309) the other digits; otherwise, it stops (311) and the final PIN key is stored to validate the device 1.

Upon a more detailed examination, the operation of the PIN code storing step (305) can be divided into two major steps, where the first one deals with managing the display and dispatch of the digits to the device 1, while the second one deals with managing the push-button 7 of the device 1 itself.

In particular, as shown in detail in Fig. 4, the displaying and dispatching step of the digits to the device 1 starts in 401 and comprises the following sub-steps:

- creating (403) the window 10 to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response, removing (407) the displaying window 10; or
- in case of a negative response, sending (409) the digit to the graphic window 10 and to the device 1; and
- requesting (411) to the device 1 whether the

digits limit for the PIN code has been reached, returning to the querying step (405): if the response is affirmative, the process finally ends in 413.

With reference to Fig. 5, instead, the flow diagram of the management step for the push-button 7 of the device 1 is shown in detail, this step being able to be divided into the following sub-steps, starting from the initial one in 501:

- querying (503) whether the digits limit has been reached;
- in case of an affirmative response, ending (509) the process; or
- in case of a negative response, checking (505) whether the push-button 7 has been pressed;
- in case of a negative response, the procedure remains waiting for a following pressure of the push-button 7; or
- in case of an affirmative response, storing (507) the last received digit and returning to the querying step (503) are performed.

After having defined the device 1 of the invention in this way and the system and process to

store and validate the personal code inside the device, it is possible to practice the real and proper process of the invention to manage the accesses to reserved pages and services being present on the Internet network.

As already stated, the system that allows such process is composed, preferably but not in a limiting way, of a central server processor (not shown) that stores and manages the authorised users, connected to a set of local client processors (not shown) equipped with the device 1 of the invention. The detailed procedure is commonly realised through programs being present on both server and client processors, and is shown in Fig.s 7 to 10 of the description.

In particular, with reference to Fig. 6, the process for authenticating a user in an Internet architecture environment comprises the following macro-steps:

- associating (601) a user with an identification device 1;
- identifying (603) the user through the device 1; and
- encrypting (605) information sent/received by/from the user.

In particular, as shown in Fig. 7, the associating step (601) of a user to the device 1 comprises the following sub-steps:

- describing (701) the user;
- generating (703) a TokenId based on describing data of the user;
- performing (705) a first irreversible safe scrambling step (preferably of the MD5 type) of the TokenId after a communication (709) with the server processor managing the keywords;
- creating (706) a first Personal Identification Number (PIN) from the first scrambling (705);
- performing (707) a second irreversible safe scrambling step (preferably of the MD5 + 3DES type) of the TokenId after a communication (709) with the server processor for the keywords;
- creating (708) a second Personal Identification Number (PIN2) from the second scrambling (705), where the second Personal Identification Number (PIN2) is different from the first Personal Identification Number

(PIN);

- associating the user with an identification string composed of the TokenId, the first Personal Identification Number (PIN) and the second Personal Identification Number (PIN2); and
- storing such complete identification string into the device 1 and the TokenId alone into a data base on the server processor.

With reference now to Fig. 8 in particular and to Fig. 9 as assembly view of the two steps shown in Fig.s 7 and 8, the user identifying step (603) through the device 1 is shown in detail; it comprises the following sub-steps:

- in case of an access by the user to web pages of the network in which an access control must be performed, the server processor sends (801) to the client processor a string of the "Server Challenge" type, that is always different; the string is associated with the first Personal Identification Number (from 706) and is processed by the client to be able to provide a response for the server. For this purpose, the process proceeds with the steps of:

- performing (803) an hashing step (preferably of the MD5 type) on the "Server Challenge" string and the first Personal Identification Number, thereby producing (805) a text string;
- using (807) the second Personal Identification Number (PIN2) (from 708) as encrypting key of a cryptography (809) (preferably of the 3DES type) on the text string;
- generating (811, 813) a string comprising the TokenId and a Response Client and sending such string to the server processor;
- comparing (step 901 in Fig. 9) on the server the received string with the Response Client being generated on the server side by re-processing the first and second Personal Identification Numbers (PIN, PIN2); and
- in case of a positive response to such comparing step (901), pointing out (step 903 in Fig. 9) the existence of a correct identification code; or
- in case of a negative response to such comparing step (901), pointing out (step 905

in Fig. 9) the existence of an incorrect or counterfeited identification code.

Finally, with reference to Fig. 10, the information encrypting step (605) comprises the following sub-steps, performed by the server processor:

- generating (1000) an encryption key from the previous encrypting step (809) by using as input the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page from the network;
- encrypting (1001) (preferably using the Blowfish encryption) the received page through the generated encryption key; and
- sending (1005) the encrypted page to the client processor, which, once having received the encrypted pages, is able to decrypt them and reproduce them in a clear way, because it knows both the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2).

Some embodiments of the invention have been described, but obviously they are subjected to further modifications and variations within the

same inventive idea. For example, several construction variations of the device 1 will be possible, both from the point of view of the connections to external processor ports, and from the point of view of the internal circuitry to realise the described functionalities. Moreover, the various processes of the invention could be applied to various types of authentication devices, and the systems to realise the described processes could be implemented according to different connection configurations to various types of networks.

CLAIMS

1. Device (1) for authenticating a user in an Internet architecture environment, characterised in that the device comprises:

- a support structure (3);
- a terminal (5) for the connection to a port of a processor;
- a microprocessor circuitry contained inside said support structure (3), said circuitry being adapted to perform safety functions and operating on cryptographic algorithms; and
- activation means (7) supported by said structure (3) and adapted to control said microprocessor circuitry to allow enabling therein an authentication code.

2. Device (1) according to Claim 1, characterised in that said terminal (5) is adapted to be connected to a port of the Universal Serial Bus (USB) type of a personal computer.

3. Device (1) according to Claim 1, characterised in that said activation means (7) are composed of a push-button.

4. Device (1) according to Claim 1, characterised in that said cryptographic algorithms performed by said microprocessor circuitry are of the private-key time-varying type.

5. Device (1) according to Claim 3, characterised in that said cryptographic algorithms are of the "Challenge Response" type.

6. Process for authenticating a user in an Internet architecture environment, characterised in that the process comprises the following steps:

- associating (601) a user with an identification device (1);
- identifying (603) said user through said device (1); and
- encrypting (605) information sent/received by/from said user.

7. Process according to Claim 6, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

8. Process according to Claim 6, characterised in that said associating step (601) comprises the following sub-steps:

- describing (701) said user;
- generating (703) a TokenId based on describing data of said user;
- performing (705) a first irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor;
- creating (706) a first Personal Identification Number (PIN) from said first scrambling (705);
- performing (707) a second irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor, said second scrambling (707) being different from said first scrambling (705);
- creating (708) a second Personal Identification Number (PIN2) from said second scrambling (705), said second Personal Identification Number (PIN2) being different from said first Personal Identification Number (PIN);
- associating said user with an identification string composed of said TokenId, said first Personal Identification Number (PIN) and said

second Personal Identification Number (PIN2); and

- storing said complete identification string into said device (1) and said TokenId into a data base on said server processor.

9. Process according to Claim 8, characterised in that said first scrambling (705) is of the MD5 type and said second scrambling (707) is of the MD5 + 3DES type.

10. Process according to any one of Claims 6 to 9, characterised in that said identifying step (603) comprises the following sub-steps:

- in case of an access by said user to pages of said network in which an access control must be performed, sending (801) by the server processor a string of the "Server Challenge" type, said string being associated with said first Personal Identification Number;
- performing (803) an hashing step on said "Server Challenge" string and said first Personal Identification Number, thereby producing (805) a text string;
- using (807) said second Personal Identification Number (PIN2) as encrypting

key of a cryptography (809) on said text string;

- generating (811, 813) a string comprising said TokenId and a Response Client and sending said string to said server processor;
- comparing (901) said received Response Client string with the Response Client being generated on the server side by re-processing said first and second Personal Identification Numbers (PIN, PIN2); and
- in case of a positive response to said comparing step (901), pointing out (903) the existence of a correct identification code; or
- in case of a negative response to said comparing step (901), pointing out (905) the existence of an incorrect or counterfeited identification code.

11. Process according to Claim 10, characterised in that said hashing is of the MD5 type and said cryptography (809) is of the 3DES type.

12. Process according to any one of Claims 6 to 11, characterised in that said encrypting step (605) comprises the following sub-steps, performed by said server processor:

- generating (1000) an encryption key from said encrypting step (809) by using as input said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page of said network;
- encrypting (1001) said received page through said generated encryption key; and
- sending (1005) said encrypted page to said client processor, said client processor being able to perform the decrypting of said encrypted page depending on said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2) being known thereto.

13. Process according to Claim 12, characterised in that said encrypting (1001) is of the Blowfish type.

14. System for authenticating a user in an Internet architecture environment, characterised in that the system comprises:

- at least one central management server processor connected in a network;
- at least one local client processor connected

in the network;

- at least one authentication device (1) according to any one of Claims 1 to 5 connected to said at least one local client processor; and
- a control program adapted to perform the process according to any one of Claims 6 to 13.

15. System for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the system comprises, connected to said device (1), a processor containing:

- at least one user library (12) for managing said device (1), said user library (12) being equipped with an identification process (14) adapted to control the enabling of said device (1);
- at least one device driver (16) connected to said user library (12), said device driver (16) being a library that manages said device (1) at connection port level; and

- at least one window (10) connected to said user library (12) to display said PIN code digit by digit.

16. System according to Claim 15, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

17. Process for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the process comprises the following steps:

- upon request of said PIN code, activating (301) a graphic window (10) to display an current digit from 0 to 9;
- sending (303) every digit of said PIN code both to the displaying window (10) and to the device (1);
- in case of actuation of activation means (7) of said device (1), storing (305) every digit as belonging to said PIN code;
- querying (307) said device (1) to check whether other digits exist;
- in case of an affirmative response to said

querying step (307), timely sending (309) the other digits; or

- in case of a negative response to said querying step (307), stopping (311) the process and storing the final PIN key to validate said device (1).

18. Process according to Claim 17, characterised in that said PIN code storing step (309) comprises the following steps:

- displaying and dispatching the digits to said device (1); and
- managing the activation means (7) of said device (1).

19. Process according to Claim 18, characterised in that said displaying and dispatching step of the digits to said device (1) comprises the following sub-steps:

- creating (403) a window (10) to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response to said querying step (405), removing (407) said displaying window (10); or

- in case of a negative response to said querying step (405), sending (409) the digit to said graphic window (10) and to said device (1); and
- requesting (411) to said device (1) whether the digits limit for the PIN code has been reached, returning to said querying step (405).

20. Process according to Claim 18, characterised in that said managing step of the activation means (7) of said device (1) comprises the following sub-steps:

- querying (503) whether the digits limit has been reached;
- in case of an affirmative response to said querying step (503), ending (509) said process; or
- in case of a negative response to said querying step (503), checking (505) whether said activation means (7) are actuated;
- in case of a negative response to said checking step (505), suspending the procedure that remains in stand-by; or
- in case of an affirmative response to said

checking step (505), storing (507) the last received digit and returning to said querying step (503).

21. Process according to Claim 17, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

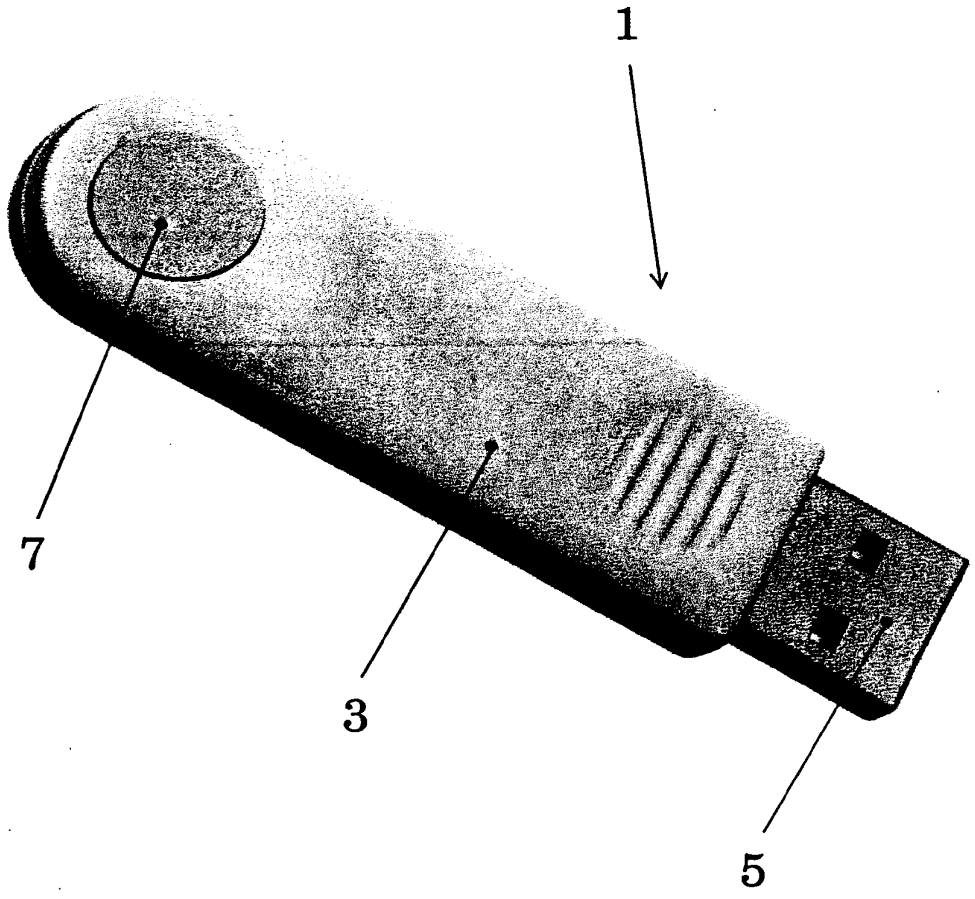


Fig. 1

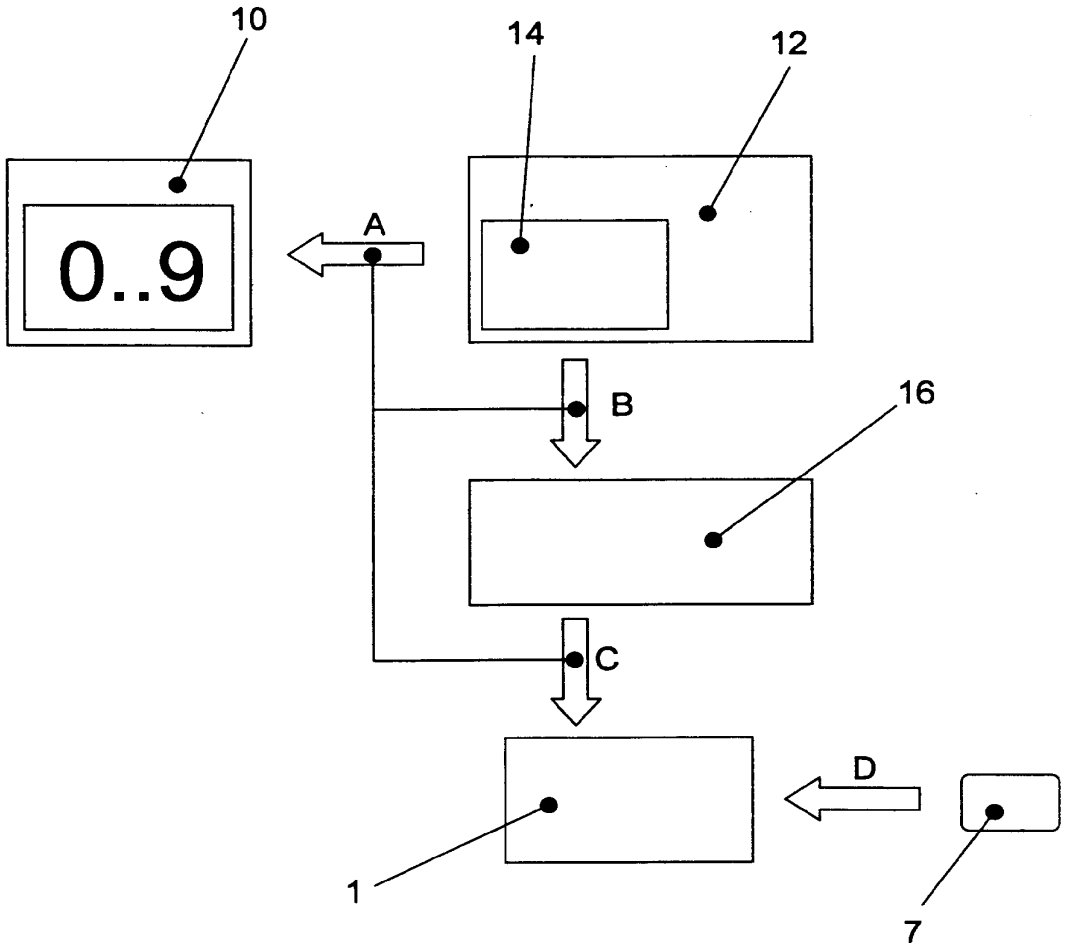


FIG. 2

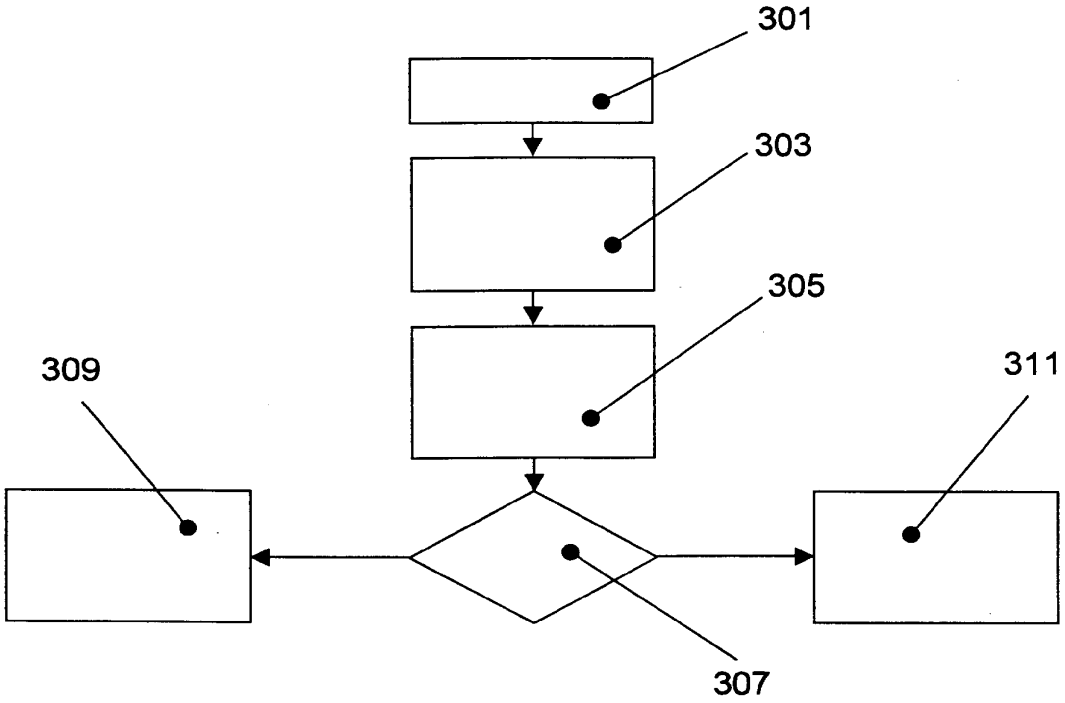


FIG. 3

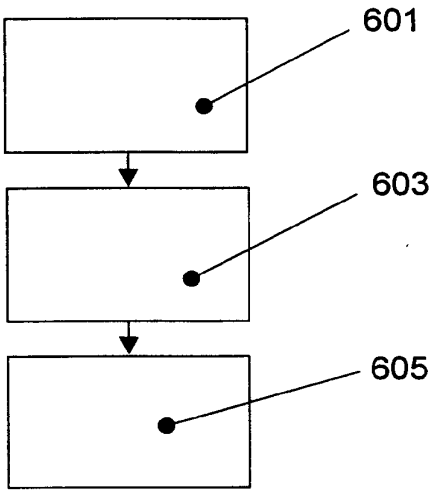


FIG. 6

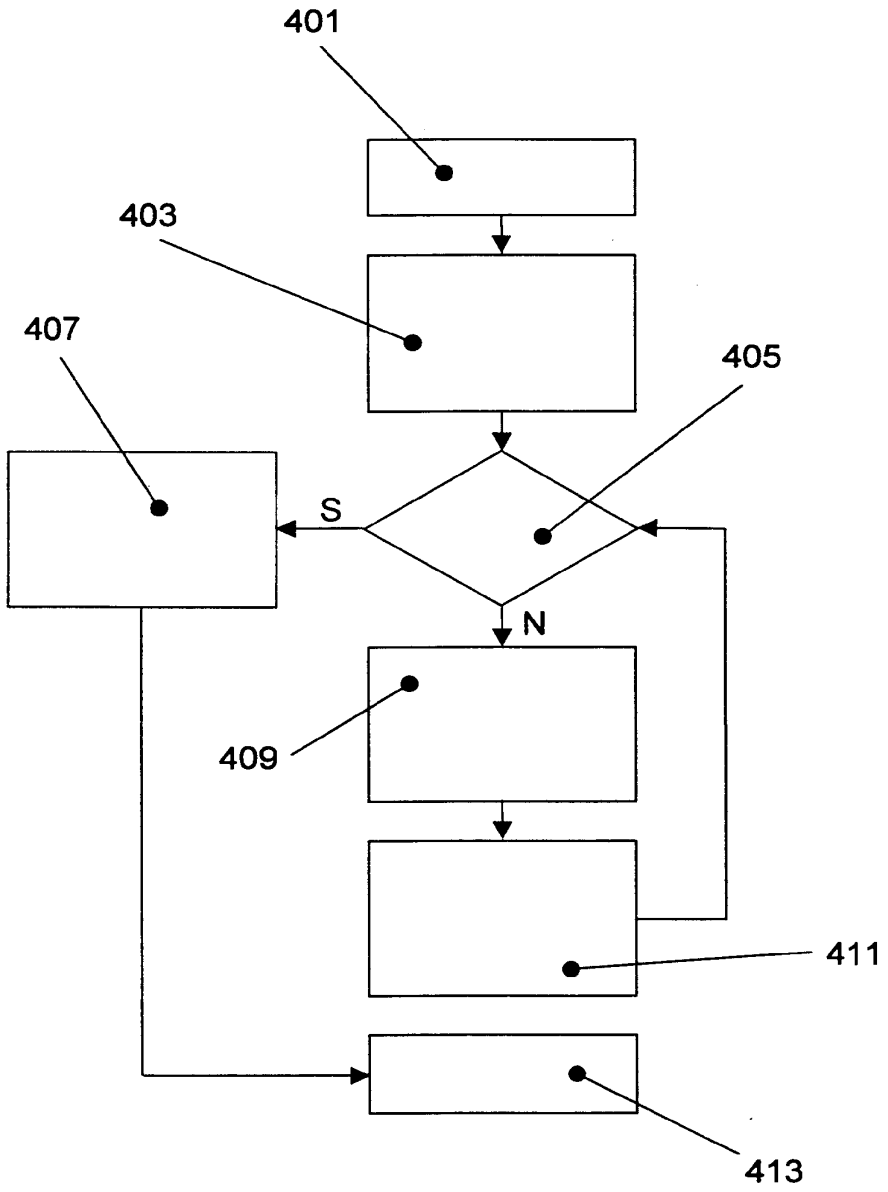


FIG. 4

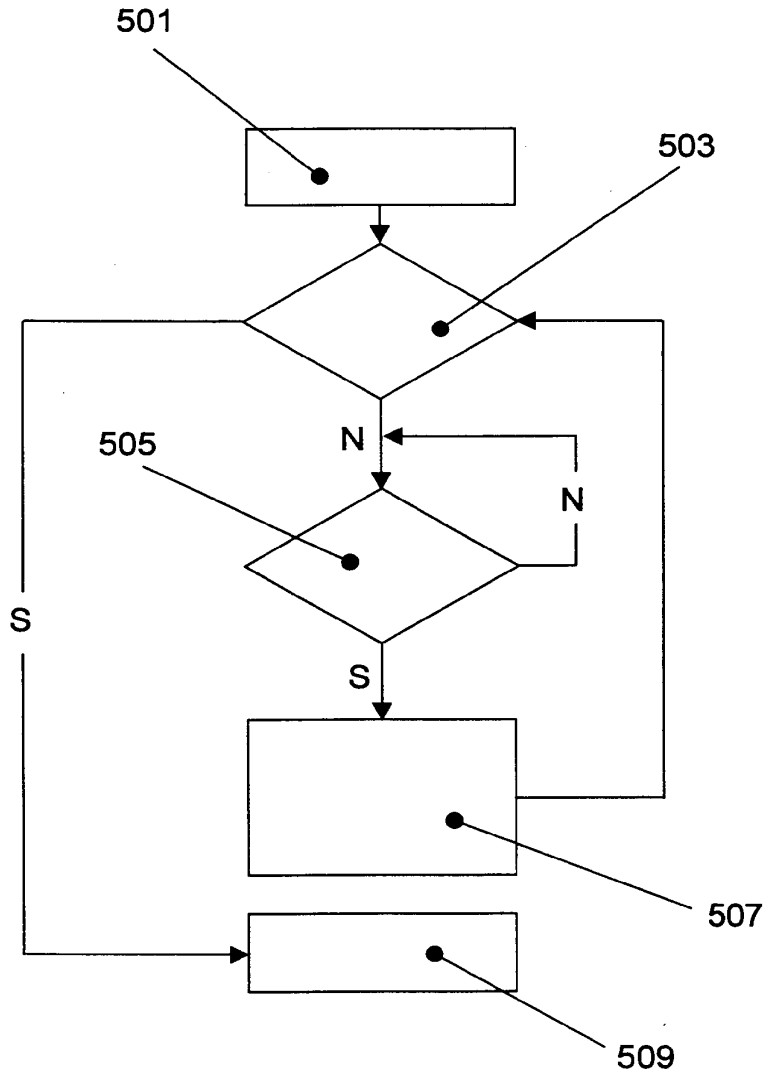


FIG. 5

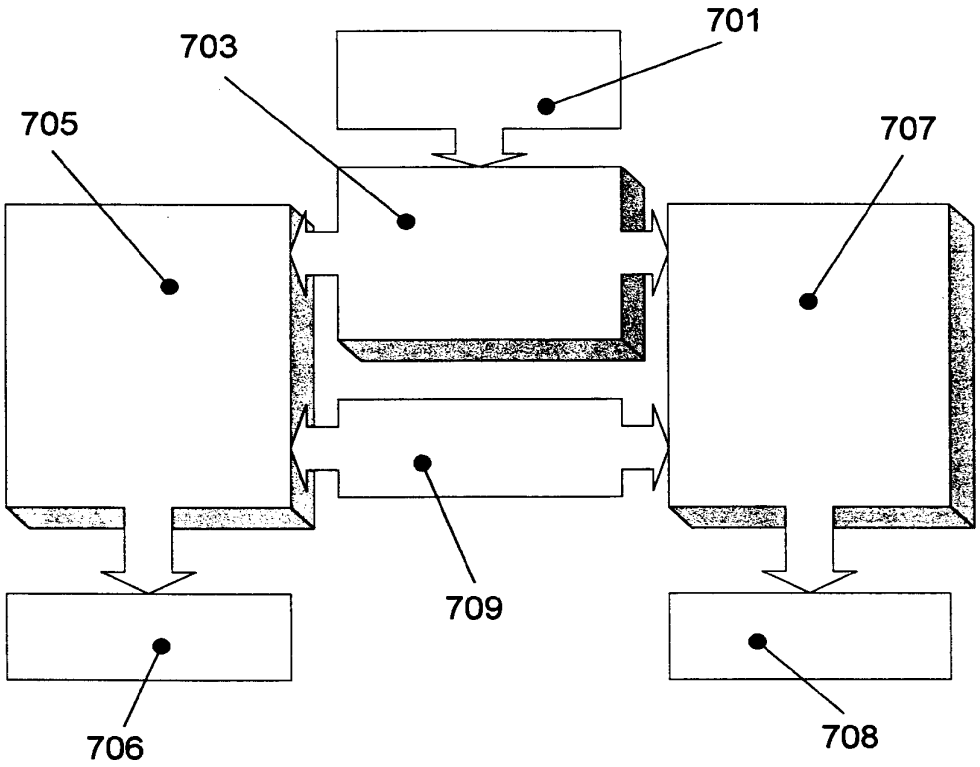


FIG. 7

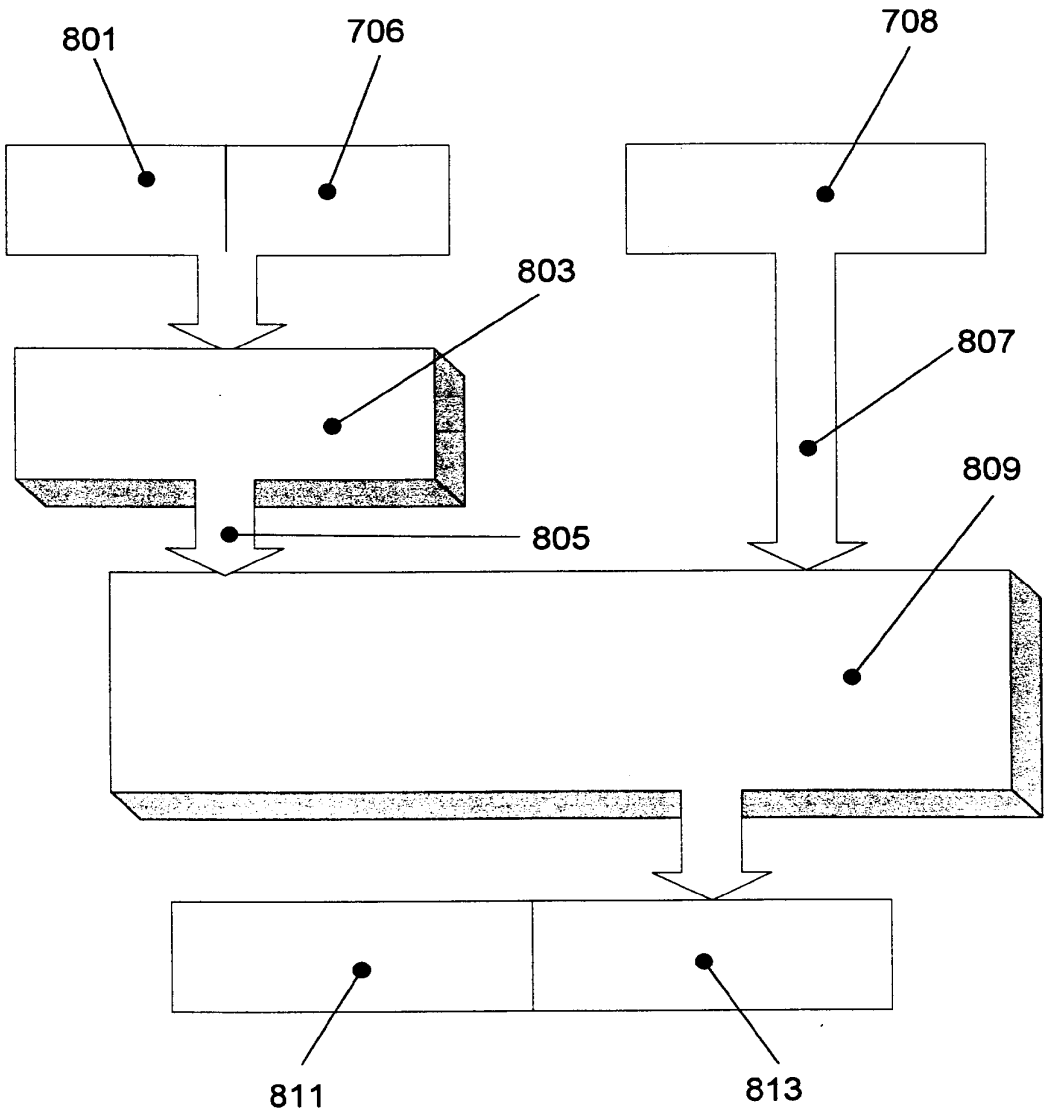


FIG. 8

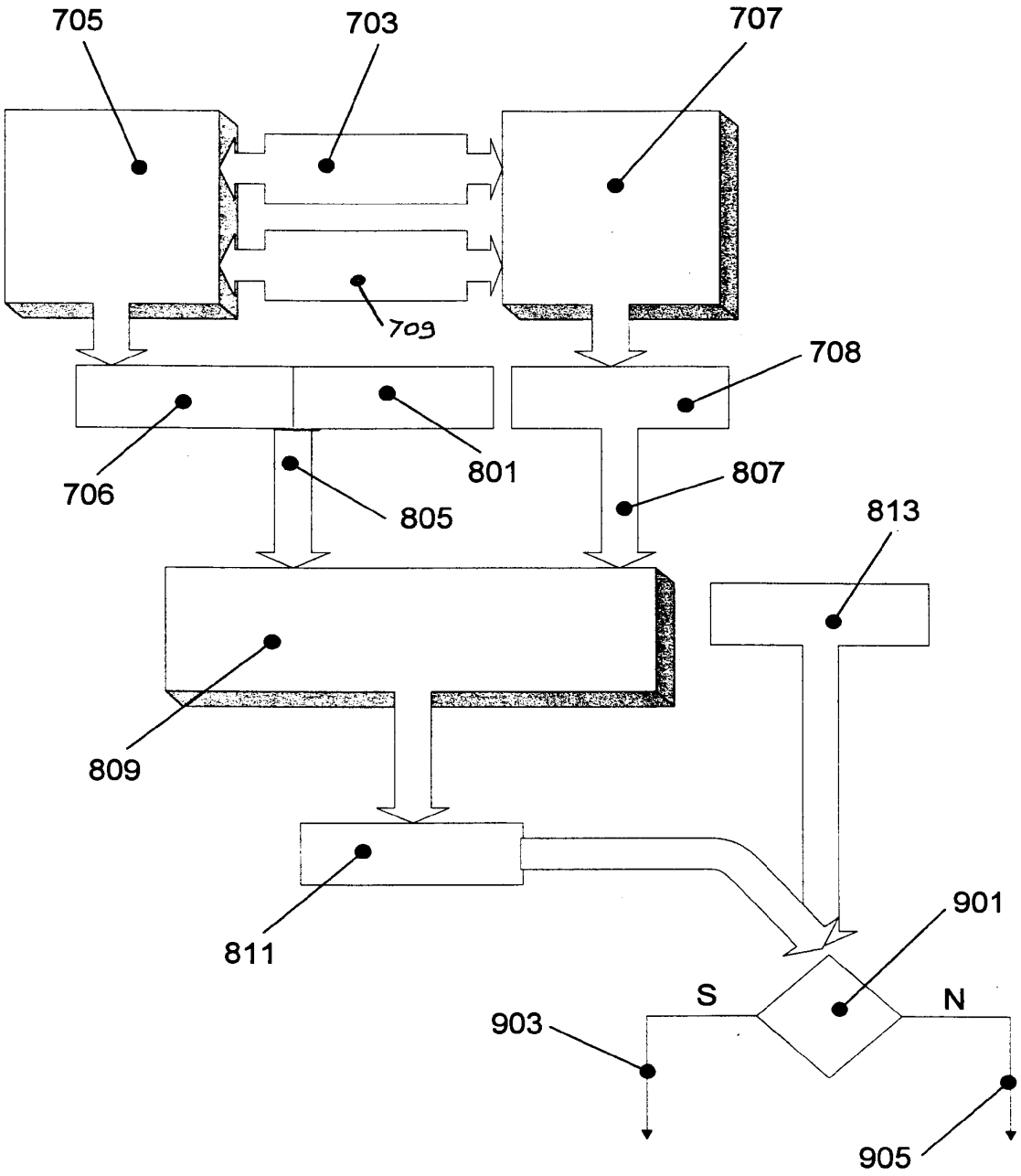


FIG. 9

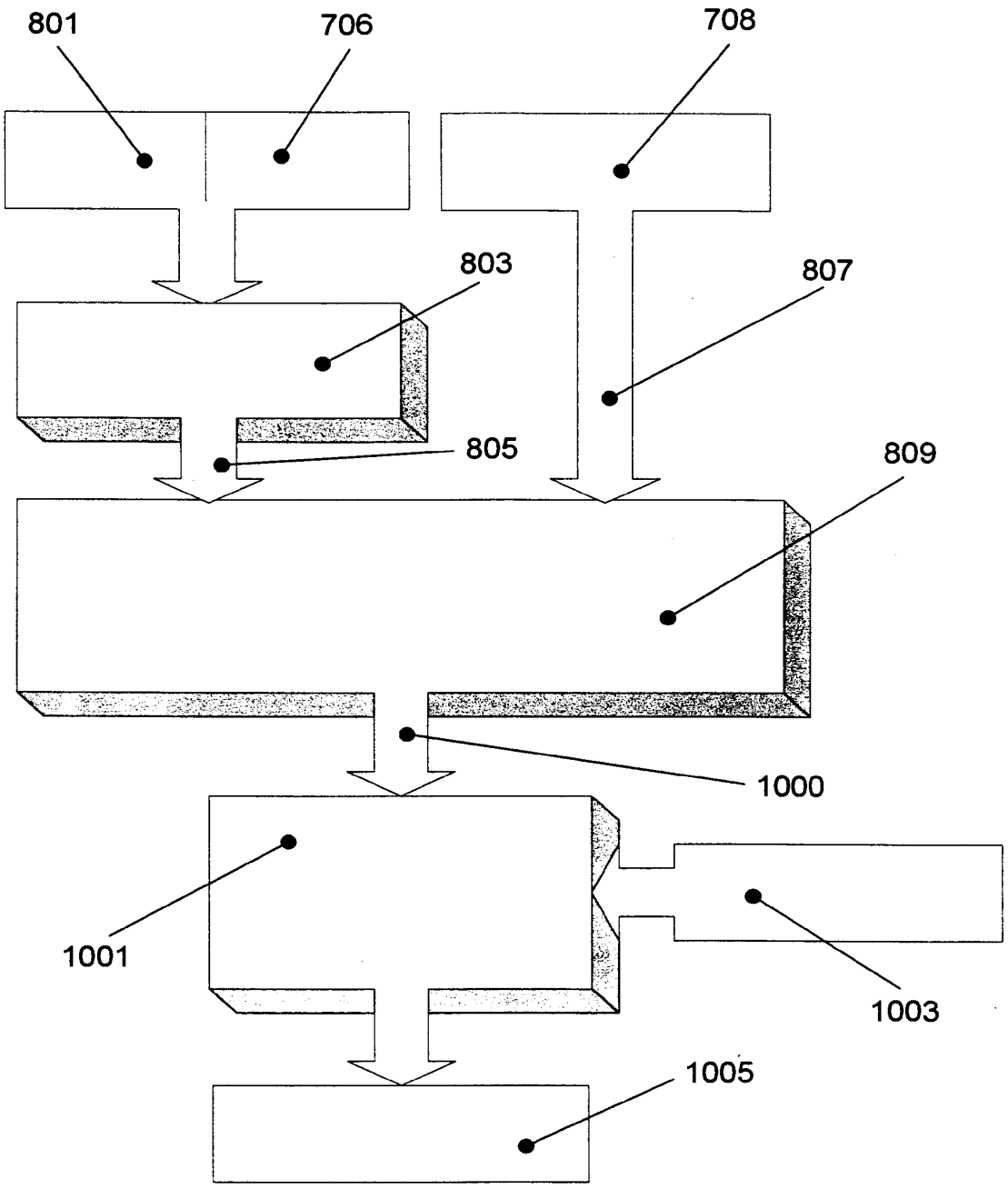


FIG. 10

INTERNATIONAL SEARCH REPORT

Int' tional Application No
PCT/IT 00/00216

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 5 778 071 A (CAPUTO ET AL) 7 July 1998 (1998-07-07) column 7, line 21 - line 36 column 10, line 51 -column 12, line 22 column 13, line 4 -column 18, line 9; figures 1D,2,4,5-8	1,3-7,14 8-13, 15-21
A	L. PREUSS: "Rainbow Technologies Adds USB Support For PC And Macintosh Software Developers To Sentinel Line" NEWS RELEASE, 17 November 1998 (1998-11-17), XP002139273 the whole document	1,2,4-7, 14,15,17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 October 2000	02/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 060 263 A (BOSEN ROBERT J ET AL) 22 October 1991 (1991-10-22) column 4, line 6 -column 5, line 24	15,17
E	WO 00 42491 A (RAINBOW TECHNOLOGIES INC) 20 July 2000 (2000-07-20) page 16, line 16 - line 20; claims 1-3,5,6; figures 7,8	1-5

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Lite tional Application No
PCT/IT 00/00216

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
US 5060263 A	22-10-1991	NONE	
WO 0042491 A	20-07-2000	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. März 2001 (01.03.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/14179 A1

(51) Internationale Patentklassifikation[7]: B60R 25/04

(21) Internationales Aktenzeichen: PCT/EP00/07769

(22) Internationales Anmeldedatum:
10. August 2000 (10.08.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 39 733.3 21. August 1999 (21.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **WITTWER, Reinhard** [DE/DE]; Beuthener Strasse 26, 42579 Heiligenhaus (DE). **BARRENBERG, Günter** [DE/DE]; Am Buschkothen 20, 42551 Velbert (DE).

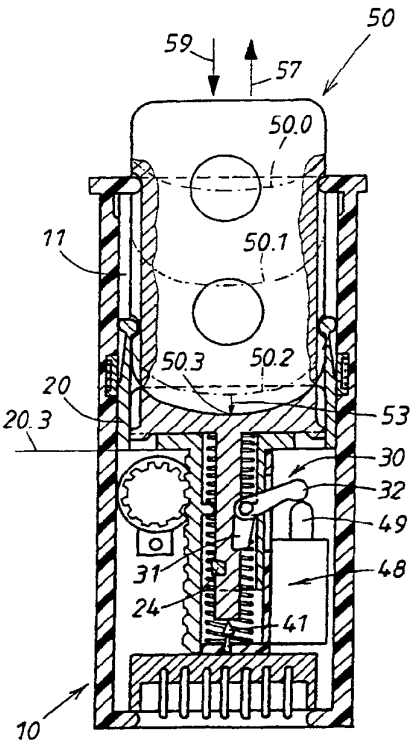
(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: DEVICE FOR STARTING A MOTOR VEHICLE MOTOR, USING AN ELECTRONIC KEY

(54) Bezeichnung: VORRICHTUNG ZUM STARTEN EINES FAHRZEUGMOTORS MITTELS EINES ELEKTRONISCHEN SCHLÜSSELS



(57) Abstract: The invention relates to a device for starting a motor vehicle motor. According to the invention, a slot is (11) used for inserting (59) the key (50) which is usually closed by a spring-loaded cover (14). The key (50) is displaced in the slot (11) into various key positions (20.1), in order to control different functions of the motor or other ancillary devices in the vehicle. In order to ensure a compact construction which is easy to use, the inventive device prevents the key (50) from turning in the slot (11) and the key (50) is displaced into at least three operating positions (20.1) for the control functions which are axially staggered. After being inserted for a first operating distance (51), the key takes up an initial position (20.1), in which it is secured in the slot (11) in a force-fit. In a subsequent second intermediate position, the key (50) is secured in a positive fit which can be locked automatically. This prevents the manual withdrawal (57) of the key (50). In order to remove the key (50), the latter is axially pushed into a third final position, in which the lock on the operating position can be released. During its course of operation, the key (50) is axially spring-tensioned (41) in the direction of the retaining position. The operating position of the key (50) determines the different vehicle functions.

(57) Zusammenfassung: Bei einer Vorrichtung zum Starten eines Motors wird eine Aufnahme (11) zum Einstecken (59) des Schlüssels (50) verwendet, die normalerweise von einer federnden Abdeckung (14) verschlossen ist. Der Schlüssel (50) wird in der Aufnahme (11) in verschiedene Schlüssellagen (20.1) überführt, um verschiedene Funktionen vom Motor oder weiteren Zusatzgeräten im Fahrzeug zu steuern. Um einen platzsparenden Aufbau und

[Fortsetzung auf der nächsten Seite]

WO 01/14179 A1

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*
— *Mit geänderten Ansprüchen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

eine einfache Betätigung zu gewährleisten, wird vorgeschlagen, den Schlüssel (50) in der Aufnahme (11) unverdrehbar zu machen und für die Steuerung den Schlüssel (50) in mindestens drei zueinander axial versetzte Hublagen (20.1) zu überführen. Nach einer ersten Hubstrecke (51) des eingeführten Schlüssels kommt der Schlüssel in einer Anfangslage (20.1), wo er in der Aufnahme (11) kraftschlüssig festgehalten wird. Eine formschlüssige Sicherung des Schlüssels (50) ergibt sich in einer dann folgenden zweiten Mittellage, welche selbsttätig verriegelbar ist. Dann ist ein manuelles Herausziehen (57) des Schlüssels (50) verhindert. Zur Entnahme des Schlüssels (50) wird dieser in eine dritte Endlage axial eingedrückt, wo die Verriegelung der Betriebslage aufgehoben werden kann. Bei diesen Hubbewegungen ist der Schlüssel (50) in Richtung auf die Haltelage axial federbelastet (41). Die verschiedenen Funktionen des Fahrzeugs werden durch die Hublage des Schlüssels (50) mitbestimmt, (Fig. 5).

Vorrichtung zum Starten eines Fahrzeugmotors mittels eines elektronischen Schlüssels

Die Erfindung richtet sich auf eine Vorrichtung der im Oberbegriff des Anspruches 1 angegebenen Art. Solche Vorrichtungen werden üblicherweise als elektronisches „Zündschloss" bzw. „Zünd-Lenk-Schloss" bezeichnet. Mit einem elektronischen Schlüssel wird üblicherweise der Zugang zum Fahrzeug gesichert und entsichert. Dafür sind geeignete Türschlösser vorgesehen. Bei der Verwendung dieses Schlüssel bei der hier interessierenden Vorrichtung wird der Schlüssel in eine im Kraftfahrzeug vorgesehene Aufnahme eingesteckt. In manchen Fällen wird dabei eine dort vorgesehene Abdeckung weggedrückt. Zur Steuerung von verschiedenen Funktionen im Kraftfahrzeug wird der eingesteckte Schlüssel in der Aufnahme in verschiedene Schlüssellagen überführt.

Bei der bekannten Vorrichtung dieser Art (DE 44 34 655 A1) werden die verschiedenen Funktionen durch entsprechende Drehstellungen des elektronischen Schlüssels in der Aufnahme angewählt. Dazu besteht die Aufnahme aus einem Rotor und einem Stator und verschiedenen Sensoren am Stator, welche die verschiedenen Drehstellungen des Rotors zu ermitteln haben. Das ist bau- und platzaufwendig. Um das erforderliche Drehmoment zur Verstellung des Schlüssels manuell ausüben zu können, muss der Schlüssel ausreichend weit aus der Öffnung der Aufnahme herausragen. Ein weit herausragender Schlüssel erhöht aber beim Crashfall des

Fahrzeugs die Verletzungsgefahr. Zusätzlich oder alternativ zur rotatorischen Bewegung kann auch eine translatorische Bewegung des Schlüssels stattfinden.

Bei einer Vorrichtung anderer Art (DE 198 14 964 A1) wird das Fahrberechtigungssignal durch eine Detektion eines Fingerabdrucks der berechtigten Person erzeugt. Dabei wird ein Autorisierungselement in Form einer Scheckkarte verwendet, welche in einen Schlitz neben einem Wippschalter oder in einem Drehschalter eingeführt wird. Der Drehschalter und der Wippschalter besitzen Sensoren für den Fingerabdruck und sind zwischen verschiedenen Schalterlagen druckbetätigbar oder verdrehbar. Dadurch werden verschiedene Funktionen des Motors gesteuert. In diesem Fall sind außer der Einsteckbewegung des Autorisierungselements sowohl eine Drehung oder Druckbewegung eines Schalters als auch die Anbringung eines Fingerabdrucks an der den Sensor aufweisenden Stelle erforderlich. Diese komplexe Betätigung ist umständlich.

Schließlich ist es bekannt, bei einem Startschalter für ein Kraftfahrzeug (DE 195 04 991 C1) in einem Drehgriff einen Schacht zur vollständigen Einführung einer Identifikationskarte vorzusehen. Diese Einführung ist nur in einer ersten Position des Drehgriffs möglich. Von dieser Position ausgehend kann dann der Drehgriff mit der eingesteckten Karte in verschiedene weitere Drehpositionen überführt werden, welche verschiedene Funktionen des Motors steuert. In diesem Fall sind außer den Steckbewegungen auch noch rotative Bewegungen des Drehgriffs erforderlich.

Der Erfindung liegt die Aufgabe zugrunde, eine zuverlässige, bequem betätigbare Vorrichtung der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, welche die vorerwähnten Nachteile vermeidet. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Bei der Erfindung wird der Schlüssel zur Funktionsauswahl nicht gedreht. Der Schlüssel wird vielmehr beim Einschieben in die Aufnahme in drei zueinander axial versetzte Hublagen überführt, von denen aber für die Zündung des Motors die zweite Hublage maßgeblich ist. In dieser zweiten Hublage ist der Schlüssel nahezu ganz in

der Aufnahme eingeführt. In dieser zweiten Hublage und in der noch tieferen dritten Hublage werden die wesentlichsten Funktionen im Kraftfahrzeug ausgeführt, wofür fallweise weitere manuelle Betätiger oder Pedale genutzt werden. Der Kraftfahrzeugbenutzer braucht nicht am Schlüssel Betätigungen auszuführen, um die gewünschten Funktionen im Fahrzeug auszulösen. Der Schlüssel bleibt vielmehr in der Aufnahme weitgehend versenkt, weshalb im Crashfall keine Verletzungsgefahr durch weit herausragende Schlüsselteile zu befürchten ist.

In seiner zweiten Hublage ist der Schlüssel durch ein Richtgesperre in der Aufnahme fixiert, dessen formschlüssige Haltemittel den Schlüssel gegenüber einer axialen Federkraft sichern. Um den Schlüssel wieder entnehmen zu können, genügt es ihn an seinem Ende anzutippen. Dann wird der Schlüssel in seine dritte Hublage überführt. Das Schlüsselende kann sich dabei beliebig tief in der Aufnahme befinden. In dieser dritten Hublage kann die Verriegelung fallweise freigegeben werden. Dann wird der Schlüssel aufgrund einer auf ihn mittelbar oder unmittelbar einwirkenden axialen Rückstellfederung wieder in seine Anfangslage zurückgedrückt. Dann liegt nur eine kraftschlüssige Verbindung eines Rastgesperres vor. Der Schlüssel kann manuell wieder entnommen werden. Bei der Erfindung sind folglich nur axiale Bewegungen des elektronischen Schlüssels zwischen mindestens drei Hublagen erforderlich, um den Motor oder weitere Zusatzgeräte im Kraftfahrzeug zu steuern. Diese axiale Bewegung ist mit dem Einstecken des Schlüssels in die Aufnahme des Fahrzeugs gleichgerichtet. Es liegt also eine sehr sinnfällige Handhabung des Schlüssels bei der erfindungsgemäßen Vorrichtung vor.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung schematisch in zwei Ausführungsbeispielen dargestellt, von denen jedes der beiden von eigenständiger erfinderischer Bedeutung ist. Das erste Ausführungsbeispiel ist in den Fig. 1 bis 8 und das zweite Ausführungsbeispiel in den Fig. 9 bis 14 veranschaulicht. Es zeigen:

Fig. 1, einen Axialschnitt durch die Vorrichtung des ersten Ausführungsbeispiels, längs der Schnittlinie I - I von Fig. 3, wobei die Bauteile sich in einer Ausgangsstellung vor dem Einstecken eines zugehörigen elektronischen Schlüssels befinden,

Fig. 2 die in Fig. 1 gezeigte Vorrichtung in einem demgegenüber rechtwinklig versetzten Axialschnitt, der in Fig. 3 mit II - II gekennzeichnet ist, bei gleicher Stellung der Bauteile,

Fig. 3 einen Querschnitt durch die Vorrichtung, längs der in Fig. 1 mit III - III gekennzeichneten Schnittlinie,

Fig. 4 die stirnseitige Draufsicht auf die Vorrichtung von Fig. 1 bis 3,

Fig. 5, in einer der Fig. 1 entsprechenden Darstellung eine erste Hublage der Bauteile, die sich nach einem anfänglichen Einstecken des elektronischen Schlüssels ergibt,

Fig. 6 eine durch weiteres axiales Einstecken des Schlüssels in die Aufnahme von Fig. 5 sich ergebende zweite Hublage der Bauteile der in Fig. 1 gezeigten Vorrichtung,

Fig. 7 eine gegenüber Fig. 6 noch ein wenig tiefer liegende Hublage des eingesteckten Schlüssels, um ihn aus der zweiten Hublage von Fig. 6 in die in Fig. 5 erläuterte erste Hublage zu überführen,

Fig. 8 die Vorderansicht auf eine im Gehäuse der Vorrichtung vorgesehene Leiterplatte, teilweise im Einbauzustand im Gehäuse,

Fig. 9 in Analogie zu Fig. 6, einen entsprechenden Axialschnitt durch das zweite Ausführungsbeispiel der erfindungsgemäßen

Vorrichtung, wenn sich der Schlüssel in seiner zweiten Hublage befindet,

Fig. 10 die in Fig. 9 gezeigte zweite Vorrichtung nach der Erfindung bei gleicher Stellung der Bauteile, allerdings in einem gegenüber Fig. 9 rechtwinklig versetzten Axialschnitt durch die Vorrichtung,

Fig. 11 nur einige Bauteile der in Fig. 9 gezeigten Vorrichtung in einer Ausgangsstellung, die sich bei einem aus der Vorrichtung entnommenen Schlüssel ergibt und

Fig. 12-14, in einer der Fig. 11 entsprechenden Darstellung, die Stellung der Bauteile, wenn sich der Schlüssel in drei verschiedenen Hublagen befindet, in Analogie zu den in Fig. 5, 6 und 7 gezeigten Schlüssellagen des ersten Ausführungsbeispiels.

Das in Fig. 1 bis 8 gezeigte erste Ausführungsbeispiel der erfindungsgemäßen Vorrichtung besitzt eine Aufnahme 11 zum Halten eines elektronischen Schlüssels. Die Aufnahme 11 befindet sich im Inneren eines Gehäuses 10. Dieses Gehäuse 10 kann in einer Armatur im Fahrzeuginneren integriert sein, deren Kontur 12 strichpunktiert in Fig. 1 und 2 angedeutet ist. Die Fig. 1 bis 4 zeigen die Vorrichtung bei entnommenen Schlüssel 50. Dann ist die stirnseitige Öffnung 13 der Aufnahme 11 durch eine Abdeckung 14 verschlossen.

Die Abdeckung 14 ist relativ zu einem im Gehäuse 10 vorgesehenen Schieber 20 mit einer leichten Druckfeder 15 belastet und dort zwischen zwei Stellungen, nämlich 14.1 von Fig. 1 und 14.2 axial von Fig. 5 verschieblich. Diese beiden Stellungen 14.1 und 14.2 sind durch einen vorderen und einen hinteren Endanschlag 22, 29 im Schieber 20 bestimmt. Bei entnommenen Schlüssel gemäß Fig. 1 bis 4 liegt die vordere Ausschubstellung 14.1 der Abdeckung 14 vor, wo die Öffnung 13 verschlossen ist. Dann kann Schmutz in das Innere der Aufnahme 11 nicht eindringen. Die Abdeckung 14 befindet sich dann, unter Wirkung ihrer Druckfeder

15 am vorderen Endanschlag 22. Die andere Stellung 14.2 gemäß Fig. 5 wird auf folgende Weise erreicht.

Damit der Schlüssel 50 mit der Vorrichtung zusammenwirken kann, ist eine durch den Pfeil 59 in Fig. 1 und 2 verdeutlichte Einsteckbewegung des Schlüssels 50 in die Aufnahme 11 erforderlich. Dabei kommt der Schlüssel mit der Abdeckung 14 in Berührung. Das ist die strichpunktiert in Fig. 1 und 2 verdeutlichte axiale Lage 50.0. Dabei taucht der Schlüssel mit einem Vorderstück 58 in eine entsprechende Aussparung der Abdeckung 14 bereits ein, welche zu der nachfolgenden Aufnahme 11 im Gehäuse 10 noch hinzukommt. Diese Lage 50.0 des Schlüssels 50 soll nachfolgend kurz „Berührungslage" bezeichnet werden. Davon ausgehend sollen alle weiteren Hublagen des Schlüssels anhand von Fig. 5 bis 7 beschrieben werden.

Nach einer anfänglichen Einsteckbewegung 59 um eine aus Fig. 5 ersichtliche erste Hubstrecke 51 kommt der Schlüssel in seine in Fig. 5 mit 50.1 gekennzeichnete erste axiale Hublage. Dabei wird, wie bereits erwähnt wurde, die Abdeckung 14 zurückgedrückt und kommt an ihrem zweiten Endanschlag 29 im Inneren des Schiebers 20 zur Anlage. Die Öffnung 13 der Aufnahme ist zwar frei, aber jetzt durch den eingesteckten Schlüssel 50 verschlossen. Die Abdeckung 14 befindet sich dann in ihrer Einschubstellung 14.2. In dieser Hublage 50.1 wird der Schlüssel 50 kraftschlüssig in seiner Aufnahme 11 gehalten wofür die Halteelemente 21, 22, 55 sorgen, deren Aufbau am besten anhand von Fig. 1 zu erkennen ist. Der Schieber 20 ist dosenförmig ausgebildet, wobei die Dosenwand stellenweise eine radial federnde Zunge 21 aufweist, welche ein erstes Halteelement bildet. Diese Zunge 21 ist zunächst ein erster Bestandteil eines zwischen Schlüssel 50 und Schieber 20 bestehenden Rastgesperres. Am Ende der Zunge 21 befindet sich nämlich ein radialer Vorsprung 22, der ein weiteres Halteelement des Rastgesperres darstellt. Dieser Vorsprung 22 kann im Übrigen auch die bereits erwähnten Anschlagfunktionen in der Ausschubstellung 14.1 der Abdeckung 14 erfüllen. Beim Einstecken 59 des Schlüssels 50 führen die Zungen 21 kurzzeitig eine radiale Spreizbewegung aus, bis der an den Zungen 21 sitzende Vorsprung 22 in eine zugeordnete Rastvertiefung 55 am Schlüssel kraftschlüssig eingreift. Das ist in Fig. 5 gegeben. Die Rastvertiefung 55 ist ebenfalls Bestandteil des erwähnten Rastgesperres. Diese erste Hublage 50.1

soll nachfolgend kurz „Anfangslage" des Schlüssels bezeichnet werden. In dieser Anfangslage 50.1 liegt eine kraftschlüssige Sicherung des Schlüssels in der Aufnahme 11 vor.

Die vorerwähnte Spreizbewegung der Zunge 21 beim Einstecken 59 des Schlüssels ist möglich, obwohl die Zunge 21 auf ihrer dem rastwirksamen Vorsprung 22 gegenüberliegenden Seite einen radialen Gegenvorsprung 23 aufweist. In diesem Bereich besitzt nämlich das Gehäuse 10 eine aus Fig. 1 erkennbare radiale Aussparung 16, in welche dieser Gegenvorsprung 23 beim Schlüsseleinstecken 29 radial ausweichen kann.

Ausweislich der Draufsicht von Fig. 4 ist die Öffnung 13 für die Aufnahme durch eine Blende 17 umgrenzt, die Führungsmittel 18 für den Schlüssel 50 besitzt. Diese bestehen hier aus zwei einander gegenüberliegend angeordneten Stegen 18 an der Blende 17. Die zugehörigen Führungsmittel 54 am Schlüssel bestehen, wie aus Fig. 1 und 2 hervorgeht, aus einer Längsnut. Diese beiseitigen Längsnuten 54 sorgen für ein gutes axiales Einstecken 59 des Schlüssels 50, auch wenn die Außenflächen des Schlüssels aus stilistischen Gründen nicht achsparallel ausgeführt sein sollten. Die vorerwähnte haltewirksame Rastvertiefung 55 ist im Übrigen im Bereich dieser Längsnut 54 angeordnet. Der in seine Anfangslage 50.1 von Fig. 5 befindliche Schlüssel 50 kann von Hand wieder im Sinne des Pfeils 57 von Fig. 5 manuell herausgezogen werden. Dann fährt die Abdeckung 14 wieder in ihre Ausschubstellung 40.1 von Fig. 1 zurück. Der Schlüssel kann auch in einer um 180 ° gewendeten Position eingesteckt werden.

Das Herausziehen 57 des Schlüssels ist aber verhindert, wenn der Schlüssel, ausgehend von seiner Anfangslage 50.1 von Fig. 5 um eine weitere, beträchtliche Hubstrecke 52 bis zu seiner in Fig. 6 erkennbaren zweiten axialen Hublage 50.2 überführt worden ist. Dann ist nämlich der Schlüssel 50 sogar formschlüssig in der Aufnahme 11 gesichert. An diesem Formschluss sind zunächst die gleichen Halteelemente 21, 22, 55 wie beim Rastgesperre beteiligt, das vorausgehend für den kraftschlüssigen Zusammenhalt zwischen dem Schieber 20 und dem Schlüssel 50 sorgte. Der an der federnden Zunge 21 vom Schieber 20 vorgesehene

Gegenvorsprung 23 kommt in diese Hublage 50.2 an einer aus Fig. 6 erkennbaren radialen Stützfläche 19 im Gehäuse 10 zu liegen. Diese Stützfläche 19 befindet sich unterhalb der vorausgehend in der Anfangslage 50.1 damit ausgerichteten radialen Aussparung 16. In seiner Hublage 50.2 wird also der Schlüssel 50 in der Aufnahme 14 formschlüssig verriegelt. Ein Herausziehen 57 im Sinne des auch in Fig. 6 eingezeichneten Pfeils ist nicht möglich. Diese zweite Hublage 50.2 des Schlüssels soll nachfolgend kurz „Mittellage" bezeichnet werden.

Die axiale Position des Schiebers 20 von Fig. 5 oder 6 wird durch eine weitere Einsteckbewegungen 59 des Schlüssels 50 erreicht. In Fig. 5 befindet sich der Schieber 20 in einer dort mit 20.1 gekennzeichneten Ausgangsposition, welche die äußere Position des Schiebers im Gehäuse 10 ist. Diese Ausgangsposition 20.1 liegt im Übrigen auch in Fig. 1 bzw. Fig. 2 vor, wo der Schlüssel 50 ganz entfernt ist oder mit der Abdeckung 14 in Berührung 50.0 kommt. Die vorgenommene Hublage 50.2 des Schlüssels 50 ist zunächst gesichert, weil der den Schlüssel 50 aufnehmende Schieber 20 in der zugehörigen Axialposition 20.2 verriegelt wird. Dafür dient ein hier als federnde Klinke 30 ausgebildeter Riegel, der einen Sperrarm 31 und einen damit drehfesten Stellarm 32 aufweist. Der Riegel 30 ist bei 33 ortsfest im Gehäuse 10 schwenkbar gelagert und greift mit seinem Sperrarm 31 in den Betätigungsweg einer Schulter 24, die beim Axialbewegen des Schiebers 20 mitbewegt wird. Die Schulter 24 befindet sich hier an einem Nocken, der Bestandteil eines aus Fig. 5 erkennbaren Axialansatzes 25 des Schiebers 20 ist. Der Axialansatz 25 taucht beim Bewegen des Schiebers 20 entlang der Hubstrecke 52 teleskopartig in eine gehäusefeste Hülse 45 ein.

Die Gehäusehülse 45 und der Axialansatz 25 dienen im Übrigen auch zur Aufnahme einer kräftigen Rückstellfeder 40, die bestrebt ist, den Schieber 20 in dessen Ausgangsposition 20.1 zu halten. Dazu ist zweckmäßigerweise auch der Axialansatz 25 vom Schieber 20 rohrförmig ausgebildet und besitzt einen Innenbund 26 an dem sich das obere Ende der Rückstellfeder 40 abstützt. Der obere Bereich dieses rohrförmigen Axialansatzes 25 kann seinerseits als Aufnahme für die bereits oben beschriebene Abdeck-Druckfeder 15 dienen, die demgegenüber sehr viel weicher ausgebildet ist. Die Rückstellfeder 40 übt auf den Schieber 20 eine durch den Pfeil

41 in Fig. 5 verdeutlichte Rückstellkraft aus. Dadurch wird der Schieber 20 gegen einen gehäusefesten Endanschlag 42 gedrückt, der hier durch die Innenfläche der beschriebenen Blende 17 gebildet wird. Dieser Anschlag 42 bestimmt die Ausgangsposition 20.1 des Schiebers 20. Der Nocken mit der Schulter 24 befindet sich in der Ausgangsposition 20.1 des Schiebers 20 noch axial oberhalb der Klinke 30.

Die Schulter 24 wirkt mit der Klinke 30 nach Art eines sogenannten „Richtgesperres" zusammen. Der Sperrarm 31 befindet sich mit seinem Sperrende in dem durch eine Punktlinie 27 in Fig. 5 veranschaulichten Verschiebungsweg 27 der Schulter 24. Bei der Einsteckbewegung 59 von Fig. 5 fährt der die Schulter 24 tragende Nocken gegen den Sperrarm 31 der Klinke 30 und drückt diese weg, bis die Schulter 24 in ihrer aus Fig. 6 ersichtliche Position gekommen ist. Dann schnappt der Sperrarm 31 vor die Schulter 24 und hält den Schieber 20, gegen die axiale Federbelastung 41 in der Axialposition 20.2 fest. Eine Rückbewegung des Schiebers 20 in die vorausgehende Axialposition 20.1 ist zunächst nicht möglich.

Die der Mittellage 50.2 des Schlüssels 50 von Fig. 6 entsprechende Axialposition 20.2 des Schiebers 20 soll als „Arbeitsposition" bezeichnet werden. In dieser Mittellage 50.2 erkennt zunächst eine elektronische Steuereinheit der Vorrichtung z.B. auf elektrischem oder elektromagnetischem Weg, dass es sich um den richtigen Schlüssel 50 handelt. Als Identifikationsmittel dient im vorliegenden Fall ein im Gehäuse 10 integrierter Transponder 43, der Bestandteil der nicht näher gezeigten elektrischen Steuereinheit ist. Wenn die Übereinstimmung des Schlüssels 50 mit der Vorrichtung festgestellt ist, schaltet die Steuereinheit ihre elektrischen Ausgänge und/oder Eingänge wirksam. Eine bis dahin bestehende eventuelle Sperre der Fahrzeuglenkung wird entriegelt. Vor allem werden Sensoren 44 wirksam gesetzt, die zu einem hier manuell bedienbaren Betätiger 35 gehören. Mit diesen Sensoren 44 werden die gewünschten verschiedenen Funktionen im Fahrzeug ausgewählt.

Der Betätiger 35 besteht im vorliegenden Fall aus einem Taster, der, wie am besten aus Fig. 2 und 8 zu erkennen ist, in einem Nachbarbereich des gleichen Gehäuses 10 integriert sein kann. Der Taster 35 ist aufgrund einer Axialführung 34 im Sinne des

Druckpfeils 36 von Fig. 8 axial betätigbar und wird mittels einer Rückstellfeder 37 und entsprechende Endanschläge in seine Ausgangsstellung von Fig. 2 zurückgeführt. Welche Betätigungen zu welchen Funktionen im Fahrzeug führen, hängt von der Programmierung der elektrischen Steuereinheit ab. Eine Möglichkeit besteht darin, dass beim ersten Drücken 38 des Tasters 35 ein Radio sowie eine Elektronik im Fahrzeug eingeschaltet wird, z.B. das Parklicht, der Antrieb für Fensterheber, die motorische Sitzverstellung und das Schiebedach. An der Funktionssteuerung der Elektronik können auch noch andere, an sich übliche Steuerglieder im Fahrzeug beteiligt sein, z.B. die Fußbremse. Die vorerwähnte Radioeinstellung erfolgt in diesem Fall ohne Betätigung der Fußbremse. Die weiteren Funktionen im Fahrzeug können auf folgende Weise ausgelöst werden.

Durch ein zweites Drücken 36 des Tasters 35, ohne gleichzeitige Betätigung der Fußbremse, erfolgt beispielsweise die Zündung des Motors. Wird der Taster 35 gedrückt 36 und gleichzeitig die Fußbremse getreten, dann startet der Motor. Wird daraufhin der Taster 35 nochmals gedrückt 36, so geht der Motor wieder aus. Letzteres kann dann mit oder ohne Betätigung der Fußbremse erfolgen.

Diese Funktionen können auch optisch im Bereich des Tasters 35 angezeigt werden, wie am besten anhand von Fig. 8 zu entnehmen ist. Über die Steuerelektronik wird bei der Funktion „Start" eine erste Diode 46 angesteuert, die ein Teil-Schriftfeld 38 des Tasters 35 gemäß Fig. 4 beleuchtet. Lichttrennwände 39 sorgen für eine entsprechende Teilbelichtung auf der Schauseite des Tasters 35. Bei der Funktion „Stop" wird durch die Steuereinheit dagegen eine zweite Diode 46' bestromt, worauf dann im Nachbar-Schriftfeld 38' die Beleuchtung eingeschaltet wird und die schauseitige Beschriftung im Taster 35 ablesbar macht.

Die Verriegelung des Schlüssels 50 in der Mittellage 50.2 erfolgt, wie oben beschrieben wurde, durch den Sperrarm 31 der Klinke 30, der über die Schulter 24 auch den Schieber 20 in dessen entsprechende Arbeitsposition 20.2 festhält. Die Klinke 30 befindet sich aufgrund ihrer nicht näher gezeigten Drehfederbelastung und entsprechender Drehanschläge normalerweise in ihrer Sperrposition von Fig. 6. Der Schlüssel 50 ist dabei größtenteils in der Aufnahme 11 versenkt angeordnet und ragt

nur mit einem minimalen Endstück 56 aus der Aufnahme 11 gemäß Fig. 6 heraus. Um den Schlüssel 50 aus der Mittellage 50.2 lösen zu können, muss der Schlüssel 50 zunächst in eine noch tiefere Hublage 50.3 gemäß Fig. 7 im Sinne des dortigen Einsteckpfeils 59 eingedrückt werden. Diese Hublage 50.3 kurz „Endlage" bezeichnet werden. In Fig. 7 sind die vorausgehenden Hublagen 50.0 bis 50.2 ebenfalls strichpunktiert eingezeichnet.

Zum Übergang von Fig. 6 auf Fig. 7 wird der Schlüssel 50 nur noch um eine verhältnismäßig kleine dritte Hubstrecke 53 gemäß Fig. 7 gegen die axiale Federkraft 41 eingedrückt. Der Schlüssel erreicht dann seine unterste dritte Hublage 50.3, welche natürlich wieder einer entsprechenden Endposition 20.3 des Schiebers 20 entspricht. Diese Endposition 20.3 wird von weiteren Sensoren 47 erfasst, die zu der erfindungsgemäßen Steuereinheit gehören. Im Ansprechfall schaltet die Steuereinheit einen Antrieb 48 ein, der hier aus einem elektrischen Hubmagneten besteht. Dieser Hubmagnet 48 bewegt einen Stößel 49 od. dgl. in eine Arbeitsposition, in welcher er den vorerwähnten Stellarm 32 der Klinke 30 trifft. Weil der Stellarm 32 drehfest mit dem Sperrarm 31 ist, wird durch diese Schwenkbewegung gemäß Fig. 7 der Sperrarm 31 aus seiner bisherigen Sperrposition wegbewegt. Die Schulter 24 wird freigegeben. Die Blockade des Schiebers 20 ist dann aufgehoben. Der Schieber 20 wird aufgrund der wirkenden Federkraft 41 im Sinne des Bewegungspfeils 57 von Fig. 7 automatisch zurückbewegt. Der Sperrarm 31 bleibt dabei solange durch den Hubmagneten 48 in seiner entriegelten Position von Fig. 7, bis die mit dem Schieber 20 mitbewegliche Schulter 24 sich an seinem Sperrende vorbeibewegt hat; d.h. bis kurz nach der aus Fig. 6 erkennbaren Mittellage 50.2 des Schlüssels.

Nach der Entriegelung von Fig. 7 bewegt die axiale Federkraft 41 den Schieber 20, und mit ihm den Schlüssel 50 bis sich wieder die Verhältnisse von Fig. 5 ergeben. Der Schieber 20 stoppt erst in seiner dortigen Ausgangsposition 20.1, wo die Federkraft 41 von dem erwähnten Endanschlag 42 für den Schieber 20 aufgenommen wird. Der Schlüssel 50 steckt aber immer noch in seiner Aufnahme 11. Jetzt ragt der Schlüssel 50 allerdings mit einem größeren Teilstück 28 aus der Aufnahme 11 heraus. Er kann mit der Hand bequem erfasst und manuell ganz im Sinne des Pfeils

57 herausgezogen werden. In der Anfangslage 50.1 von Fig. 5 liegt nämlich wieder die beschriebene kraftschlüssige Halterung des Schlüssels 50 im Schieber 20 vor.

Durch eine plötzliche Rückstellbewegung des Schiebers 20 aus der Endposition von Fig. 2.3 in die Ausgangsposition 20.1 von Fig. 5 könnte der Schlüssel 50 Beschleunigungskräften ausgesetzt sein, die ihn aus der Aufnahme 11 heraus katapultieren, über seine kraftschlüssige Anfangslage 50.1 in Fig. 5 hinaus. Dies lässt sich leicht durch eine geeignete Dämpfungseinrichtung 60 beheben. Diese besteht im vorliegenden Fall aus einem Dämpfungsrad 60, das ortsfest im Gehäuse 10 bei 61 drehgelagert ist, wie aus Fig. 1 und 2 zu erkennen ist. Das Dämpfungsrad 60 steht über ein Stirnrad 62 in Zahneingriff mit einer Zahnstange 63, die mit dem Schieber 20 mitbeweglich ist. Die Zahnstange 63 kann in den vorerwähnten Axialansatz 25 gemäß Fig. 1 und 2 integriert sein, wo auch der Nocken für die Schulter 24 sitzt. Sofern als Sensor 47 ein Mikroschalter verwendet wird, kann der entsprechende Schaltnocken 64 an diesem Ansatz 25 sitzen.

Die erwähnte Steuereinheit ist über die am unteren Gehäuseende vorgesehenen Steckkontakte 65 mit den elektrischen Bauteilen im Inneren des Gehäuses 10 verbunden. Man kann dazu eine auch aus Fig. 8 erkennbare Leiterplatte 66 nutzen, die durch geeignete Zwischenböden 67 in ihrer Position im Inneren des Gehäuses gemäß Fig. 3 gehalten wird.

Wie erwähnt wurde, wird der Schlüssel 50 aus seinem Formschluss in Fig. 6 über Fig. 7 auf elektromechanische Weise freigegeben und selbsttätig in seine Anfangslage 50.1 von Fig. 5 zurückgeführt. Die Bedingung hierfür, welche die erwähnte elektrische Steuereinheit überwacht, ist, dass der Motor des Fahrzeugs ausgeschaltet ist. Wenn man, bei eingeschaltetem Motor, in der Mittellage 50.2 den Schlüssel 50 eindrückt, so wird der beschriebene Hubmagnet 48 nicht wirksam gesetzt; die Klinke 30 bleibt sperrwirksam und fängt den Schlüssel wieder in der Mittellage 50.2 von Fig. 6. Damit ist eine Fehlbedienung der erfindungsgemäßen Vorrichtung ausgeschlossen.

Eine Alternative kann aber darin bestehen, dass bei stehendem Fahrzeug, wo die Räder sich nicht mehr drehen, der Motor noch an ist. Auch dies wird von der elektrischen Steuereinheit registriert. Wird dann wieder im Sinne von Fig. 7 auf den Schlüssel 50 gedrückt, so kann über einen Impulsschalter der Motor ausgeschaltet werden. Der beschriebene Formschluss des Schlüssels 50 wird dann wieder elektromechanisch freigegeben und kann über die Kraftschlussraste aus einer Anfangslage 50.1 in Fig. 5 manuell entnommen werden.

Wie bereits erwähnt wurde, zeigen die Fig. 9 bis 14 den Aufbau und die Wirkungsweise eines zweiten Ausführungsbeispiels der erfindungsgemäßen Vorrichtung, welcher eine eigenständige erfinderische Bedeutung zukommt. Zur Benennung analoger Bauteile sind die gleichen Bezugszeichen wie im ersten Ausführungsbeispiel verwendet, weshalb insoweit die bisherige Beschreibung gilt. Es genügt lediglich auf die Unterschiede einzugehen. Bei dieser Vorrichtung besitzt der Schlüssel 50 die Form einer Scheckkarte.

Die stirnseitige Öffnung 13 der dortigen Aufnahme 11 besteht aus einem Schlitz im Gehäuse 10. Die Abdeckung 14' der Öffnung 13 erfolgt hier durch eine Klappe, deren Aufklapplage in Fig. 10 ausgezogen und deren Zuklapplage bei entnommenem Schlüssel in Fig. 10 strichpunktiert angedeutet ist. Identifikationsmittel für den Schlüssel 50 sind im Gehäuse 10 integriert und bestehen auch in diesem Fall z.B. aus einem Transponder 43. Einen Schieber 20, wie im ersten Ausführungsbeispiel, gibt es nicht. Die Haltemittel und Verriegelungen wirken unmittelbar mit dem Schlüssel 50 zusammen, dessen am besten aus Fig. 11 erkennbarer Scheckkartenumriss 68 in geeigneter Weise profiliert ist. Auch in diesem Fall kann der Schlüssel 50 in der Aufnahme 11 in drei axiale Hublagen 50.1, 50.2 und 50.3 überführt und positioniert werden. Diese drei Hublagen sind in Fig. 9 durch Höhenlinien veranschaulicht und in Fig. 12 bis 14 zusammen mit den damit zusammenwirkenden Bauteile verdeutlicht.

Beim Einschieben 59 des Schlüssels 50 wird zunächst die in Fig. 12 gezeigte Anfangslage 50.1 des Schlüssels 50 erreicht, wo der Schlüssel 50 durch ein Rastgesperre 70 kraftschlüssig im Gehäuse 10 gesichert ist. Auch in diesem Fall besteht das Halteelement 71 aus einer radial federnden Zunge, doch ist diese, im

Gegensatz zum ersten Ausführungsbeispiel, ortsfest im Gehäuseinneren positioniert. Zum Rastgesperre 70 gehört eine Rastvertiefung 55 im Schlüssel 50, die durch ein entsprechendes Kantenprofil seines erwähnten Kantenumrisses 68 erzeugt ist. Ein radialer Vorsprung 75 an der Zunge 71 untergreift kraftschlüssig eine Haltekante 76 an der Rastvertiefung 55.

Weil es in diesem Fall, wie gesagt, einen Schieber nicht gibt, wirken in Fig. 9 angedeutete Rückstellkräfte 41 unmittelbar auf den Schlüssel 50 ein. Maßgeblich dafür sind hier doppelt vorgesehene Rückstellfedern 40, 40', die über einen zugehörigen Stößel 74 bzw. 74', welcher auf die Unterkante 69 des Schlüsselumrisses 68 drücken können. In Fig. 12 ist gerade der eine Stößel 74 in Kantenberührung und übt eine nur geringe Rückstellkraft 41 aus. Die kraftschlüssige Haltekraft der federnden Zunge 41 reicht jedenfalls aus, um die Anfangslage 50.1 des Schlüssels 50 von Fig. 12 sicherzustellen. Eine Entnahme 57 des Schlüssels ist gegen die Wirkung des Rastgesperres 70 in Fig. 12 möglich.

Auch bei diesem zweiten Ausführungsbeispiel lässt sich der Schlüssel 50 von der Anfangslage 50.1 um eine Hubstrecke 52 in die aus Fig. 13 ersichtliche zweite Mittellage 50.2 in der Aufnahme 11 der Vorrichtung weiterschieben 59. Auch in diesem Fall kommt es in der Mittellage 50.2 zu einem Formschluss. Die hierfür maßgeblichen Halteelemente 81 sind in diesem Fall, im Gegensatz zum ersten Ausführungsbeispiel, nicht Bestandteil des Rastgesperres 70, sondern gehören zu einem davon gesonderten Gesperre 80, welches eine mehrfache Funktion zu erfüllen hat. Dieses Gesperre besteht im vorliegenden Fall aus einer Klinke 80, die an einem ortsfesten Lager 84 im Gehäuse 10 schwenkgelagert ist. Eine Klinken-Federbelastung 85 ist bestrebt die Klinke 80 in ihrer aus Fig. 11 ersichtlichen Lage zu halten, wo sie mit einem Stellarm 82 auf den Betätiger 73 eines hier als Mikroschalter ausgebildeten Sensors 72 einwirkt. Dies liegt bereits bei entnommenen Schlüssel gemäß Fig. 11 vor. Dieser Stellarm 82 ist drehfest mit dem vorbeschriebenen Halteelement 81 dieses Verriegelungsgesperres 80 verbunden.

In der in Fig. 12 beschriebenen Ausgangslage 50.1 des eingesteckten Schlüssels 50 kommt das Halteelement 81 der Klinke 80 mit dem Profilbereich 79 der

Umrisskontur 68 in Berührung, durch welche die Klinke 80 gegen ihre Rückschwenkkraft 86 zurückgeschwenkt wird. Dadurch wird der Betätiger 73 des Klinken-Sensors 72 vom Stellarm 82 freigegeben. Das wird von einer auch bei dieser Vorrichtung vorgesehenen elektrischen Steuereinheit festgestellt, an die dieser Klinken-Sensor 72 angeschlossen ist. Der vorerwähnte Transponder 43 wird wirksam gesetzt und stellt fest, ob der „richtige Schlüssel" eingestellt ist. Nur beim richtigen Schlüssel werden bereits erste Funktionen im Fahrzeug von der Steuereinheit eingeschaltet, z.B. die Spannungsversorgung für ein Radio, für das Parklicht, für einen Antrieb eines Fensterhebers, einer motorischen Sitzverstellung und eines Schiebedachs.

Beim Weiterdrücken 52 des Schlüssels 50 in die bereits erwähnte Mittellage 50.2 von Fig. 13 kommt der Formschluss dadurch zustande, dass das Halteelement 81 ein Hakenende 87 aufweist, welches eine Schulter 88 vom Schlüssel 50 hintergreift. Jetzt ist eine Entnahme des Schlüssels im Sinne des Pfeils 57 blockiert. Bei der Verschiebung 52 des Schlüssels 50 von Fig. 12 auf Fig. 13 ist auch eine Hubarbeit gegen die von der Rückstellfeder 40 bedingte Rückstellkraft 41 ausgeübt worden. In Fig. 13 kommt aber auch die andere Rückstellfeder 40' mit ihrem Stößel 74' an der Unterkante 69 des Schlüsselprofils 68 zur Anlage. Die Schulter 88 gehört zu einem Randausbruch 89 im Scheckkartenumriss 68. Aufgrund seiner Rückschwenkkraft 86 ist daher die Klinke 80 wieder in ihrer bereits in Fig. 11 beschriebenen Ausgangs-Schwenkstellung, wo ihr Stellarm 82 den Betätiger 73 des Klinken-Sensors 72 drückt. In dieser Mittellage 50.2 des Schlüssels schaltet die zugehörige elektrische Steuereinheit die Zündung des Motors im Fahrzeug ein.

In der Mittellage 50.2 von Fig. 13 kommt es auf die kraftschlüssige Haltewirkung des Rastgesperres 70 nicht mehr an. Ein an der federnden Zunge 71 befindlicher radialer Vorsprung 75 greift zwar immer noch in die erwähnte Rastvertiefung 55 des Schlüssels 50 ein, doch liegt dieser Vorsprung 75, im Gegensatz zu Fig. 12, in Abstand von der für den Kraftschluss von Fig. 12 sorgenden Haltekante 76.

Ausgehend von Fig. 13 kann der Schlüssel 50 um eine weitere Hubstrecke 53 in die aus Fig. 14 ersichtliche Endlage 50.3 überführt werden. Dazu ist eine höhere Kraft

erforderlich, weil dem Einschieben 59 nicht nur die bisherige Rückstellfeder 40, sondern auch die zweite Rückstellfeder 40' entgegenwirken. Die Endlage 50.3 wird von einem weiteren Sensor 77 festgestellt. Dieser besteht im vorliegenden Fall ebenfalls aus einem Mikroschalter, dessen Betätiger 78 von der Unterkante 69 des Schlüsselprofils gedrückt wird. Auch dieser Schlüssel-Sensor 77 ist natürlich mit der elektrischen Steuereinheit verbunden. Gleichzeitig stellt die Steuereinheit in Fig. 14 den gedrückten Zustand des Klinken-Sensors 72 fest. Aufgrund ihrer Programmierung schaltet die Steuereinheit den Anlasser des Motors an. Der Motor startet. Dies kann zeitgesteuert erfolgen. Als weitere Bedingung kann die elektrische Steuerung das pedale Betätigen einer Fußbremse überwachen. Auf diese Weise kann ein versehentlicher Start des Motors verhindert werden, wenn die Fußbremse nicht getreten wird. Darüber hinaus wird aber im vorliegenden Fall die Endlage 50.3 des Schlüssels nur impulsweise erreicht, wie aus folgendem Umstand in Fig. 14 zu ersehen ist.

Der vorbeschriebene Halterarm 81 der Klinke 80 kann mit seinem Hakenende 87 sich in dem entsprechend breit bemessenen Randausbruch 89 des Schlüssels von seiner die Verriegelung bedingenden Schulter 88 axial entfernen. Trotz des Eingriffs der Klinke 80 in den Randausbruch 89 erweist sich diese Verriegelung 80 von Fig. 13 als ein „Richtgesperre", welches zwar das Herausziehen 57 des Schlüssels 50 aus der Mittellage 50.2 von Fig. 13 verhindert, aber ein tieferes Einschieben 59 des Schlüssels in die Endlage 50.3 gestattet. Es handelt sich um eine ähnliche Wirkung, die beim ersten Ausführungsbeispiel von gesonderten Mitteln 30, 31, 24 besorgt werden musste. In diesem zweiten Ausführungsbeispiel übernehmen die Haltemittel 81, 88, 89 der formschlüssigen Verriegelung 80 zugleich die Funktion dieses „Richtgesperres".

Der vorbeschriebene weitere Abwärtshub 53 des Schlüssels wird auch nicht von den Elementen des kraftschlüssigen Rastgesperres 70 behindert. Wie Fig. 14 zeigt, erlaubt die Größe der Rastaussparung 55 eine entsprechend ungestörte Verschiebung des radialen Vorsprungs 75 an der zugehörigen federnden Zunge 71. Der Freiraum bei 89 im Bereich der Klinke 80 einerseits und bei 55 im Bereich des Rastgesperres 70 andererseits erlauben es, dass die von den Rückstellfedern 40, 40' ausgeübte

Rückstellkraft 41 den Schlüssel 50 aus Fig. 14 wieder in die Mittellage 50.2 von Fig. 13 zurückführt. Die Mittellage 50.2 ist ja durch das wie ein „Sperrarm" wirkende Halteelement 81 der Klinke 80 gesichert; das Hakenende 87 hintergreift wieder die Schulter 88 vom Schlüssel 50. Es liegt dann wieder die im Zusammenhang mit Fig. 13 bereits beschriebene Stellung „Zündung" des Motors vor. Der vorausgehend in Fig. 14 gestartete Motor läuft in Fig. 13 weiter.

Um den Motor auszuschalten, braucht, ausgehend von der Mittellage 15.2 des Schlüssels 50 in Fig. 13 der Schlüssel 50 nur noch erneut, ein zweites Mal, in seine Endlage von Fig. 14 gedrückt zu werden. Es kommt dabei nicht darauf an, ob die Fußbremse dabei ebenfalls getreten oder nicht getreten wird. Stattdessen kann die elektrische Steuerung über einen Sensor den Bremskonkakt oder die Raddrehung vom Fahrzeug sensieren. Die elektrische Steuereinheit schaltet aber auch einen auf die Klinke 80 wirkenden Antrieb 48 gemäß Fig. 9 ein. Dieser besteht auch in diesem zweiten Ausführungsbeispiel aus einem Hubmagneten 48, der über einen Stößel 49 auf einen drehfest mit der Klinke 80 verbundenen Lösearm 83 einwirkt. Die Klinke 80 wird in die strichpunktiert in Fig. 9 verdeutlichte Entriegelungsstellung 80' überführt. Dann ist die Schulter 88 frei. Weil die Rückstellfeder 40 eine Rückstellkraft 41 ausübt, schiebt sie den Schlüssel 50 aus der Mittellage 50.2 von Fig. 13 bzw. 9 wieder in die Anfangslage 50.1 von Fig. 12 zurück. Dann ist der Formschluss beseitigt. Das Verriegelungsgesperre 80 ist gemäß Fig. 12 durch den beschriebenen Profilbereich 79 entriegelt. Es liegt wieder nur der Kraftschluss des Rastgesperres 70 vor. Die manuelle Entnahme 57 des Schlüssels 50 ist in Fig. 12 wieder ohne weiteres möglich. Beim Klinken-Sensor 72 befindet sich der Betätiger 73 wieder im umgedrückten Zustand.

Ausgehend von der Anfangslage 50.1 des Schlüssels 50 in Fig. 12 kann der Schlüssel 50 natürlich alternativ, durch erneutes zweistufiges Drücken 59, über die Mittellage 50.2 von Fig. 13, wo sich die Zündung von der Steuereinheit wieder einschaltet, die Endlage 50.3 gemäß Fig. 14 gebracht werden, wo der Motor gestartet wird. Eine Fehlbedienung ist ausgeschlossen.

Auch in diesem zweiten Ausführungsbeispiel kann der mit der Klinke 80 zusammenwirkende Hubmagnet 48 dazu genutzt werden, um einen „falschen Schlüssel" aus der Vorrichtung zu entfernen. Es könnten zunächst die Haltelage 50.1 von Fig. 12 und möglicherweise auch die Endlage 50.2 von Fig. 13 mit einem falschen Schlüssel erreicht sein. Spätestens dann identifiziert aber der Transponder 43 od. dgl. den „falschen Schlüssel". Daraufhin schaltet die elektrische Steuereinheit den Hubmagneten 48 ein, der über seinen Stößel 49 die Klinke 80 in ihre beschriebene Entriegelungsstellung 80' überführt. Die von den Rückstellfedern 40 ausgeübte Rückstellkraft 41 drückt dann den falschen Schlüssel in die Anfangslage 50.1 von Fig. 12 zurück. Der Motor konnte mit dem falschen Schlüssel nicht gestartet werden.

Sofern das Fahrzeug mit einem „Automatikgetriebe" versehen ist, muss bei der Schlüsselentnahme 57 in der Anfangsstellung 50.1 von Fig. 12 der Wählhebel auf den Stellungen „B" oder „N" stehen. Außerdem ist bei dieser Vorrichtung ebenso wie beim ersten Ausführungsbeispiel eine elektrische Lenkradverriegelung vorgesehen, die bei entnommenen Schlüssel für eine Verriegelung des Lenkrads sorgt. Befindet sich der richtige Schlüssel in der Aufnahme 11, der dann vom Transponder 43 festgestellt wird, so wird die Lenkradverriegelung unwirksam gesetzt. Außerdem ist ein nicht näher gezeigter Sensor im Bereich der Aufnahme 11 vorgesehen, welcher in beiden Ausführungsbeispielen eine Verriegelung des Lenkrads dann ausschließt, solange der Schlüssel 50 sich in einen seiner drei Hublagen 50.1, 50.2 oder 50.3 befindet. Erst wenn der Schlüssel 57 aus dem Gehäuse 10 ganz entnommen ist, wird die Lenkradverriegelung wirksam gesetzt. Ebenso wird in allen Fahrtstellungen eines Automatik-Getriebes eine Auswurfbewegung auf den in der Mittellage 50.2 befindlichen Schlüssel 50 der Schlüssel nicht freigegeben und die Lenkradsicherung nicht in ihre Verriegelungsposition überführt. So lassen sich leicht Fehlbedienungen verhindern.

Im Gehäuse kann eine aus Fig. 9 und 10 ersichtliche Beleuchtung 90 vorgesehen sein, die beim Öffnen der Tür für eine bestimmte Zeit aktiviert wird. Dann wird der Einführschlitz 13 beleuchtet und erleichtert das Einführen der Karte 50.

Bezugszeichenliste :

10	Gehäuse
11	Aufnahme
12	Kontur der Armatur
13	stirnseitige Öffnung von 11
14	Abdeckung von 11
14'	Abdeckklappe (Fig. 10)
14.1	Ausschubstellung von 14 (Fig. 1, 2)
14.2	Einschubstellung von 14 (Fig. 6 bis 7)
15	Abdeck-Druckfeder für 14
16	radiale Aussparung von 10 für 23
17	Blende für 13
18	axiales Führungsmittel bei 17, Steg
19	radiale Stützfläche für 23 von 10
20	Schieber
20.1	erste Axialposition von 20, Ausgangsposition (Fig. 1 bis 5)
20.2	zweite Axialposition von 20, Arbeitsposition (Fig. 6)
20.3	dritte Axialposition von 20, Endposition (Fig. 7)
21	Halteelement für 50, federnde Zunge
22	erster Endanschlag für 14, Halteelement für 50, federnder Vorsprung
23	Gegenvorsprung an 21
24	Schulter für 31, Nocken (Richtgesperre)
25	Axialansatz von 20
26	Innenbund in 25 für 40
27	Punktlinie, Verschiebungsweg von 24
28	herausragendes Teilstück von 50 (Fig. 5)
29	zweiter Endanschlag von 14 (Fig. 5)
30	Riegel, Klinke (Richtgesperre)
31	Sperrarm von 30 (Richtgesperre)

32	Lösearm von 30
33	Schwenklager von 30
34	Axialführung für 35 (Fig. 8)
35	Betätiger, Taster
36	Druckbetätigungspfeil zur Tasterbetätigung für 35 (Fig. 8)
37	Rückstellfeder für 35
38	Schriftfeld-Teil von 35 für 46
38'	Schriftfeld-Rest von 35 für 46'
39	Lichttrennwand an 35 (Fig. 8)
40	Rückstellfeder für 20 (Fig. 1 bis 8) bzw. für 50 (Fig. 9 bis 14)
40'	weitere Rückfestellfeder für 50 (Fig. 9 bis 14)
41	Pfeil der axialen Rückstellkraft von 20 bzw. 50, axiale Federbelastung
42	Endanschlag an 10 für 20 (Fig. 5)
43	Transponder der elektronischen Steuereinheit
44	Sensor für 35 (Fig. 2, 8)
45	Gehäusehülse für 25
46	Diode für „Start" in 35 (Fig. 8)
46'	Diode für „Stop" in 35 (Fig. 8)
47	Sensor für 50.3
48	Antrieb, Hubmagnet
49	Stößel von 48
50	elektronischer Schlüssel
50.0	Berührungslage von 50 (Fig. 1, 2)
50.1	erste axiale Hublage von 50, Anfangslage (Fig. 5)
50.2	zweite axiale Hublage von 50, Mittellage (Fig. 6)
50.3	dritte axiale Hublage von 50, Endlage (Fig. 7)
51	erste Hubstrecke von 50 (Fig. 5)
52	zweite Hubstrecke von 50 (Fig. 6)
53	dritte Hubstrecke von 50 (Fig. 7)
54	axiales Führungsmittel an 50, Längsnut
55	Halteelement, Rastvertiefung
56	herausragendes Endstück von 50 bei 50.2 (Fig. 6)
57	Pfeil des Rückschubs, Herausziehbewegung von 50 aus 11

58 Vorderstück von 50
59 Pfeil der Einschubbewegung von 50 in 11
60 Dämpfungseinrichtung für 20, Dämpfungsrad
61 Drehachse von 60
62 Stirnrad von 60
63 Zahnstange für 62
64 Schaltnocken für 47 (Fig. 2)
65 Steckkontakt an 10
66 Leiterplatte
67 Zwischenboden (Fig. 3)
68 Kartenumriss von 50 (Fig. 11), Schlüsselprofil
69 Unterkante von 50
70 kraftschlüssiges Rastgesperre
71 Halteelement von 70, federnde Zunge
72 Klinken-Sensor
73 Betätiger von 72
74 Stößel für 40
74' Stößel für 40'
75 federnder Vorsprung an 71
76 Haltekante von 55 für 50 (Fig. 12)
77 Schlüssel-Sensor
78 Betätiger von 77
79 Profilbereich von 68 für Abstützung von 81
80 Richtgesperre, Klinke (Verriegelungsstellung)
80' Entriegelungsstellung von 80
81 Halteelement von 80, Sperrarm
82 Stellarm von 80
83 Lösearm von 80
84 Schwenklager für 80
85 Klinken-Federbelastung
86 Rückschwenk-Kraft von 85 auf 80
87 Hakenende von 81
88 Schulter für 87 von 80

89 Randausbruch von 68 für 87

90 Beleuchtung in 11 (Fig. 10)

Patentansprüche :

1.) Vorrichtung zum Starten eines Fahrzeug-Motors mittels eines elektronischen Schlüssels (50), der gegebenenfalls ein Scheckkarten-Format aufweist,

mit einer zum Einstecken (59) des Schlüssels (50) dienenden Aufnahme (11) im Fahrzeug,

wobei der in der Aufnahme (11) eingesteckte Schlüssel (50) manuell in verschiedene Schlüssellagen überführbar ist

und die Schlüssellagen von Sensoren einer elektronischen Steuereinheit überwacht und zur Steuerung von verschiedenen Funktionen des Motors und gegebenenfalls weiterer Zusatzgeräte im Kraftfahrzeug, wie einem Radio, genutzt werden,

dadurch gekennzeichnet ,

dass der eingesteckte Schlüssel (50) in der Aufnahme (11) unverdrehbar und mindestens zwischen drei zueinander axial versetzten Hublagen (50.1, 50.2, 50.3) längsverschiebbar (51, 52, 53) ist, nämlich,

beim anfänglichen Einstecken (59), zunächst in eine den Schlüssel (50) im vorderen Bereich der Aufnahme (11) nur kraftschlüssig sichernden Anfangslage (50.1),

dann, beim Weiterschieben (59) um eine erste Hubstrecke (52), in eine den Schlüssel (50) im mittleren Bereich der Aufnahme (11) formschlüssig sichernden Mittellage (50.2),

welche zwar ein manuelles Herausziehen (57) des Schlüssels (50) aus der Aufnahme (11) verhindert, aber ein Weiterschieben (59) des Schlüssels (50) erlaubt,

und schließlich beim Weiterschieben (59) um eine zweite Hubstrecke (53) in eine den Schlüssel (50) im hinteren Bereich der Aufnahme (11) positionierende Endlage (50.3),

dass der Schlüssel (50) mindestens in seiner Mittel- und Endlage (50.2, 50.3) in Richtung seiner Anfangslage (50.1) entweder unmittelbar oder mittelbar (20) von einer Rückstellfeder (40) axial federbelastet (41) ist, wobei die Sensoren der Steuereinheit mindestens einige der drei Schlüssel-Hublagen (50.1, 50.2, 50.3) überwachen.

2.) Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass wenigstens ein manueller und/oder pedaler Betätiger (35) im Fahrzeug angeordnet ist und mit der Steuereinheit in Wirkverbindung steht

und dass eine Betätigung des Betätigers (35) die Auswahl der verschiedenen Funktionen des Fahrzeugs mitbestimmt.

3.) Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Schlüssel (50) beim Weiterschieben (59) aus der Mittellage (50.2) seine Endlage (50.3) nur impulsweise erreicht

und dass - nach Beendigung des manuellen Einschubdrucks - die Rückstellfeder (40) den Schlüssel (50) selbsttätig wieder in die Mittellage (50.2) oder die Anfangslage (50.1) zurückschiebt (75).

4.) Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Aufnahme (11) sowohl ein den Kraftschluss erzeugendes Rastgesperre (21, 22, 55; 70) für den eingesteckten Schlüssel (50) als auch ein mittelbar (20) oder unmittelbar mit dem Schlüssel (50) zusammenwirkendes Richtgesperre (24, 30, 31; 80) besitzt,

dass das Rastgesperre (21, 22, 55; 70) mindestens in der Anfangslage (50.1), aber das Richtgesperre (24, 30, 31; 80) sowohl in der Mittellage (50.2) als auch in der Endlage (50.3) des Schlüssels (50) wirksam sind

und dass bei wirksamem Richtgesperre (24, 30, 31; 80) das Weiterschieben (59) des Schlüssels (50) aus der Mittellage (50.2) in die Endlage (50.3) und das rückstellfederbedingte Zurückschieben (57) des Schlüssels (50) aus der Endlage (50.3) in die Mittellage (50.2) zwar möglich sind,

aber ein Zurückschieben (57) des Schlüssels (50) aus der Mittellage (50.2) in die Anfangslage (50.1) verhindert ist.

5.) Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, dass beim Einschieben (59) des Schlüssels (50) in die Anfangslage (50.1) das Rastgesperre (21, 22, 50; 70) und beim Einschieben (59) in die Mittellage (50.2) das Richtgesperre (24, 30, 31; 80) selbsttätig wirksam setzbar sind

und dass die Steuereinheit auf ein einmaliges oder mehrmaliges Eindrücken (59) des Schlüssels (50) zwischen der Mittellage (50.2) in die Endlage (50.3) anspricht und das Richtgesperre (24, 30, 31; 80) solange unwirksam setzt, bis die Rückstellfeder-Kraft (41) den Schlüssel (50) in die Anfangslage (50.1) zurückgeschoben (57) hat.

6.) Vorrichtung nach Anspruch 5, dadurch gekennzeichnet,

dass das Richtgesperre einen seinerseits federbelasteten (85) Riegel (30; 80) aufweist, der in den axialen Weg (27) einer entweder unmittelbar oder mittelbar (20) mit dem Schlüssel (50) mitverschieblichen Schulter (24; 88) hineinragt und die Schulter (24; 88) in der Endlage (50.3) des Schlüssels (50) hintergreift

und dass die Steuereinheit im Ansteuerungsfall den Riegel (30; 80) gegen seine Riegel-Federbelastung (86) aus dem axialen Weg der Schulter (24; 88) herausbewegt.

7.) Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, dass der Riegel aus einer federbelasteten Klinke (30; 80) besteht, wobei die Klinke (30; 80) außer einem mit der Schulter (21; 88) zusammenwirkenden Sperrarm (31; 81) einen damit drehfesten Lösearm (32) besitzt,

und dass der Lösearm (32; 83) mit einem Antrieb (48), wie einem elektrischen Hubmagneten (48), verbunden ist, der von der elektrischen Steuereinheit gesteuert wird.

8.) Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass in der Aufnahme (11) elektronische Identifikationsmittel für den Schlüssel (50) angeordnet sind, die mit der elektrischen Steuereinheit in Wirkverbindung stehen,

und dass bei Ermittlung eines falschen Schlüssels (50) der Antrieb (48) für die Klinke (30; 80) wirksamgesetzt wird und den Riegel freigibt,

wodurch der falsche Schlüssel (50) von der Rückstellfederkraft (41) in seine Anfangslage (50.1) in der Aufnahme (11) zurückgeschoben wird.

9.) Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass die elektronischen Identifikationsmittel aus einem Transponder (48) bestehen.

10.) Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die kraftschlüssigen Halteelemente (21; 81) des Rastgesperres einerseits aus einem federnden Glied (22) im Bereich der Aufnahme (11) und andererseits aus einer Rastvertiefung (59) am Schlüssel (50) bestehen.

11.) Vorrichtung nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass der Schlüssel (50) die Umrissform (68) einer Scheckkarte hat.

12.) Vorrichtung nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass das Rastgesperre (70) und Richtgesperre (80) ortsfest in einem die Aufnahme (11) umschließenden Gehäuse (10) angeordnet sind,

dass nicht nur die Rastvertiefung (55) für das Rastgesperre (70), sondern auch die Schulter (88) des Richtgesperres (80) unmittelbar am Umrissprofil (68) des Schlüssels (50) sich befinden

und dass die Verriegelungs-Elemente (81) des Richtgesperres (80) zugleich die formschlüssigen Halteelemente für den Schlüssel (59) sind.

13.) Vorrichtung nach einem der Ansprüche 6 bis 12, dadurch gekennzeichnet, dass die Klinke (80) des Richtgesperres einen drehfest mit dem Sperr- und Lösearm (81, 83) ausgebildeten Stellarm (82) aufweist

und der Stellarm (82) auf einen Klinken-Sensor (72) einwirkt.

14.) Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass die Sperrstellung der Klinke (80) durch die Klinken-Federbelastung (85) und gegebenenfalls einen Drehanschlag bestimmt ist,

dass die Sperrstellung sowohl bei herausgezogenem Schlüssel (50), also bei leerer Aufnahme (11), als auch bei einem in der Mittellage (50.2) und in der Endlage (50.3) befindlichen Schlüssel (50) vorliegt

und dass der Klinken-Sensor (72) vom Stellarm (82) zwar in der Sperrstellung der Klinke (80) betätigt wird,

aber in der Anfangslage (50.1) des Schlüssels (50) die Klinke (80) von einem Profilabschnitt (79) des Schlüssel-Umrissprofils (68) aus ihrer Sperrstellung gegen die Klinken-Federbelastung (86) verschwenkt (80') ist und den Klinken-Sensor (72) freigibt.

15.) Vorrichtung nach Anspruch 14, dadurch gekennzeichnet, dass die Aufnahme (11) außer dem Klinken-Sensor (72) einen ebenfalls mit der Steuereinheit in Verbindung stehenden Schlüssel-Sensor (77) besitzt, der die Endlage (50.3) des Schlüssels (50) überwacht.

16.) Vorrichtung nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass die auf den Schlüssel (50) wirkende axiale Rückstellkraft (41) sich in Abhängigkeit von dessen Hublage (50.1, 50.2, 50.3) in der Aufnahme (11) stufenartig verändert

und dass die Rückstellkraft (41) in der Anfangslage (50.1) des Schlüssels (50) geringer als in der Mittellage (50.2) und der Endlage (50.3) ist.

17.) Vorrichtung nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, dass der zur Auswahl verschiedener Funktionen im Fahrzeug dienende manuelle oder pedale Betätiger (35) zwar in der Mittellage (50.2) des Schlüssels wirksam, aber in allen übrigen Lagen (50.0, 50.1, 50.3) des Schlüssels (50) unwirksam ist.

18.) Vorrichtung nach einem der Ansprüche 1 bis 11 und 17 mit einer Aufnahme (11), deren Öffnung (13) normalerweise von einer federnden (15) Abdeckung (14) verschlossen (14.1) ist,

wobei die Abdeckung (14) beim Einstecken (59) vom Schlüssel (50) gegen die Abdeck-Federbelastung (15) weggedrückt (14.2) wird,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Abdeckung (14) Bestandteil eines im Gehäuse (10) der Aufnahme (11) axial beweglichen Schiebers (20) ist,

dass der Schieber (20) beim Einstecken (59) das Vorderstück (48) des Schlüssels (50) aufnimmt und der Schieber (20) sowohl die kraftschlüssig als auch formschlüssig auf den Schlüssel (50) einwirkenden Haltemittel (21, 22, 55) besitzt, wobei diese Haltemittel den Schlüssel (50) im Schieber (20) sichern,

dass der Schieber (20) durch die Axialbewegung (59) des Schlüssels (50) in verschiedene Axialpositionen (20.1, 20.2, 20.3) überführbar ist, welche die verschiedenen Hublagen (50.1, 50.2, 50.3) des Schlüssels (50) bestimmen,

und dass der Schieber (20) axial federbelastet (40) ist und dadurch auf den eingesteckten Schlüssel (50) ausgeübte Rückstellkraft (41) erzeugt,

und dass der Schieber (20) in seiner die Mittellage (50.2) des Schlüssels (50) bestimmenden mittleren Axialposition (50.2) von einem federnden Riegel (30) eines Richtgesperres festgehalten wird und dieses Richtgesperre mittelbar, über den Schieber (20), auf den Schlüssel (50) wirkt.

19.) Vorrichtung nach Anspruch 18, dadurch gekennzeichnet, dass der Schieber (20) sowohl in der Anfangslage (50.1) des eingesteckten Schlüssels (50) als auch bei herausgezogenem Schlüssel sich in der gleichen Ausgangsposition (20.1) im Gehäuse (10) der Aufnahme (11) befindet,

und dass die Ausgangsposition (50.1) durch die auf den Schieber (20) wirkende axiale Federkraft (41) einerseits und einen Endanschlag (42) im Gehäuse (10) der Aufnahme (11) andererseits bestimmt ist.

20.) Vorrichtung nach Anspruch 19, dadurch gekennzeichnet, dass die Abdeckung (14) für die Öffnung (13) der Aufnahme (11) ihrerseits zwischen zwei Stellungen (14.1, 14.2) im Schieber (20) axial verschieblich ist,

dass diese beiden Stellungen (14.1, 14.2) durch einen vorderen und einen hinteren Endanschlag (22, 29) im Schieber (20) bestimmt sind,

dass die Abdeck-Federbelastung (15) bestrebt ist, die Abdeckung (14) axial gegen den vorderen Endanschlag (22) zu drücken,

und dass der vordere Endanschlag (22) und die Abdeck-Federbelastung (15) die bei herausgezogenem Schlüssel (50) sich ergebende abdeckwirksame Ausschubstellung (14.1) der Abdeckung (14) an der Öffnung (13) bestimmen.

21.) Vorrichtung nach Anspruch 20, dadurch gekennzeichnet, dass bei eingestecktem Schlüssel (50) die Abdeckung (14) sich in einer durch den

hinteren Endanschlag (29) am Schieber (20) bestimmten Einschubstellung (14.2) befindet

und dass diese Einschubstellung (14.2) der Abdeckung (14) in allen drei axialen Hublagen des Schlüssels (50) vorliegt.

22.) Vorrichtung nach einem der Ansprüche 18 bis 21, dadurch gekennzeichnet, dass die gleichen Halteelemente (21, 22, 55), welche die kraftschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) erzeugen, auch bei der formschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) beteiligt sind.

23.) Vorrichtung nach Anspruch 22, dadurch gekennzeichnet, dass die am Schieber (20) befindlichen kraftschlüssigen Halteelemente (21, 22) einen federnden Vorsprung (22) aufweisen

dass dem Vorsprung (22) ein Gegenvorsprung (23) auf seiner dem Gehäuse (10) der Aufnahme (11) zugekehrten Rückseite zugeordnet ist,

dass dieser Gegenvorsprung (23) in der die Haltelage (50.1) des Schlüssels (50) kennzeichenden Ausgangsposition (20.1) des Schiebers (20) mit einer Aussparung (16) im Gehäuse (10) radial ausgerichtet ist, in welchen der Gegenvorsprung (23) federnd ausweicht, wenn der Schlüssel (50) eingesteckt (59) wird,

und dass dem Gegenvorsprung (23) eine radiale Stützfläche (19) im Gehäuse (10) zugeordnet ist, die das federnde Glied (22) radial versteift, wenn der Schieber (20) vom Schlüssel (50) aus seiner Ausgangsposition (20.1) in eine der tiefer gelegenen Axialpositionen (20.2, 20.3) weiterbewegt wird.

24.) Vorrichtung nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass der axialbewegliche Schieber (20) ein mit einer Dämpfungseinrichtung (60) versehen ist,

und dass die Dämpfungseinrichtung (60) die federbedingte (40) axiale Rückbewegung (57) des im Schieber (20) aufgenommenen Schlüssels (50) aus dessen Endlage (50.3), über die Mittellage (50.2), bis zur Anfangslage (50.1) bremst.

25.) Vorrichtung nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktion dienende Steuereinheit auch auf Betätigung bzw. Nichtbetätigung weiterer Steuerglieder im Fahrzeug anspricht, wie eine Fußbremse.

26.) Vorrichtung nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktionen dienende Steuereinheit auf eine Nicht-Betätigung weiterer Steuerglieder im Fahrzeug anspricht.

27.) Vorrichtung nach einem der Ansprüche 1 bis 26, dadurch gekennzeichnet, dass der für die verschiedenen Funktionen im Kraftfahrzeug dienende Betätiger einen Taster (35) umfasst

und dass die elektrische Steuereinheit die Anzahl und/oder die Reihenfolge der verschiedenen Betätigungen (36) unterscheidet und dementsprechend die ausgewählten Funktionen im Kraftfahrzeug auslöst.

28.) Vorrichtung nach einem der Ansprüche 1 bis 27, dadurch gekennzeichnet, dass zum unverdrehbaren Einstecken axiale Führungsmittel (18, 54) zwischen dem Schlüssel (50) einerseits und der Aufnahme (11) andererseits vorgesehen sind.

29.) Vorrichtung nach Anspruch 28, dadurch gekennzeichnet, dass die zur Aufnahme (11) gehörenden axialen Führungsmittel (18) in einer die Öffnung (13) der Aufnahme umschließenden Blende (17) angeordnet sind

und dass im Bereich der am Schlüssel (50) vorgesehenen Führungsmittel (54) auch die Angriffsstellen (55) für die kraftschlüssig und/oder formschlüssig wirksamen Halteelemente (21, 22, 23) des Rast- und/oder Richtgesperres angeordnet sind.

GEÄNDERTE ANSPRÜCHE

[beim Internationalen Büro am 09. Januar 2001 (09.01.01) eingegangen; ursprüngliche Ansprüche 1-29 durch neue Ansprüche 1-20 ersetzt (8 Seiten)]

1.) Vorrichtung zum Starten eines Fahrzeug-Motors mittels eines elektronischen Schlüssels (50), der gegebenenfalls ein Scheckkarten-Format aufweist,

mit einer zum Einstecken (59) des Schlüssels (50) dienenden Aufnahme (11) im Fahrzeug,

wobei der in der Aufnahme (11) eingesteckte Schlüssel (50) unverdrehbar und mindestens zwischen drei zueinander axial versetzten Hublagen (50.1, 50.2, 50.3) längsverschiebbar (51, 52, 53) ist

wobei der Schlüssel (50) in seiner Endlage (50.3) in Richtung seiner Anfangslage (50.1) entweder unmittelbar oder mittelbar von einer Rückstellfeder (40) axial federbelastet (41) ist und

einige der drei Schlüssel-Hublagen (50.1, 50.2, 50.3) von Sensoren einer Steuereinheit überwacht und zur Steuerung von verschiedenen Funktionen des Motors genutzt werden,

dadurch gekennzeichnet,

dass der Schlüssel (50) auch in seiner Mittellage (50.2) in Richtung seiner Anfangslage (50.1) von einer Rückstellfeder (40) axial federbelastet (41) ist und

beim Einschieben (59) des Schlüssels (50) in die Anfangslage (50.1) ein Rastgesperre (21, 22; 50; 70) und beim Einschieben (59) in die Mittellage (50.2) ein mit dem Schlüssel (50) mittelbar (20) oder unmittelbar zusammenwirkendes Richtgesperre (24; 30, 31; 80) selbsttätig wirksam setzbar sind und

dass die Steuereinheit auf ein einmaliges oder mehrmaliges Eindrücken (59) des Schlüssels (50) zwischen der Mittellage (50.2) in die Endlage (50.3) anspricht und das Richtgesperre (24; 30, 31; 80) solange unwirksam setzt, bis die Rückstellfederkraft (41) den Schlüssel (50) selbsttätig in die Anfangslage (50.1) zurückgeschoben (57) hat.

2.) Vorrichtung nach Anspruch 1, dadurch gekennzeichnet,

dass das Richtgesperre einen seinerseits federbelasteten (85) Riegel (30; 80) aufweist, der in den axialen Weg (27) einer entweder unmittelbar oder mittelbar (20) mit dem Schlüssel (50) mitverschieblichen Schulter (24; 88) hineinragt und die Schulter (24; 88) in der Endlage (50.3) des Schlüssels (50) hintergreift

und dass die Steuereinheit im Ansteuerungsfall den Riegel (30; 80) gegen seine Riegel-Federbelastung (86) aus dem axialen Weg der Schulter (24; 88) herausbewegt.

3.) Vorrichtung nach Anspruch 2, dadurch gekennzeichnet, dass der Riegel aus einer federbelasteten Klinke (30; 80) besteht, wobei die Klinke (30; 80) außer einem mit der Schulter (21; 88) zusammenwirkenden Sperrarm (31; 81) einen damit drehfesten Lösearm (32) besitzt,

und dass der Lösearm (32; 83) mit einem Antrieb (48), wie einem elektrischen Hubmagneten (48), verbunden ist, der von der elektrischen Steuereinheit gesteuert wird.

4.) Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass in der Aufnahme (11) elektronische Identifikationsmittel für den Schlüssel

(50) angeordnet sind, die mit der elektrischen Steuereinheit in Wirkverbindung stehen,

und dass bei Ermittlung eines falschen Schlüssels (50) der Antrieb (48) für die Klinke (30; 80) wirksamgesetzt wird und den Riegel freigibt,

wodurch der falsche Schlüssel (50) von der Rückstellfederkraft (41) in seine Anfangslage (50.1) in der Aufnahme (11) zurückgeschoben wird.

5.) Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, dass die elektronischen Identifikationsmittel aus einem Transponder (43) bestehen.

6.) Vorrichtung nach einem der Ansprüche 2 bis 5, dadurch gekennzeichnet, dass die Klinke (80) des Richtgesperres einen drehfest mit dem Sperr- und Lösearm (81, 83) ausgebildeten Stellarm (82) aufweist

und der Stellarm (82) auf einen Klinken-Sensor (72) einwirkt.

7.) Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, dass die Sperrstellung der Klinke (80) durch die Klinken-Federbelastung (85) und gegebenenfalls einen Drehanschlag bestimmt ist,

dass die Sperrstellung sowohl bei herausgezogenem Schlüssel (50), also bei leerer Aufnahme (11), als auch bei einem in der Mittellage (50.2) und in der Endlage (50.3) befindlichen Schlüssel (50) vorliegt

und dass der Klinken-Sensor (72) vom Stellarm (82) zwar in der Sperrstellung der Klinke (80) betätigt wird,

aber in der Anfangslage (50.1) des Schlüssels (50) die Klinke (80) von einem Profilabschnitt (79) des Schlüssel-Umrissprofils (68) aus ihrer Sperrstellung gegen die Klinken-Federbelastung (86) verschwenkt (80') ist und den Klinken-Sensor (72) freigibt.

8.) Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass die Aufnahme (11) außer dem Klinken-Sensor (72) einen ebenfalls mit der Steuereinheit in Verbindung stehenden Schlüssel-Sensor (77) besitzt, der die Endlage (50.3) des Schlüssels (50) überwacht.

9.) Vorrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die auf den Schlüssel (50) wirkende axiale Rückstellkraft (41) sich in Abhängigkeit von dessen Hublage (50.1, 50.2, 50.3) in der Aufnahme (11) stufenartig verändert

und dass die Rückstellkraft (41) in der Anfangslage (50.1) des Schlüssels (50) geringer als in der Mittellage (50.2) und der Endlage (50.3) ist.

10.) Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass der zur Auswahl verschiedener Funktionen im Fahrzeug dienende manuelle oder pedale Betätiger (35) zwar in der Mittellage (50.2) des Schlüssels wirksam, aber in allen übrigen Lagen (50.0, 50.1, 50.3) des Schlüssels (50) unwirksam ist.

11.) Vorrichtung nach einem der Ansprüche 1 bis 5 und 10 mit einer Aufnahme (11), deren Öffnung (13) normalerweise von einer federnden (15) Abdeckung (14) verschlossen (14.1) ist,

wobei die Abdeckung (14) beim Einstecken (59) vom Schlüssel (50) gegen die Abdeck-Federbelastung (15) weggedrückt (14.2) wird,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Abdeckung (14) Bestandteil eines im Gehäuse (10) der Aufnahme (11) axial beweglichen Schiebers (20) ist,

dass der Schieber (20) beim Einstecken (59) das Vorderstück (48) des Schlüssels (50) aufnimmt und der Schieber (20) sowohl die kraftschlüssig als auch formschlüssig auf den Schlüssel (50) einwirkenden Haltemittel (21, 22, 55) besitzt, wobei diese Haltemittel den Schlüssel (50) im Schieber (20) sichern,

dass der Schieber (20) durch die Axialbewegung (59) des Schlüssels (50) in verschiedene Axialpositionen (20.1, 20.2, 20.3) überführbar ist, welche die verschiedenen Hublagen (50.1, 50.2, 50.3) des Schlüssels (50) bestimmen,

und dass der Schieber (20) axial federbelastet (40) ist und dadurch auf den eingesteckten Schlüssel (50) ausgeübte Rückstellkraft (41) erzeugt,

und dass der Schieber (20) in seiner die Mittellage (50.2) des Schlüssels (50) bestimmenden mittleren Axialposition (50.2) von einem federnden Riegel (30) eines Richtgesperres festgehalten wird und dieses Richtgesperre mittelbar, über den Schieber (20), auf den Schlüssel (50) wirkt.

12.) Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, dass der Schieber (20) sowohl in der Anfangslage (50.1) des eingesteckten Schlüssels (50) als auch bei herausgezogenem Schlüssel sich in der gleichen Ausgangsposition (20.1) im Gehäuse (10) der Aufnahme (11) befindet.

und dass die Ausgangsposition (50.1) durch die auf den Schieber (20) wirkende axiale Federkraft (41) einerseits und einen Endanschlag (42) im Gehäuse (10) der Aufnahme (11) andererseits bestimmt ist.

13.) Vorrichtung nach Anspruch 12, dadurch gekennzeichnet, dass die Abdeckung (14) für die Öffnung (13) der Aufnahme (11) ihrerseits zwischen zwei Stellungen (14.1, 14.2) im Schieber (20) axial verschieblich ist,

dass diese beiden Stellungen (14.1, 14.2) durch einen vorderen und einen hinteren Endanschlag (22, 29) im Schieber (20) bestimmt sind,

dass die Abdeck-Federbelastung (15) bestrebt ist, die Abdeckung (14) axial gegen den vorderen Endanschlag (22) zu drücken,

und dass der vordere Endanschlag (22) und die Abdeck-Federbelastung (15) die bei herausgezogenem Schlüssel (50) sich ergebende abdeckwirksame Ausschubstellung (14.1) der Abdeckung (14) an der Öffnung (13) bestimmen.

14.) Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass bei eingestecktem Schlüssel (50) die Abdeckung (14) sich in einer durch den hinteren Endanschlag (29) am Schieber (20) bestimmten Einschubstellung (14.2) befindet

und dass diese Einschubstellung (14.2) der Abdeckung (14) in allen drei axialen Hublagen des Schlüssels (50) vorliegt.

15.) Vorrichtung nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, dass die gleichen Halteelemente (21, 22, 55), welche die kraftschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) erzeugen,

auch bei der formschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) beteiligt sind.

16.) Vorrichtung nach Anspruch 15, dadurch gekennzeichnet, dass die am Schieber (20) befindlichen kraftschlüssigen Halteelemente (21, 22) einen federnden Vorsprung (22) aufweisen

dass dem Vorsprung (22) ein Gegenvorsprung (23) auf seiner dem Gehäuse (10) der Aufnahme (11) zugekehrten Rückseite zugeordnet ist,

dass dieser Gegenvorsprung (23) in der die Haltelage (50.1) des Schlüssels (50) kennzeichenden Ausgangsposition (20.1) des Schiebers (20) mit einer Aussparung (16) im Gehäuse (10) radial ausgerichtet ist, in welchen der Gegenvorsprung (23) federnd ausweicht, wenn der Schlüssel (50) eingesteckt (59) wird,

und dass dem Gegenvorsprung (23) eine radiale Stützfläche (19) im Gehäuse (10) zugeordnet ist, die das federnde Glied (22) radial versteift, wenn der Schieber (20) vom Schlüssel (50) aus seiner Ausgangsposition (20.1) in eine der tiefer gelegenen Axialpositionen (20.2, 20.3) weiterbewegt wird.

17.) Vorrichtung nach einem der Ansprüche 10 bis 16, dadurch gekennzeichnet, dass der axialbewegliche Schieber (20) ein mit einer Dämpfungseinrichtung (60) versehen ist,

und dass die Dämpfungseinrichtung (60) die federbedingte (40) axiale Rückbewegung (57) des im Schieber (20) aufgenommenen Schlüssels (50) aus dessen Endlage (50.3), über die Mittellage (50.2), bis zur Anfangslage (50.1) bremst.

18.) Vorrichtung nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktion dienende Steuereinheit auch auf Betätigung bzw. Nichtbetätigung weiterer Steuerglieder im Fahrzeug anspricht, wie eine Fußbremse.

19.) Vorrichtung nach einem der Ansprüche 1 bis 18, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktionen dienende Steuereinheit auf eine Nicht-Betätigung weiterer Steuerglieder im Fahrzeug anspricht.

20.) Vorrichtung nach einem der Ansprüche 1 bis 19, dadurch gekennzeichnet, dass der für die verschiedenen Funktionen im Kraftfahrzeug dienende Betätiger einen Taster (35) umfasst

und dass die elektrische Steuereinheit die Anzahl und/oder die Reihenfolge der verschiedenen Betätigungen (36) unterscheidet und dementsprechend die ausgewählten Funktionen im Kraftfahrzeug auslöst.

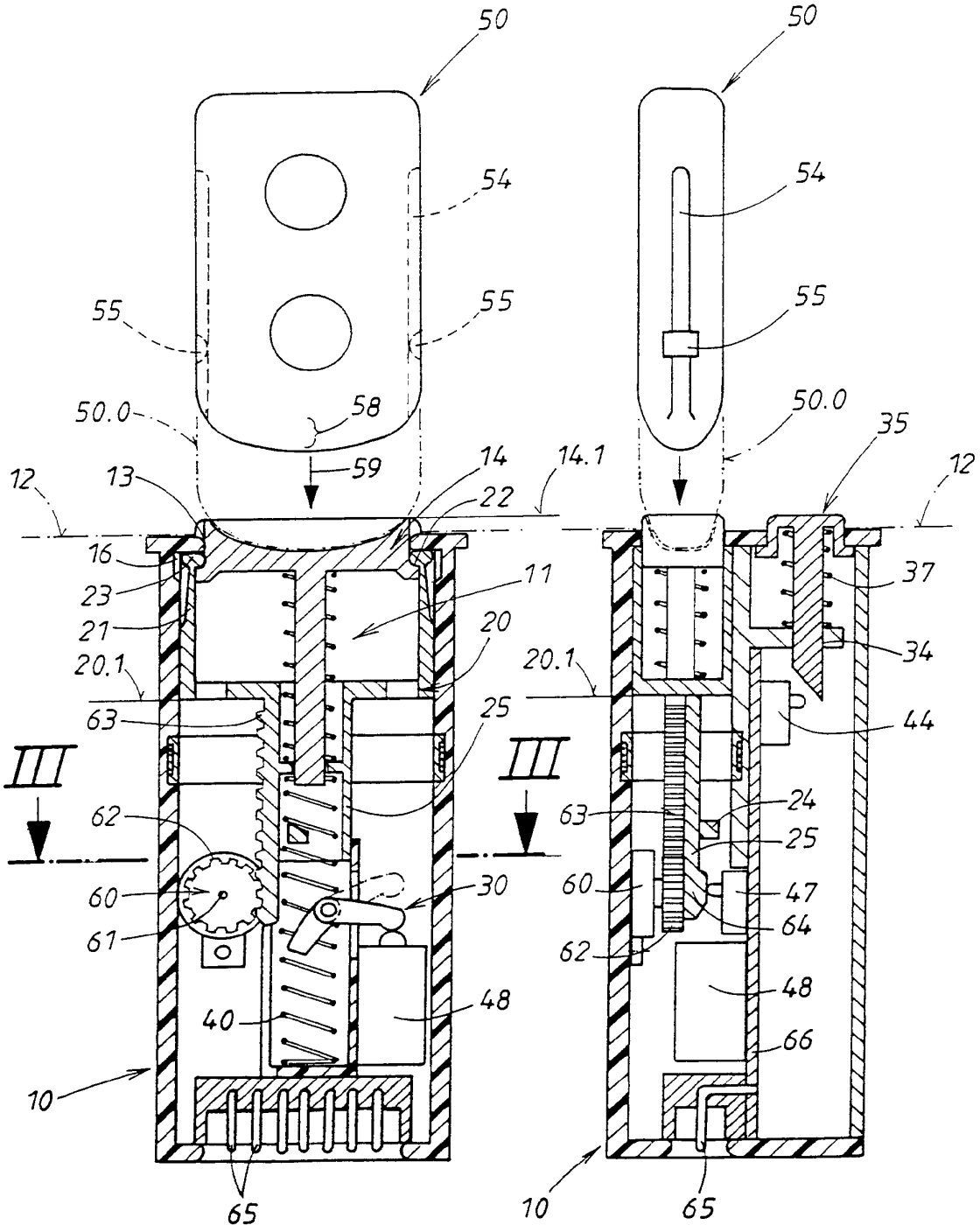

50
54
55
55
50.0
58
59
12
13
14
14.1
22
16
23
21
20.1
63
11
20
25
III
62
60
61
30
40
48
10
65
50
54
55
50.0
35
12
37
34
20.1
44
63
24
25
60
47
64
62
48
66
10
65

FIG. 1 FIG. 2

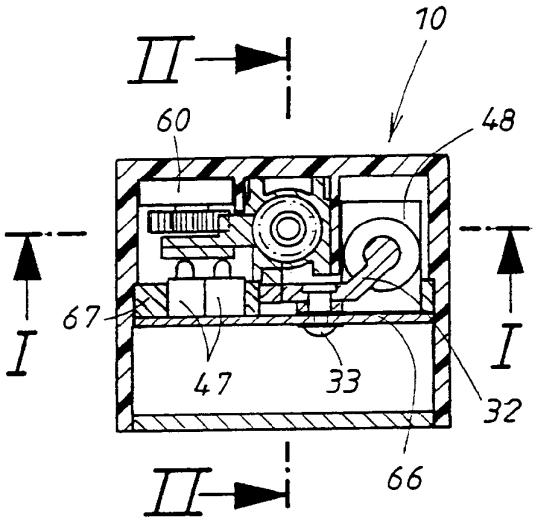


FIG. 3

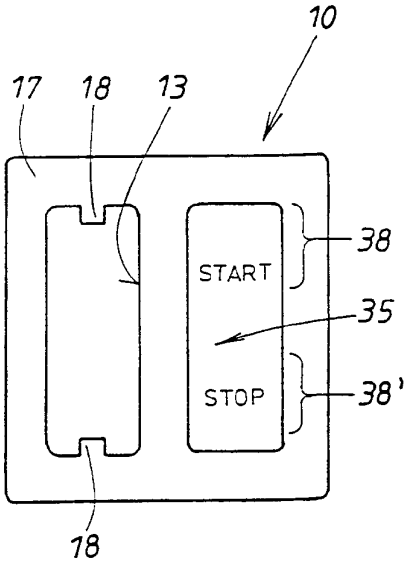


FIG. 4

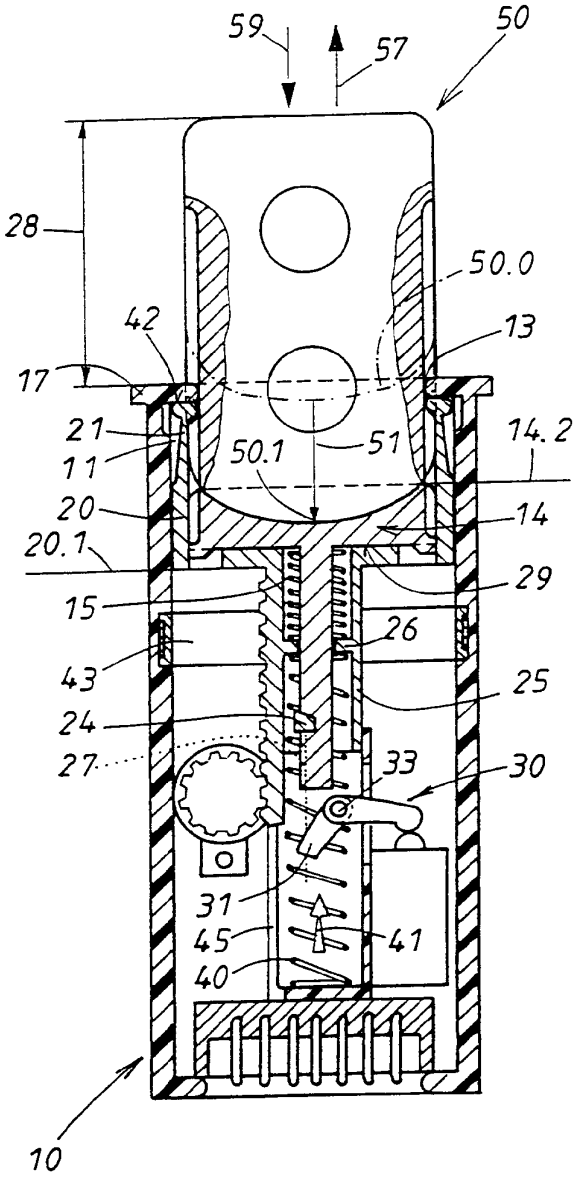

59
57
50
28
50.0
42
13
17
21
11
50.1
51
14.2
20
14
20.1
29
15
26
43
25
24
27
33
30
31
45
41
40
10

FIG. 5

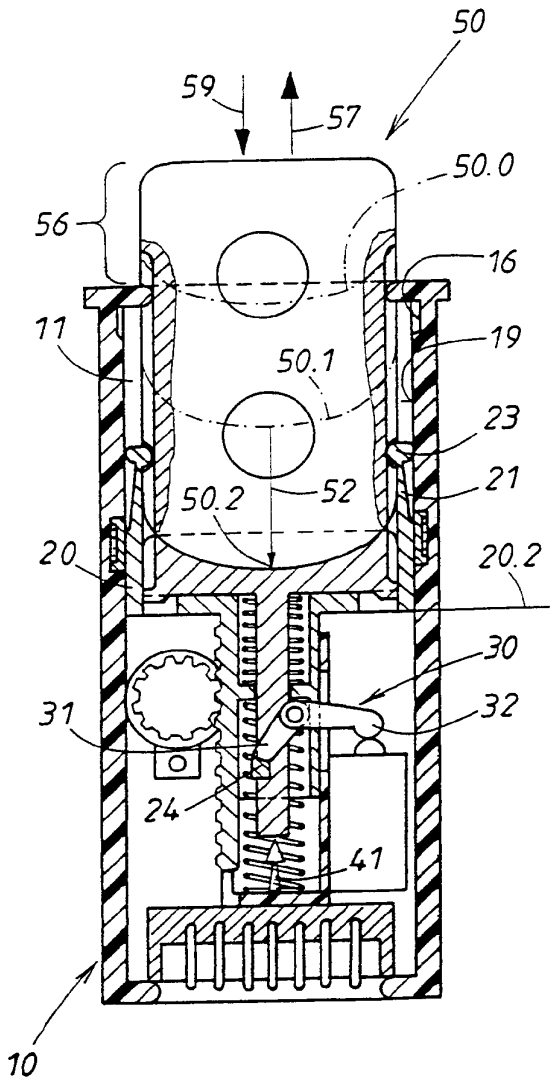

50
59
57
50.0
56
16
11
19
50.1
23
21
50.2
52
20
20.2
30
31
32
24
41
10

FIG. 6

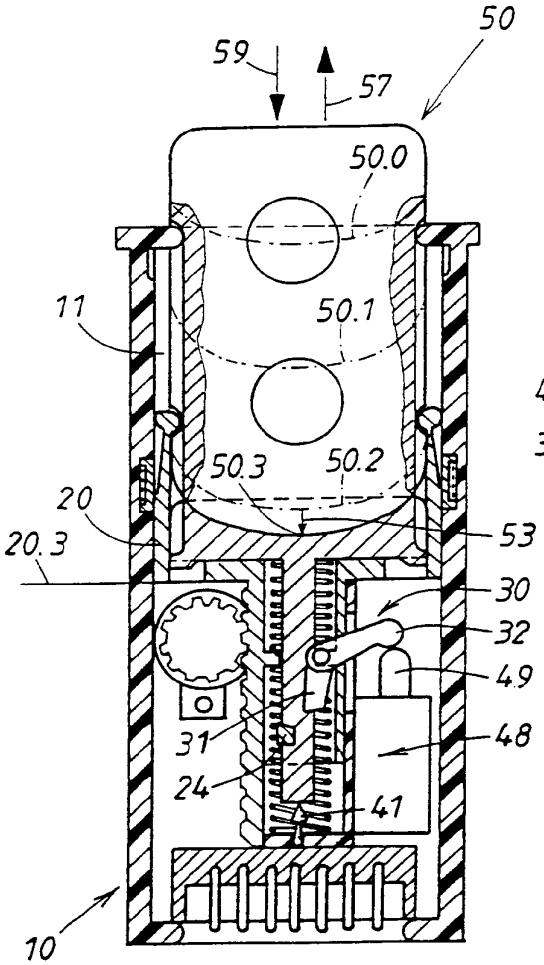

50
59
57
50.0
11
50.1
50.3
50.2
20
20.3
53
30
32
49
48
31
24
41
10

FIG. 7

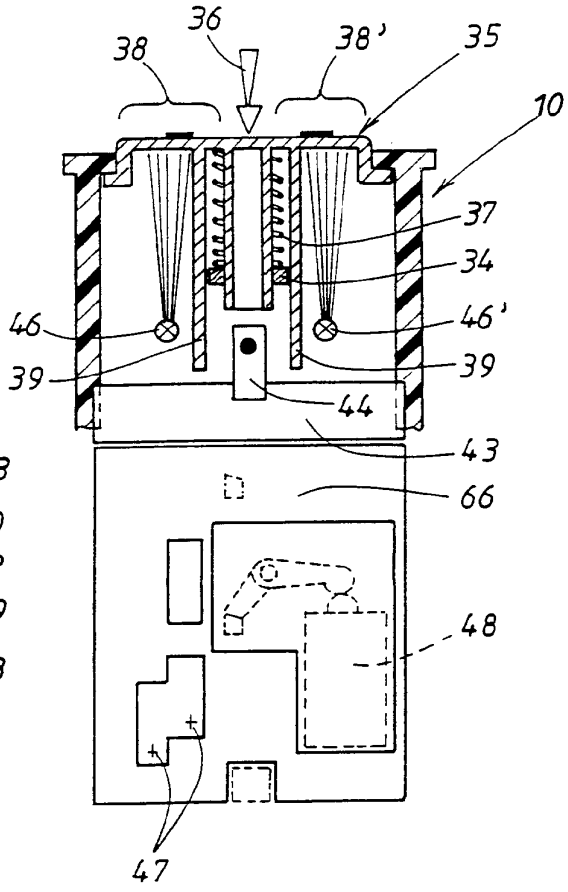

36
38
38'
35
10
37
34
46
46'
39
39
44
43
66
48
47

FIG. 8

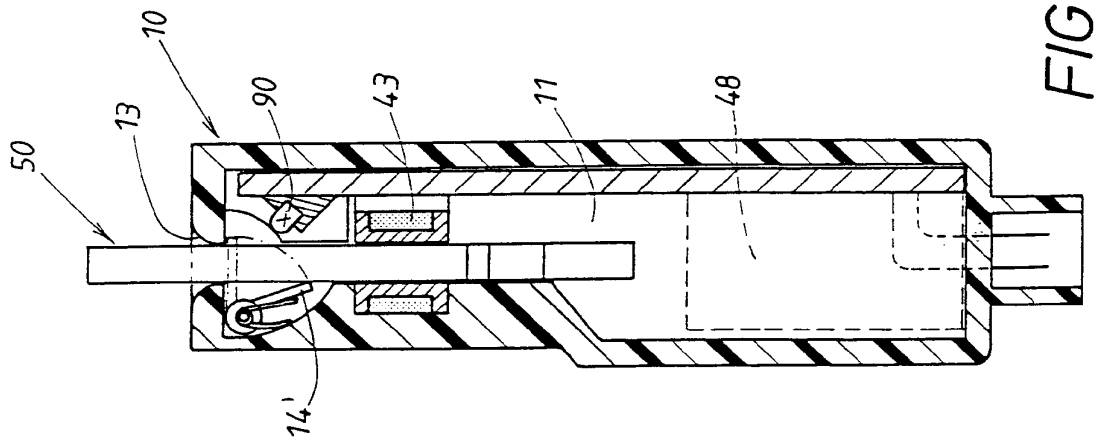

10
13
90
43
11
48
50
14'

FIG. 10

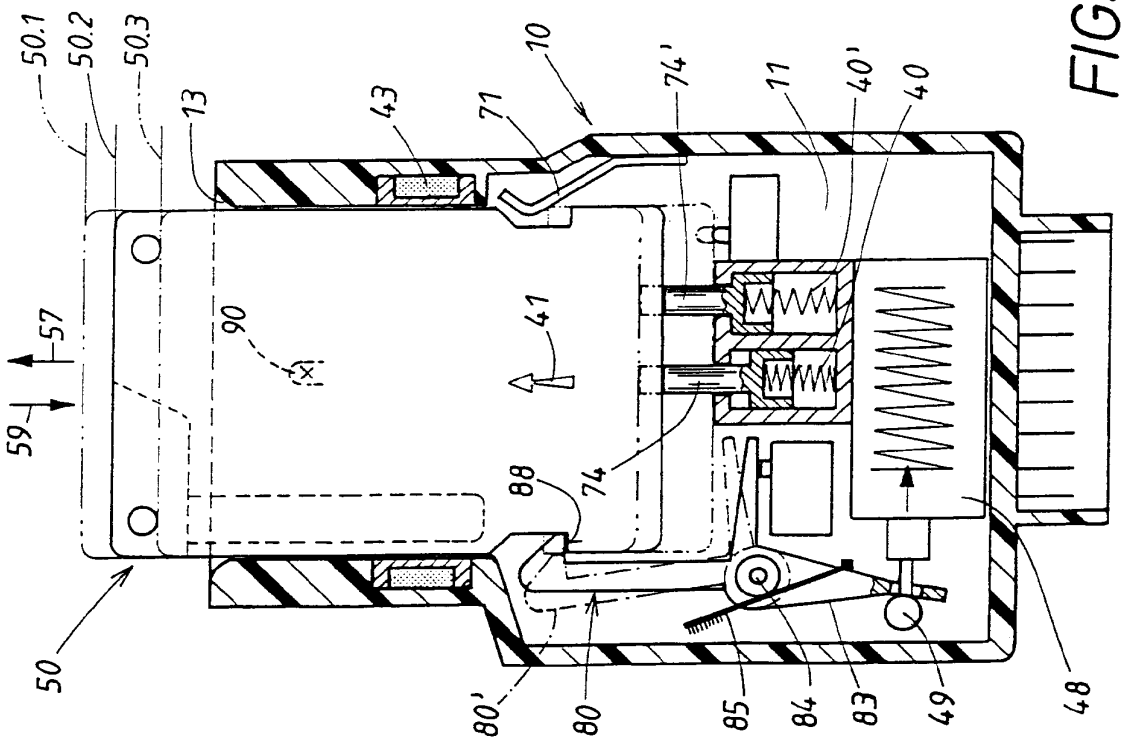

50.1
50.2
50.3
13
43
71
10
74'
11
40'
40
57
59
90
41
74
88
50
80'
80
85
84
83
49
48

FIG. 9

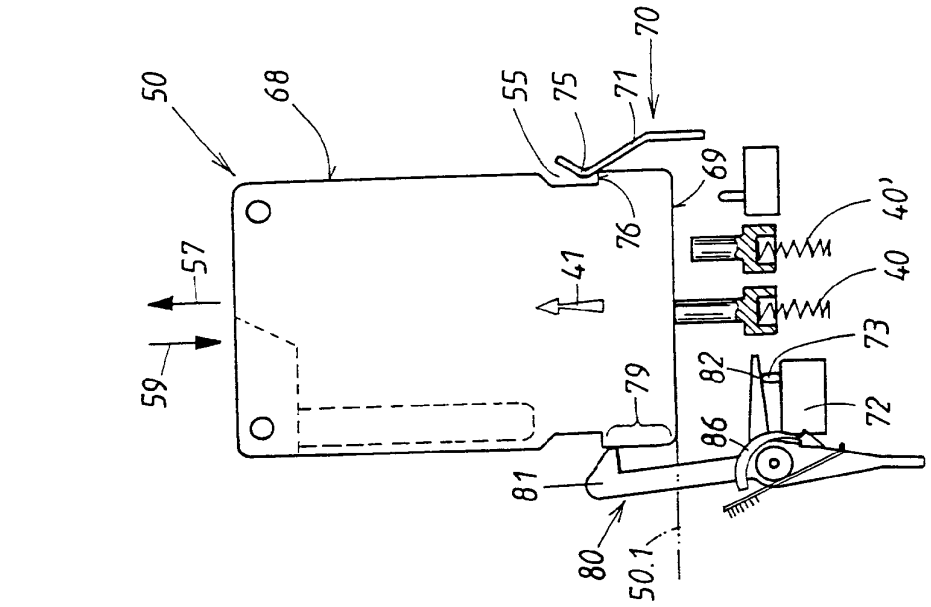

50
68
55
75
71
70
69
40'
40
73
72
82
86
79
76
41
57
59
81
80
50.1

FIG. 12

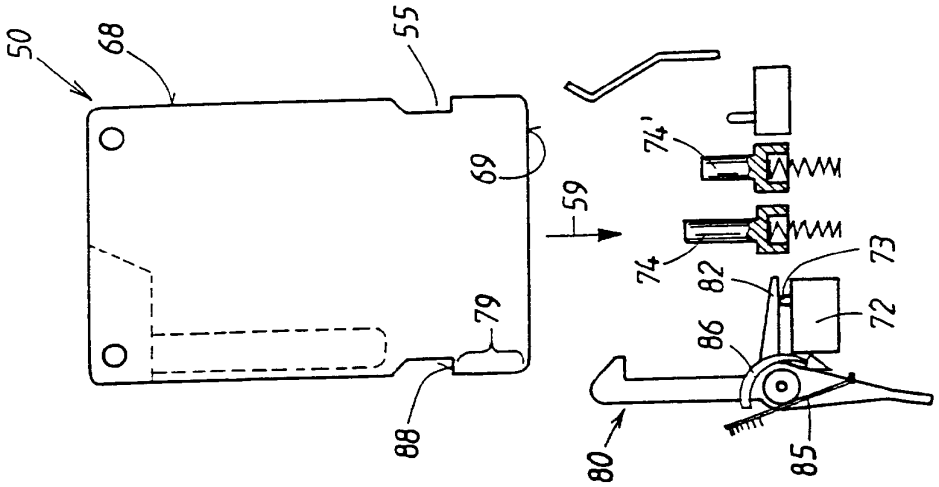

50
68
55
69
59
74'
74
73
72
82
86
79
88
80
85

FIG. 11

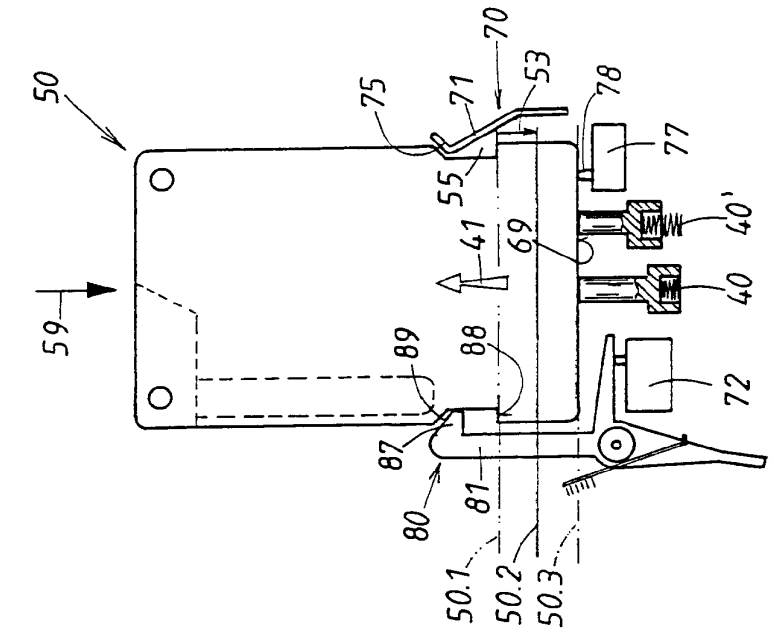

50
75
71
70
53
78
77
55
41
69
40'
40
59
89
88
72
87
81
80
50.1
50.2
50.3

FIG. 14

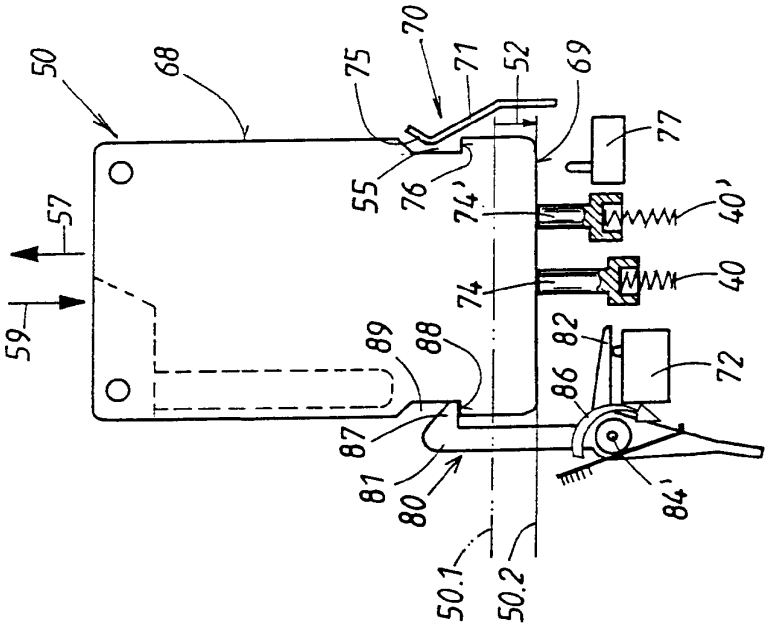

50
68
75
70
71
52
69
77
55
76
74'
40'
57
59
74
40
89
88
82
72
86
87
81
80
84'
50.1
50.2

FIG. 13

INTERNATIONAL SEARCH REPORT

Interr.. .nal Application No
PCT/EP 00/07769

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 B60R25/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 33 06 863 A (DAIMLER BENZ AG) 6 September 1984 (1984-09-06)	1-4,28
Y	page 12, paragraph 2 -page 15, paragraph 2	10-12
A	figures 3-8	17
Y	DE 196 41 898 C (KOSTAL LEOPOLD GMBH & CO KG) 13 November 1997 (1997-11-13) column 2, line 30 - line 49; figures 1,2	10,12
Y	DE 197 47 732 A (BOSCH GMBH ROBERT) 20 May 1999 (1999-05-20) column 2, line 6 - line 14	11
A	US 5 254 996 A (CLAAR KLAUS ET AL) 19 October 1993 (1993-10-19) column 5, line 25 -column 6, line 32; figures 1,2	11

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 2000	04/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Areal Calama, A-A

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/EP 00/07769

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 00 29267 A (BOSCH GMBH ROBERT ;FEUCHTER UWE (DE); GEIL ANDREAS (DE)) 25 May 2000 (2000-05-25) page 14, paragraph 4 -page 18, last paragraph; figures 1-3	1,3,10, 11

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. nal Application No
PCT/EP 00/07769

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3306863 A	06-09-1984	NONE	
DE 19641898 C	13-11-1997	NONE	
DE 19747732 A	20-05-1999	AU 1142699 A	17-05-1999
		WO 9921741 A	06-05-1999
US 5254996 A	19-10-1993	DE 4038038 C	02-01-1992
		EP 0492061 A	01-07-1992
		ES 2061141 T	01-12-1994
		JP 2053015 C	10-05-1996
		JP 4273794 A	29-09-1992
		JP 7044729 B	15-05-1995
WO 0029267 A	25-05-2000	DE 19853075 A	25-05-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Interr. nales Aktenzeichen
PCT/EP 00/07769

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 B60R25/04

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 B60R

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y A	DE 33 06 863 A (DAIMLER BENZ AG) 6. September 1984 (1984-09-06) Seite 12, Absatz 2 -Seite 15, Absatz 2 Abbildungen 3-8	1-4,28 10-12 17
Y	DE 196 41 898 C (KOSTAL LEOPOLD GMBH & CO KG) 13. November 1997 (1997-11-13) Spalte 2, Zeile 30 - Zeile 49; Abbildungen 1,2	10,12
Y	DE 197 47 732 A (BOSCH GMBH ROBERT) 20. Mai 1999 (1999-05-20) Spalte 2, Zeile 6 - Zeile 14	11
A	US 5 254 996 A (CLAAR KLAUS ET AL) 19. Oktober 1993 (1993-10-19) Spalte 5, Zeile 25 -Spalte 6, Zeile 32; Abbildungen 1,2	11

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. November 2000	04/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Areal Calama, A-A

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Interi. ,nales Aktenzeichen
PCT/EP 00/07769

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	WO 00 29267 A (BOSCH GMBH ROBERT ;FEUCHTER UWE (DE); GEIL ANDREAS (DE)) 25. Mai 2000 (2000-05-25) Seite 14, Absatz 4 -Seite 18, letzter Absatz; Abbildungen 1-3	1,3,10, 11

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/07769

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
DE 3306863	A	06-09-1984	KEINE		
DE 19641898	C	13-11-1997	KEINE		
DE 19747732	A	20-05-1999	AU	1142699 A	17-05-1999
			WO	9921741 A	06-05-1999
US 5254996	A	19-10-1993	DE	4038038 C	02-01-1992
			EP	0492061 A	01-07-1992
			ES	2061141 T	01-12-1994
			JP	2053015 C	10-05-1996
			JP	4273794 A	29-09-1992
			JP	7044729 B	15-05-1995
WO 0029267	A	25-05-2000	DE	19853075 A	25-05-2000

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
31. Mai 2001 (31.05.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/38673 A1

(51) Internationale Patentklassifikation[7]: E05B 19/04, A45C 11/32

(21) Internationales Aktenzeichen: PCT/EP00/11504

(22) Internationales Anmeldedatum:
18. November 2000 (18.11.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 56 392.6 24. November 1999 (24.11.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **WITTWER, Reinhard** [DE/DE]; Beuthener Strasse 26, 42579 Heiligenhaus (DE). **BARRENBERG, Günter** [DE/DE]; Am Buschkothen 20, 42551 Velbert (DE). **HABECKE, Mathias** [DE/DE]; Nikolaus-Gross-Strasse 12, 45529 Hattingen (DE). **JACOB, Dirk** [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE).

(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

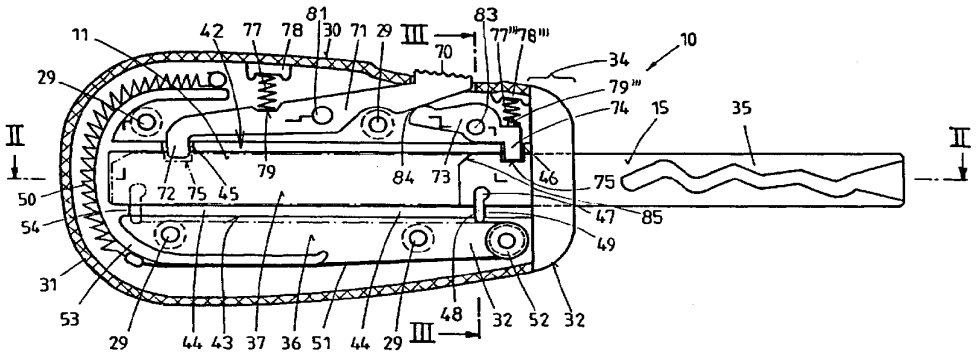
(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: KEY, IN PARTICULAR FOR A MOTOR VEHICLE

(54) Bezeichnung: SCHLÜSSEL, INSBESONDERE FÜR KFZ



(57) Abstract: The invention relates to a key, in particular for a motor vehicle, comprising a housing (30) and a mechanical key part (35) connected thereto. In keys of this type, the locking element of the key part is usually converted from an inoperative position (11) into a working position (15), in which the key (10) can be used to mechanically operate a lock or a locking cylinder, by means of a mechanism (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) which is located in the housing. In order to improve a key of this type, the invention proposes the provision of a traction or force of pressure regulator (50) for the mechanism (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) which acts indirectly upon the actuator (47) via traction or thrust means (51).

(57) Zusammenfassung: Die Erfindung betrifft einen Schlüssel, insbesondere für Kfz mit einem Gehäuseteil (30) und einem daran angeordneten mechanischen Schlüsselteil (35). Bei solchen Schlüsseln ist es bekannt, den schliesswirksamen Teil des Schlüsselteils mittels einer Mimik (47, 50, 51, 52, 60, 61, 62, 64, 65, 66), welche im Gehäuse angeordnet ist, von einer Ruhestellung (11) in eine Arbeitsstellung (15) zu überführen, in der der Schlüssel (10) zur mechanischen Betätigung eines Schlosses oder Schliesszylinders benutzt werden kann. Zur Verbesserung eines derartigen Schlüssels wird vorgeschlagen, dass die Mimik (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) einen Zug- (50) oder Druckkraftspeicher umfasst, der indirekt über ein Zug- (51) oder Schubmittel an dem Stellglied (47) angreift.

WO 01/38673 A1

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*
— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Schlüssel, insbesondere für Kfz

Die Erfindung richtet sich auf einen Schlüssel der in Anspruch 1 genannten Art. Derartige Schlüssel kommen insbesondere bei Kraftfahrzeugen zur Anwendung.

Aus der US 2,690,666, als nächstliegenden Stand der Technik, ist ein Schlüsselhalter bekannt, bei dem in einem Gehäuse befindliche Schlüssel über ihnen zugeordnete Druckfedern aus dem Gehäuse herausbewegt werden können. Bei diesem Schlüsselhalter kann jeweils ein Schlüssel über einen Wahlschalter ausgewählt werden, und der Schlüssel dann durch Betätigung eines Auslösemittels freigegeben werden. Der ausgewählte Schlüssel wird daraufhin von der Kraft der Druckfeder aus dem Gehäuse heraus in seine Arbeitsstellung überführt. Die Federn greifen bei dem Gegenstand der US-Schrift direkt am hinteren Ende der Schlüssel an, so daß sie in der Ruhestellung des Schlüssels im Gehäuseinnenraum einen erheblichen Teil der Baulänge des Schlüsselgehäuses einnehmen. Eine erhöhte Baulänge ist jedoch insbesondere bei Kfz-Schlüsseln nicht wünschenswert, die während des Betriebes eines Kfz in dessen Zündschloß verbleiben, da durch die in

den Bewegungsraum eines Knies hineinragenden Schlüssel das Verletzungsrisiko im Bereich des rechten Knies einer Fahrerin oder eines Fahrers erhöht wird.

Aus der US 2,550,375 ist ebenfalls ein in einem Gehäuse lateral verschieblich angeordneter Schlüssel bekannt. Auch bei diesem Schlüssel ist im rückwärtigen Bauraum des Schlüssels ein Federglied angeordnet, welches direkt auf den Schlüssel einwirkt. Das Federglied ist hier jedoch als Zugfeder ausgeführt, welches den Schlüssel von seiner ausgeschobenen Lage in seine eingezogene Position automatisch zurückfährt, wenn eine Auslösetaste betätigt wird, die den Schlüssel freigibt.

Aus der DE-GM 17 13 197 ist ein Schlüsselgehäuse bekannt, bei dem ein darin liegender Schlüssel über eine manuelle Betätigung aus dem Gehäuse heraus oder in das Gehäuse hineingeschoben werden kann. Die Betätigung des Schlüssels über eine auf diesen einwirkende Mimik ist dieser Schrift nicht zu entnehmen. Der in dem Gehäuse befindliche Schlüssel kann lediglich über ein oder mehrere Federelemente in seiner im Gehäuse eingezogenen oder aus dem Gehäuse herausgeschobenen Stellung fixiert werden.

Bei einem von der Firma Huf gefertigten Elektronischen-Mechanischen-Schlüssel ist es bekannt, einen mechanischen Schlüsselteil aus- und einklappbar an einem Schlüsselgehäuse anzuordnen. Bei diesem Schlüssel ist die Schlüsselelektronik in einem ersten Gehäuseteil und der mechanische Schlüsselteil in und an einem zweiten Gehäuseteil angeordnet. Die Schnittstellen zwischen dem ersten und dem zweiten Gehäuseteil sind bei diesem Schlüssel sehr verwinkelt und maßlich kompliziert.

Der mechanische Schlüsselteil liegt im eingeklappten Zustand an einer Längsseite des Schlüsselgehäuses, innerhalb einer Eintiefung, die als Schlüsselaufnahme dient.

Der Schlüssel ist in der Aufnahme des Gehäuses an seiner in Ausklapprichtung liegenden Seite offen zugänglich.

Außen an dem Schlüssel ist eine Auslösetaste angeordnet, über deren Betätigung der Schlüssel von seiner Ruhestellung am Gehäuse in eine Arbeitsstellung ausgeklappt werden kann, in der das mechanische Schlüsselteil z.B. zur Betätigung eines Schließzylinders oder eines Zündschlosses benutzt werden kann. Der Ausklappvorgang geschieht nach Betätigen der Auslösetaste automatisch über einen im Schlüsselgehäuse angeordneten Federtrieb der auf den mechanischen Schlüsselteil wirkt.

Zum Einklappen des mechanischen Schlüsselteils muss erneut die Auslösetaste gedrückt werden und der Schlüssel dann manuell wieder in seine Ruhestellung in der seitlich am Gehäuse angeordneten Aufnahme eingeklappt werden.

Von Nachteil bei einem derartigen Schlüssel ist es, dass sich an dem in der Aufnahme offen zugänglichen Schlüssel Dreckpartikel sammeln, die über den mechanischen Schlüsselteil in den zu betätigenden Schließzylinder und/oder des Zündschloss etc. gelangen und diese dadurch auf Dauer verschmutzen und gegebenenfalls funktionsuntüchtig werden können. Auch ist die Öffnung in die der Schlüssel einklappen kann optisch unschön.

Aus der DE 296 18 616 U1 ist ein Kraftfahrzeugschlüssel bekannt, der ebenfalls über eine Mimik von einer an einer Gehäuseseite angeklappten Lage in eine aus dem Gehäuse herausstehende, ausgeklappte Arbeitslage überführbar ist.

Aufgabe der vorliegenden Erfindung ist es, einen Schlüssel bereitzustellen, der einen verhältnismäßig kurzen Bauraum aufweist und der ein gutes optisches Erscheinungsbild aufweist.

Dieses wird erfindungsgemäß durch die im Anspruch 1 genannten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt. Zur Lösung der patentgemäßen Aufgabe wird vorgeschlagen, das Schlüsselteil in seiner Ruhestellung innen im Gehäuse anzuordnen, wobei das Schlüsselteil nach Betätigung der Auslösetaste über eine in dem Gehäuse angeordnete Mimik von seiner Ruhestellung im Inneren des Gehäuses durch eine Längsverschiebung in seine Arbeitsstellung überführt wird, in der zumindest der schließwirksame Teil des mechanischen Schlüsselteils außerhalb des Gehäuses liegt. Hierzu weist die Mimik einen Zug- oder Druckkraftspeicher auf, der indirekt über ein Zug- oder Schubmittel an dem Stellglied des Schlüsselteils angreift. Durch diese Maßnahmen ist es nicht mehr notwendig, den Zug- oder Druckkraftspeicher in unmittelbarer Nachbarschaft zum mechanischen Schlüsselteil anzuordnen, um das Bewegungsmoment vom Zuf- oder Druckkraftspeicher auf das mechanische Schlüsselteil zu übertragen. Vielmehr wird es möglich, den Zug- oder Druckkraftspeicher an jeder beliebigen Position im Schlüsselgehäuse anzuordnen. So kann der Zug- oder Druckkraftspeicher insbesondere auch seitlich, neben dem im Gehäuse eingezogenen Schlüssel angeordnet werden. Der Bauraum, insbesondere die Bauraumlänge des Schlüsselgehäuses kann hierdurch vermindert werden. Ebenfalls wird eine größere Variationsbreite bei der Formgestaltung des Schlüsselgehäuses ermöglicht. Der Zugkraftspeicher könnte z.B. eine zugbelastete Feder, ein Gummielement, eine Unterdruckkammer, ein Solenoid etc. sein. Als Druckkraftspeicher können z.B. vorgesehen sein linear wirkende Druckfedern, Spiralfedern, elastische Elemente (z.B. aus Kunststoff), Druckkörper, Solenoide etc.

Bei der indirekten Übertragung der Verstellbewegung vom Druckkraftspeicher auf das mechanische Schlüsselteil kann das Schubmittel z.B. ein Treibriemen, eine Stellkette, ein Stellband, ein Zahnriemen, ein Zahnrad etc. sein.

Um ein reibungsloses Herausfahren des mechanischen Schlüsselteils zu gewährleisten, sind im Innenraum des Gehäuses Mittel angeordnet, durch die das Schlüsselteil bei der Längsbewegung von seiner Ruhestellung in seine Arbeitsstellung geführt ist.

Ein weiterer Vorteil der sich aus der erfindungsgemäßen Lösung gemäß Anspruch 1 ergibt ist der, dass an dem Schlüsselgehäuse nunmehr glatte Flächen überwiegen und keine vorstehenden Kanten und unschöne Vertiefungen mehr vorhanden sind, so dass der Schlüssel eine sehr ansprechende Optik aufweist.

Außerdem ist die Bedienungsfreundlichkeit durch das automatische Ausfahren des mechanischen Schlüsselteils und dem einfach zu bewirkenden Wiedereinschieben desselben verbessert worden.

Vorteilhaft nach Anspruch 2 kann es auch sein, wenn die Schlüsselöffnung im Gehäuseteil im wesentlichen formschlüssig zur Außenkontur des mechanischen Schlüsselteils ausgeführt ist, so dass möglichst wenig Öffnungsraum zwischen Gehäusewand und Schlüsselteil vorhanden ist, an dem Schmutzpartikel in das Gehäuseinnere eindringen können. Ferner wird durch die formschlüssige Ausführung der Öffnung ein Abstreifen von eventuell während oder nach der Betätigung aufgefangenen Schmutzpartikeln ermöglicht.

In einer weiteren günstigen Ausführungsform der Erfindung kann gemäß Anspruch 3 auch ein Mittel zum Verschließen der Schlüsselöffnung, wie etwa eine Klappe oder ein Schieber, der manuell oder automatisch betätigt wird, vorgesehen sein, der das Gehäuseteil in der Ruhestellung des darin angeordneten mechanischen Schlüsselteils gegen ein Eindringen von Schmutz gänzlich abriegelt.

Vorteilhaft gemäß Anspruch 4 kann es sein, wenn das Schlüsselteil innerhalb des Gehäuseteils in einem Führungskanal liegt, innerhalb dessen das Schlüsselteil bei

seiner Längsverschiebung geführt ist. Günstigerweise können zur Erzeugung des Führungskanals auch umgebende Gehäusewände wie z.B. die an den Flächenseiten des umgebenden Gehäuseteils liegenden Wände zur Ausbildung des Führungskanals herangezogen werden.

Der Führungskanal kann eine seitliche Öffnung aufweisen, durch den ein Stellglied, wie etwa ein Zahnrad oder ein Mitnehmerzapfen, auf das mechanische Schlüsselteil einwirken kann und derart eine von der Mimik ausgeübte Verstellbewegung auf das mechanische Schlüsselteil überträgt.

Günstig kann es auch sein, wenn Rastmittel vorgesehen sind, die das mechanische Schlüsselteil in seiner Ruhe- und in seine Arbeitsstellung im wesentlichen bewegungsstarr halten. Nach Betätigung der Auslösetaste oder eines anderen Auslösemittels geben die Rastmittel das mechanische Schließteil frei, so dass diese von der einen Stellung in die andere Stellung verfahrbar ist. Die Rastmittel können z.B. an einem oder mehreren Hebeln angeordnete Haken umfassen, die in der Raststellung in eine am Umfang des Schließteils befindliche Aussparung eingreifen, oder die in einem Vorsprung, einer Nase, einem Gegenrastglied etc. eines zur Mimik gehörenden Stellmittels angreifen und derart indirekt das mechanische Schließteil in seiner Arbeits- oder Ruhestellung halten.

Bei der Verwendung eines Zugkraftspeichers kann es günstig sein, wenn der Zugweg des Zugkraftspeichers und/oder des durch den Zugkraftspeichers betätigten Zugmittels durch ein- oder mehrfache Umlenkung des Zugkraftspeichers und/oder des Zugmittels an einem oder mehreren Umlenkteilen, wie z.B. Umlenkrollen oder Umlenkstegen vergrößert ist. Durch diese Maßnahme wird ein weitgehendes Herausfahren des mechanischen Schließteils bei der Überführung von seiner Ruhestellung in seine Arbeitsstellung erreicht.

Es kann ferner vorteilhaft sein, die Schlüsselelektronik und die Schlüsselmechanik in zwei, in sich abgeschlossenen Gehäuseteilen anzuordnen, die beide entlang ebener Verbindungsflächen lösbar aneinander festgelegt sind. Günstigerweise ist der Batteriedeckel derart an dem Gehäuseteil angeordnet das die Schlüsselelektronik aufweist, dass er durch das gegenüberliegende Gehäuseteil mit der Mechanik darin verdeckt wird. Zum Wechseln der Batterie muss also lediglich eine Trennung der beiden Gehäuseteile voneinander vorgenommen werden um danach den Batteriedeckel öffnen zu können. Zur Verbindung der beiden Gehäuseteile sind die verschiedensten Verbindungsmittel denkbar. So können z.B. Schwalbenschwanznuten oder -vertiefungen und Schwalbenschwanzvorsprünge - oder -erhöhungen an den Gehäuseteilen angeordnet sein, die ineinandergeschoben die Verbindung der beiden Gehäuseteile gewährleisten.

Weitere Vorteile und Maßnahmen der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in drei Ausführungsbeispielen dargestellt. Es zeigen:

Fig. 1 schematisch eine erste Ausführungsform eines erfindungsgemäßen Schlüssels im Schnitt durch das zweite, die Mechanik enthaltene Gehäuseteil,

Fig. 2 schematisch, die erste Ausführungsform eines erfindungsgemäßen Schlüssels im Schnitt gemäß II - II aus Fig. 1,

Fig. 3 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt gemäß III - III aus Fig. 1,

Fig. 4 schematisch, das erste Gehäuseteil der ersten Ausführungsform des erfindungsgemäßen Schlüssels mit der Schlüsselelektronik gemäß dem Schnitt IV - IV aus Fig. 2,

Fig. 5 schematisch, das zweite Gehäuseteil der ersten Ausführungsform des erfindungsgemäßen Schlüssels mit dem mechanischen Schlüssel im Schnitt gemäß V - V aus Fig. 2,

Fig. 6 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels in Seitenansicht, bei dem beide Gehäuseteile aneinander festgelegt sind,

Fig. 7 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels, bei dem die Verbindungsmittel der beiden Gehäuseteile gelöst sind,

Fig. 8 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels in einem Schnitt entlang VIII - VIII aus Fig. 6,

Fig. 9 schematisch, ein zweites Ausführungsbeispiel eines erfindungsgemäßen Schlüssels, in einem Schnitt durch das zweite Gehäuseteil mit der Schlüsselmechanik,

Fig. 10 schematisch, die zweite Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt gemäß X - X aus Fig. 9,

Fig. 11 schematisch, eine dritte Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt durch das die

Mechanik aufweisende zweite Gehäuseteil, in der Ruhestellung des mechanischen Schlüsselteils,

Fig. 12 schematisch, die dritte Ausführungsform des erfindungsgemäßen Schlüssels gemäß Fig. 11 in der Arbeitsstellung des mechanischen Schlüsselteils.

In den Fig. 1 bis 8 ist eine erste Ausführungsform des erfindungsgemäßen Schlüssels 10 dargestellt. Bei dieser Ausführungsform setzt sich der Schlüssel zusammen aus einem ersten Gehäuseteil 20 und einem zweiten Gehäuseteil 30. Das erste Gehäuseteil umfasst eine Gehäusegrundplatte 22 und einen Gehäusedeckel 21. In dem Gehäusedeckel 21 sind Tastfelder 26 angeordnet, über die eine im Inneren des ersten Gehäuseteiles 20 liegende Elektronik 25 betätigt werden kann. In der Gehäusegrundplatte 22 ist ein Batteriefachdeckel 23 angeordnet, über den eine Batterie 24, die der Stromversorgung der Elektronik 25 dient, in das Gehäuseteil 20 ein- und ausgeführt werden kann. Das erste Gehäuseteil 20 ist wasserdicht verschlossen, wobei der Gehäusedeckel 21 an der Gehäusegrundplatte 22 über Schraubmittel 29 festgelegt ist. An dem Schlüssel 10 ist in diesem Ausführungsbeispiel noch eine Öse 19 vorgesehen, an die z.B. ein Schlüsselanhänger angebracht werden kann.

An dem ersten Gehäuseteil 20 ist entlang einer planaren Ebene 14 ein zweites Gehäuseteil 30 angeordnet. Das zweite Gehäuseteil 30 besteht in diesem Ausführungsbeispiel ebenfalls aus einer Gehäusegrundplatte 32 und einem diese abdeckenden Gehäusedeckel 31. Beide Gehäuseteile 20 und 30 sind über Verbindungsmittel 28, 33 lösbar miteinander verbunden. Bei diesen Verbindungsmitteln handelt es sich in diesem Ausführungsbeispiel um Verrastmittelvorsprünge 28, die in Nuten 27 in der Gehäusegrundplatte 32 des ersten Gehäuseteiles 20 angeordnet sind und auf Seiten des zweiten Gehäuseteiles 30 um Schwalbenschwanzzapfen 33, die an der Gehäusegrundplatte 32 angeformt

sind. Um beide Gehäuseteile 20, 30 voneinander zu lösen, z.B. zum Zwecke des Austausches der Batterie 23, werden beide Gehäuseteile in Demontagerichtung 17 (Fig. 7) gegeneinander verschoben, wobei ein Anfangswiderstand zu überwinden sein kann. Die Schwalbenschwanzzapfen 33 befinden sich nach dieser Verschiebung gemäß Pfeil 17 in dem offenen Teil der Nut 27, so dass nun beide Gehäuseteile 20, 30 voneinander getrennt werden können. Zur Montage müssen die beiden Gehäuseteile 20 und 30 in entsprechender Weise aneinandergesetzt werden, wobei die Schwalbenschwanzzapfen 33 in die Nut 27 an dem gegenüberliegenden Gehäuseteil eingeführt werden müssen, und das Gehäuseteil 20 daraufhin in Montagerichtung 18 (Fig. 7) gegenüber dem Gehäuseteil 30 verschoben werden. Die Schwalbenschwanzzapfen 33 verhaken sich dabei hinter dem Verrastmittelvorsprung 28 in der Gehäusegrundplatte 22 des ersten Gehäuseteiles, wodurch beide Gehäuseteile 20, 30 aneinander festgelegt werden. Durch das Festlegen der beiden Gehäuseteile entlang einer Ebene wird die vorbeschriebene Montage/Demontage vereinfacht.

In dem zweiten Gehäuseteil 30 ist eine Schlüsselmechanik angeordnet, über die ein mechanisches Schlüsselteil 35, welches sich in einer Ruhestellung 11 im Gehäuseinnenraum 36 des zweiten Gehäuseteils 30 befindet, durch Betätigung eines Auslösemittels, wie etwa einer Auslösetaste 70 automatisch in eine Arbeitsstellung 15 verfahren werden kann, in der das mechanische Schlüsselteil 35 zur Betätigung eines Schließzylinders oder eines Zündschlosses etc. verwendet werden kann. Das mechanische Schlüsselteil 35 ist dazu in dem vorliegenden Ausführungsbeispiel gemäß den Fig. 1 bis 8 wie folgt in dem zweiten Gehäuseteil 30 angeordnet.

Im Gehäuseinnenraum 36 des zweiten Gehäuseteils 30 ist ein Führungskanal 37 angeordnet, dessen beide Flächenwände 40 und 41 aus den Flächenseiten 38 und 39 der angrenzenden Gehäusegrundplatte 32 und des Gehäusedeckels 31 gebildet wird. Der Führungskanal 37 wird weiterhin zu seinen beiden Seiten von den Wänden 42 und 43 begrenzt. In dem Führungskanal 37 ist das mechanische Schlüsselteil 35

verschiebbar angeordnet. Dieser Führungskanal 37 ist an seinem vorderen Ende mit einer Schlüsselöffnung 12 versehen, durch die das mechanische Schlüsselteil 35 aus dem Gehäuseteil 20 heraus in seiner Arbeitsstellung 15 gelangen kann. In seinem hinteren Bereich ist der Führungskanal 37 in diesem Ausführungsbeispiel durch eine Führungswand 53 abgeschlossen. An der, der Wand 42 zugewandten Schmalseite des mechanischen Schlüsselteils 35 ist eine Aussparung 75 im hinteren Bereich des mechanischen Schlüsselteils 35 angeordnet. In dieser Aussparung 75 greift in der Ruhestellung 11 der Rasthaken 72 eines Hebels 71, durch den das mechanische Schlüsselteil 35 in der Ruhestellung 11 gehalten wird. Der Rasthaken 72 wird dabei mit der Kraft eines Druckmittels 77, wie etwa einer Feder, die an der Ansatzstelle 79 am Hebel 71 angreift und die anderenends in einem Federsitz 78 an der Wand des Gehäusedeckels 31 abgestützt ist, in der Aussparung 75 gehalten. Der Hebel 71 ist an einer Achse 81 schwenkbar gelagert. Der Hebel 71 ist über eine Auslösetaste 70, die in diesem Ausführungsbeispiel an den Hebel 71 angeformt ist, zu betätigen, wodurch der Rasthaken 72 aus der Aussparung 75 ausrastet, wenn das mechanische Schlüsselteil 35 in seiner Ruhestellung 11 sitzt.

Damit der Rasthaken 72 die Wand 42 durchgreifen kann, um in die Aussparung 75 im mechanischen Schlüsselteil 35 einzugreifen, ist in der Wand 42 eine Öffnung 45 vorgesehen.

Im vorderen Bereich des Schlüssels 10 unmittelbar hinter einem Frontteil 34 der Gehäusegrundplatte, in welcher die Schlüsselöffnung 12 sitzt, ist ein zweiter Hebel 73 angeordnet, der um eine Achse 83 verschwenkbar ist, und der einen Rasthaken 74 aufweist, der in der Arbeitsstellung 15 des mechanischen Schlüsselteils 35 in die Aussparung 75 im mechanischen Schlüsselteil 35 eingreift. In der Wand 42 des Führungskanals 37 ist wiederum eine Öffnung 46 vorgesehen, die ein Durchgreifen der Wand 42 durch den Rasthaken 74 erlaubt. Der Rasthaken 74 wird wiederum mittels der Kraft einer Feder 79‘‘‘, die an den Ansatzstellen 77‘‘‘ und 78‘‘‘ zwischen dem Hebel 73 und der Wand 42 des Gehäuseteils 31 festgelegt ist. Der

Hebel 73 steht an der Berührungsstelle 84 in mechanischem Kontakt mit dem Hebel 71. Bei einer Betätigung der Auslösetaste 70 wird hierdurch, neben dem Hebel 71, auch der Hebel 73 betätigt und der Rasthaken 74 aus dem Führungskanal 37 und gegebenenfalls aus der Aussparung 75 herausgezogen, wenn das mechanische Schlüsselteil 35 in seiner Arbeitsstellung 15 sitzt. Der aus den Hebeln 71 und 73 gebildete Doppelhebel ermöglicht es, dass an dem mechanischen Schlüsselteil nur eine Aussparung 75 am Ende des Schaftes des Schlüsselteils erforderlich ist.

Das mechanische Schlüsselteil 35 kann über eine Mimik nach Betätigung der Auslösetaste 70 automatisch aus seiner Ruhestellung 11 in die Arbeitsstellung 15 überführt werden. Hierzu ist in dem vorliegenden Ausführungsbeispiel zunächst ein Zugkraftspeicher 50 in Form einer Zugfeder vorgesehen, die im hinteren Bereich des Gehäuseteils 30 angeordnet ist. Die Feder 50 ist mit einem Zugmittel 51 wie etwa einem Kunststoffstrang oder Kunststoffband verbunden, wobei die Feder 50 und Zugmittel 51 im hinteren Bereich des Gehäuseteils 30 entlang der Führungswand 53 geführt sind. Das Zugmittel 51 ist andernends wiederum an einem Stellglied 47 festgelegt, welches seinerseits fest verbunden mit dem mechanischen Schlüsselteil 35 ist, welches im hinteren Bereich des Schlüsselteils 35 angeordnet ist. Das Zugmittel 51 ist im vorderen Bereich des Gehäuseteils 30 um eine Umlenkrolle 52 herumgeführt, so dass der Zugweg der Feder 50 und des Zugmittels 51 parallel zur Ausschubrichtung 16 und zum Verlauf des Führungskanals 37 des mechanischen Schlüsselteils 35 verläuft. In der Seitenwand 43 des Führungskanals 37 ist eine längliche Öffnung 44 vorgesehen, durch die das Stellglied 47 hindurchgreift. Das Zugmittel 51 ist auf der dem Führungskanal 37 abgewandten Seite des Stellgliedes 47 mit dessen Nase 48 verbunden.

In der Ruhestellung 11 des mechanischen Schlüsselteils 35 befindet sich die Nase 48 des Stellgliedes 47 an dem, die Längsöffnung 44 im rückwärtigen Bereich begrenzenden Anschlag 54. Der Schlüssel ist in der Ruhestellung 11 gänzlich in das Gehäuseteil 30 eingefahren. Zur Überführung des mechanischen Schlüsselteils 35 in

seiner Arbeitsstellung 15 muss nun die Auslösetaste 70 und somit der Hebel 71 betätigt werden, so dass der Rasthaken 72 aus der Aussparung 75 im mechanischen Schlüsselteil 35 herausfährt. Das mechanische Schlüsselteil 35 verfährt nun unter Einwirkung des Zugkraftspeichers 50 in Ausschubrichtung 16 aus dem Gehäuseteil 30 hinaus in seine Arbeitsstellung 15. Bei Erreichen der Arbeitsstellung 15 fährt die Nase 48 des Stellgliedes 47 gegen den Anschlag 49, der die Öffnung 44 an ihrem der Schlüsselöffnung zugewandten Ende begrenzt. Sobald das mechanische Schlüsselteil 35 in dieser Stellung ist, rastet zusätzlich noch der Rasthaken 74 in der Aussparung 75 am mechanischen Schlüsselteil 35 unter der Kraft der Feder 77‘‘‘ ein.

Zum Rücküberführen des mechanischen Schlüsselteiles 35 aus seiner Arbeitsstellung 15 in die Ruhestellung 11 muss wiederum die Auslösetaste 70 manuell betätigt werden, wodurch der Hebel 73 verschwenkt wird und der daran angeordnete Rasthaken 74 aus der Aussparung 75 im mechanischen Schlüsselteil 35 herausfährt. Hierdurch kann nun das mechanische Schlüsselteil 35 manuell wieder in den Führungskanal 37 im Gehäuseteil 30 eingeschoben werden. Kurz vor Erreichen der Ruhestellung 11 fährt das mechanische Schlüsselteil 35 mit seinem hinteren Ende im Bereich seiner Auflaufschräge 85 gegen den Rasthaken 72 und stößt diesen gegen die Kraft der Feder 77 aus dem Führungskanal 37 hinaus. Der Rasthaken 72 schnappt dann bei Erreichen der Ruhestellung 11 durch das mechanische Schlüsselteil wieder in die Aussparung 75 ein und verrastet dort das mechanische Schlüsselteil 35.

Durch die manuelle Rücküberführung des mechanischen Schlüsselteils 35 in die Ruhestellung 11 ist der Zugkraftspeicher 50 wieder vorgespannt worden, so dass er bei einer erneuten Betätigung der Auslösetaste 70 das mechanische Schlüsselteil 35 wiederum aus seiner Ruhestellung 11 in seine Arbeitsstellung 15 überführen kann.

In den Fig. 9 und 10 ist nun ein weiteres Ausführungsbeispiel des erfindungsgemäßen Schlüssels dargestellt. In einem Gehäuseteil 30' ist wiederum ein mechanisches Schlüsselteil 35' in einem in dem Gehäuseteil 30' liegenden Führungskanal 37' verschieblich angeordnet. Der Führungskanal 37' wird gebildet aus den beiden Flächenwänden 40' und 41', die Abschnitten der Flächenseiten 38' und 39' der Gehäusegrundplatte 32' und des Gehäusedeckels 31' entsprechen. Die Seiten des Führungskanals 37' werden durch Wände 42' und 43' gebildet. In der Wand 43' ist eine Öffnung 44' vorgesehen, durch die ein als Zahnrad ausgeformtes Stellglied 47' hindurchgreift und die Zähne 62 des Zahnrades 47' in eine Zahnung 64 am mechanischen Schlüsselteil 35' eingreifen. Das Zahnrad 47' sitzt auf einer Achse 63, die in diesem Ausführungsbeispiel an der Gehäusegrundplatte 32' angeformt ist. Das Zahnrad 47' weist in seinem oberen Bereich einen Hohlraum auf, in dem ein Druckkraftspeicher 60, wie eine Spiralfeder angeordnet ist. Im unteren Umfangsbereich des Zahnrades unterhalb der Zahnung 62 ist eine Aussparung 76 vorgesehen, in die der Rasthaken 72' eines Hebels 71' hineinragt, wenn das mechanische Schlüsselteil 35' sich in seiner Ruhestellung oder seiner Arbeitsstellung befindet. Wie schon im vorausgehenden Ausführungsbeispiel ist der Hebel 71' über eine Auslösetaste 70' zu betätigen. Der Rasthaken steht wiederum unter der Kraft der Feder 77', die zwischen der rahmenseitigen Federsitz 78' und der Ansatzstelle 79' am Hebel 70' angeordnet ist. In Fig. 9 ist das mechanische Schlüsselteil 35' in seiner Arbeitsstellung 15 dargestellt. Strichpunktiert dargestellt ist ferner noch die Ruhestellung des mechanischen Schlüsselteils 35'.

An dem gehäuseteilseitigen Ende des mechanischen Schlüsselteils 35' ist eine Nase 48' in Richtung der Wand 42' an dem mechanischen Schlüsselteil 35' angeformt. Diese Nase 48' ist in einer Öffnung 46', die in der Wand 42' parallel zum Führungskanal 37' und der Ausschubrichtung 16 des mechanischen Schlüsselteils 35' verläuft, angeordnet. Durch die Nase 48' wird die Ausschubbewegung des mechanischen Schlüsselteils 35', die durch den Druckkraftspeicher 60 mittels des Zahnrades 47' auf das mechanische Schlüsselteil 35' übertragen wird, wenn die

Auslösetaste 70' gedrückt worden ist, begrenzt, da die Nase 48' beim Erreichen der Arbeitsstellung 15 gegen den Anschlag 49' fährt.

Zum Einfahren des mechanischen Schlüsselteils 35' muss wiederum die Auslösetaste 70' betätigt werden, so dass der Rasthaken 72' aus der Aussparung 76 herausfährt und derart eine Drehbewegung des Zahnrades 47' ermöglicht wird. Das mechanische Schlüsselteil 35' kann nun wieder in den Führungskanal 37' des Gehäuseteils 30' eingeschoben werden, wobei das Zahnrad 47' mitgedreht wird und derart der Druckkraftspeicher 60 bzw. die Spiralfeder wieder aufgezogen wird, um ein erneutes Ausfahren zu erlauben. Der Einschiebevorgang wird beendet, wenn die Nase 48' vor den Anschlag 54' läuft, der die Öffnung 46' an ihrem rückwärtigen Ende begrenzt. In der nun erreichten Ruhestellung 11 schnappt der Rasthaken 72' wieder in die Aussparung 76 am unteren Rand des Zahnrads 47' ein. Das mechanische Schlüsselteil 35' ist nunmehr in der Ruhestellung 11 verrastet. Das Verrasten des Rasthakens 72' in die Aussparung 76 am unteren Rand des Zahnrades 47' erfolgt also bei ein- und ausgeschobenem mechanischen Schlüsselteil. Dies bedeutet, dass eine Umdrehung des Zahnrades 47' gleich dem Hub des mechanischen Schlüsselteils sein muss.

Ein erneutes Ausfahren in die Arbeitsstellung 15 kann wiederum durch Betätigen der Auslösetaste 70' erfolgen, wodurch der Rasthaken 72' erneut aus der Aussparung 76 ausfährt und das Zahnrad 47', welches nunmehr freigegeben ist mit der Kraft der Spiralfeder 60 das mechanische Schlüsselteil 35' aus dem Führungskanal 37' hinausfährt und in die Arbeitsstellung 15 überführt.

In den Fig. 11 und 12 ist nun ein drittes Ausführungsbeispiel des erfindungsgemäßen Schlüssels wiedergegeben. Das mechanische Schlüsselteil 35'' ist in einem Gehäuseteil 30'' in einem Führungskanal 37'' angeordnet. Die Flächenwände 40'' des Führungskanals 37'' werden wiederum gebildet aus den Flächenseiten 38'' der Gehäusegrundplatte 32'' und der nicht dargestellten

Flächenseite des ebenfalls nicht dargestellten Gehäusedeckels. An den Schmalseiten des Führungskanals sind Wände 42'' und 43'' angeordnet, die bei diesem Ausführungsbeispiel jeweils einen Kanal 67 und einen Kanal 68 aufweisen. Die Wand 43'' weist eine längliche Öffnung 44'' auf, die parallel zur Ausschubrichtung 16 des mechanischen Schlüsselteils 35'' verläuft. Im hinteren Bereich des Gehäuseteils 30'' ist ein Druckkraftspeicher 60'' wie eine Spiralfeder angeordnet, die auf ein Zahnrad 65 einwirkt, welches drehbar auf einer Achse 63'' gelagert ist. Die Zahnung 62'' am Zahnrad 65 greift in Zahnöffnungen 66 eines Schubmittels 61, wie etwa eines Zahnriemens ein, der in den Kanälen 67 und 68, sowie um das Zahnrad 65 herum und an dem dort gegenüberliegenden Wandabschnitt 53'' geführt ist. Am vorderen Ende dieses Schubmittels/Zahnriemens 61 ist ein Stellglied 47'' angeordnet, mittels dessen eine vom Zahnriemen 61 ausgeübte Stellbewegung auf das mechanische Schlüsselteil 35'' übertragen werden kann. Am vorderen Ende des Zahnriemens 61 ist ebenfalls ein Sperrmittel 76' angeordnet, welches in der Ruhestellung 11 des mechanischen Schlüsselteils 35''an dem Rasthaken 72'' eines Hebels 71'' unter der Stellkraft des Druckkraftspeichers 60'' anliegt. Das Sperrmittel 76' liegt dabei über dem Wandabschnitt 53'' der Wand 47''.

Der Hebel 71'' ist auf einer Achse 81'' verschwenkbar gelagert. Er weist an seinem zweiten Ende eine Auslösetaste 70'' auf, mittels derer der Rasthaken 72'' entgegen der Federkraft einer Feder 77'', die an den Ansatzstellen 79'' und 78'' zwischen dem vorderen Arm des Hebels 71'' und der gehäuseseitigen Wand 43'' angeordnet ist.

In Fig. 11 ist der erfindungsgemäße Schlüssel in der Ruhestellung 11 des mechanischen Schlüsselteils 35'' dargestellt. Das mechanische Schlüsselteil 35'' liegt dabei gänzlich in dem Führungskanal 37'' gehäuseseitig hinter der Schlüsselstellung 12.

Wird die Auslösetaste 70'' betätigt, und der Hebel 71'' entgegen der Kraft der Feder 77'' verschwenkt, so gibt der Rasthaken 72'' das Sperrmittel/Sperrglied 76' frei. Hierdurch kann nun das Schubmittel 61 mit dem daran angeordneten Stellglied 47'' aufgrund des von dem Druckkraftspeicher 60'' ausgeübten Bewegungsmomentes das von dem Druckkraftspeicher 60'' auf das Zahnrad 65 und von diesem über die Zahnung 62'' und die Zahnöffnung 66 auf das Schubmittel 61 übertragen wird in Ausschubrichtung 16 auf die Schlüsselöffnung 12 zubewegt, wodurch der über das Stellglied 47'' betätigte mechanische Schlüsselteil 35'' aus dem Gehäuseteil 30'' heraus in seine Arbeitsstellung 15 verfahren wird. Beim Erreichen der Arbeitsstellung 15 fährt die Nase 48'' des Stellgliedes 47'' vor einem Anschlag 49'', der am Ende der Öffnung 44'' angeordnet ist. Ein Sperrmittel 76'', welches in Ausschubrichtung mit einer Auflaufschräge versehen ist, ist bei der Ausschubbewegung hinter den Rasthaken 72'' gefahren, und verhindert nun über das Schubmittel 61 und das Stellglied 47'' ein Wiederhereinfahren des mechanischen Schlüsselteils 35''.

Bei erneuter Betätigung der Auslösetaste 70'' wird das Sperrmittel 76'' wieder freigegeben und es kann das mechanische Schlüsselteil 35'' wieder manuell in den Führungskanal 37'' im Gehäuseteil 30'' hineingeschoben werden. Hierdurch bewegt sich das Schubmittel 61 in reverser Richtung am Zahnrad 65 vorbei, welches hierdurch wieder bewegt wird, so dass die an dem Zahnrad 65 angelenkte und in dem Zahnrad 65 befindliche Spiralfeder 60'' mit der Einschubbewegung des mechanischen Schlüsselteils 35'' wieder gespannt wird. Kurz vor Erreichen der Ruhestellung 11 durch das mechanische Schlüsselteil 35'' fährt das Sperrmittel/Sperrglied 76' mit seiner Auflaufschräge gegen den Rasthaken 72'' und schiebt sich an diesem vorbei. Der Rasthaken 72'' fährt unter der Krafteinwirkung der Feder 77'' wieder hinter das Sperrmittel/Sperrglied 76' und blockiert ein Wiederherausfahren des mechanischen Schlüsselteils 35'' unter der Krafteinwirkung des Druckkraftspeichers/Spiralfeder 60''. Um ein zu weites Einschieben des mechanischen Schlüsselteils 35'' zu vermeiden, ist am hinteren Ende der Öffnung

44'' ein Anschlag 54'' vorgesehen, gegen den die Nase 48'' des Stellgliedes 47'' beim Einschieben des mechanischen Schlüsselteiles 35'' fährt. Gleichzeitig läuft das Sperrmittel 76'' gegen einen Anschlag 56, der am Ende der Wand 42'' liegt.

Neben den hier dargestellten Ausführungsbeispielen sind noch weitere Ausführungsformen denkbar. So sind insbesondere Ausführungsformen denkbar, bei denen die Schlüsselöffnung durch ein weiteres Mittel verschließbar ist, wenn das mechanische Schlüsselteil sich gänzlich im Führungskanal befindet.

Weiterhin ist z.B. eine Ausführungsform denkbar, bei der eine linear wirkende und linear verstellbare Druckfeder direkt auf ein Stellglied, wie z.B. das Stellglied 47 oder 47'' wirkt und derart ein mechanischer Schlüsselteil aus einem Gehäuseteil herausgeschoben werden kann. Eine solche linear wirkende Druckfeder kann z.B. in einem weiteren Führungskanal benachbart zum Führungskanal für das mechanische Schlüsselteil angeordnet sein, oder aber eine derartige Steifigkeit aufweisen, dass eine Führung des Federelementes nicht notwendig ist.

Ebenso könnte das mechanische Schlüsselteil über elektrisch angesteuerte solenoide oder durch hydraulisch wirkende Druckkraftspeicher aus dem Gehäuseteil ausgeschoben werden. Ebenso können anstelle einer Verrastung auch reibschlüssige Bremsmittel vorgesehen sein, die das mechanische Schlüsselteil jeweils in seinen Stellungen hält.

Es versteht sich ebenfalls, dass die Verbindungsmittel zwischen dem elektrischen Gehäuseteil und dem mechanischen Gehäuseteil auch anders als bei dem ersten Ausführungsbeispiel angeordnet sein können. So konnten die Nuten 27 und die Verrastmittelvorsprünge 28 auch in den Gehäusegrundplatten 32, 32', 32'' der die Schlüsselmechanik enthaltenden zweiten Gehäuseteile angeordnet sein. Die Schwalbenschwanzzapfen 23

müssten dann in den Gehäusegrundplatten 22 der, die Elektronik enthaltenden ersten Gehäuseteile angeordnet sein.

Bezugszeichenliste:

10 Schlüssel
11 Ruhestellung
12 Schlüsselöffnung

14 Ebene
15 Arbeitsstellung
16 Ausschieberichtung / Ausfuhrrichtung
17 Demontagerichtung
18 Montagerichtung
19 Öse
20 erstes Gehäuseteil mit Schlüsselelektronik
21 Gehäusedeckel erstes Gehäuseteil
22 Gehäusegrundplatte erstes Gehäuseteil
23 Batteriefachdeckel
24 Batterie
25 Elektronikbauteile
26 Tastfelder
27 Nut in der Gehäusegrundplatte
28 Verrastmittelvorsprung
29 Schraubmittel
30 zweites Gehäuseteil mit Schlüsselmechanik
30′ zweites Gehäuseteil mit Schlüsselmechanik
30′′ zweites Gehäuseteil mit Schlüsselmechanik
31 Gehäusedeckel zweites Gehäuseteil

31' Gehäusedeckel zweites Gehäuseteil
32 Gehäusegrundplatte
32' Gehäusegrundplatte
32'' Gehäusegrundplatte
33 Schwalbenschwanzzapfen
34 Frontteil der Gehäusegrundplatte
35 Schlüsselteil
35' Schlüsselteil
36 Gehäuseinnenraum (zweites Gehäuseteil)
37 Führungskanal
37' Führungskanal
37'' Führungskanal
38 Flächenseite
38' Flächenseite
38'' Flächenseite
39 Flächenseite
39' Flächenseite
40 Flächenwand
40' Flächenwand
40'' Flächenwand
41 Flächenwand
41' Flächenwand
42 Wand
42' Wand
42'' Wand
43 Wand
43' Wand
43'' Wand
44 Längsöffnung
44' Öffnung

44'' Längsöffnung
45 Öffnung
46 Öffnung
46' Öffnung
47 Stellglied
47' Stellglied / Zahnrad
47'' Stellglied
48 Nase
48' Nase
48'' Nase
49 Anschlag (Arbeitsstellung)
49' Anschlag (Arbeitsstellung)
49'' Anschlag (Arbeitsstellung)
50 Zugkraftspeicher
51 Zugmittel
52 Umlenkteil
53 Führungswand
53'' Wandabschnitt
54 Anschlag (Ruhestellung)
54' Anschlag (Ruhestellung)
54'' Anschlag (Ruhestellung)
55 Anschlag für Sperrmittel 76'
56 Anschlag für Sperrmittel 76''
60 Druckkraftspeicher
60'' Druckkraftspeicher
61 Schubmittel
62 Zähne am Stellglied 47'
62'' Zähne am Zahnrad 65
63 Achse
63'' Achse

64 Zahnung am Schlüssel 35' /Schubmittel
65 Zahnrad / Schubmittel
66 Zahnöffnung / Schubmittel 61
67 Kanal
68 Kanal
70 Auslösetaste (Auslösemittel)
70' Auslösetaste (Auslösemittel)
70'' Auslösetaste (Auslösemittel)
71 Hebel
71' Hebel
71'' Hebel
72 Rasthaken von Hebel 71
72' Rasthaken von Hebel 71
72'' Rasthaken von Hebel 71
73 Hebel
74 Rasthaken von Hebel 73
75 Sperrmittel / Aussparung
75'' Sperrmittel
76 Sperrmittel / Aussparung
76' Sperrmittel
76'' Sperrmittel
77 Druckmittel / Feder
77' Druckmittel / Feder
77'' Druckmittel / Feder
77''' Druckmittel / Feder
78 Federsitz
78' Federsitz
78'' Federsitz
78''' Federsitz
79 Ansatzstelle

79‘ Ansatzstelle

79‘‘ Ansatzstelle

79‘‘‘ Ansatzstelle

81 Hebelachse

81‘ Hebelachse

81‘‘ Hebelachse

83 Hebelachse

84 Berührungsstelle

85 Auflaufschräge

Patentansprüche :

1. Schlüssel, insbesondere für Kfz, mit einem Gehäuseteil (30, 30', 30'') und einem daran angeordneten mechanischen Schlüsselteil (35, 35', 35''),

bei dem wenigstens ein schließwirksamer Teil des Schlüsselteils (35, 35', 35'') mittels einer Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) von einer Ruhestellung (11) in eine Arbeitsstellung (15) zu überführen ist, in der der Schlüssel (10) zur mechanischen Betätigung eines Schlosses benutzt werden kann,

wobei zur Aktivierung der Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) ein manuell zu betätigendes Auslösemittel (70) vorgesehen ist,

und das Schlüsselteil (35, 35', 35'') in der Arbeitsstellung (15) im wesentlichen bewegungsstarr ist,

dass das Schlüsselteil (35, 35', 35'') in seiner Ruhestellung (11) in einem Gehäuseinnenraum (36) angeordnet ist,

und dass das Schlüsselteil (35, 35', 35'') nach einer Betätigung des Auslösemittels (70) mittels der Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) von seiner Ruhestellung (11) im Gehäuseinnenraum (36) durch eine laterale Verschiebung aus dem Gehäuseteil (30, 30', 30'') heraus, in die Arbeitsstellung (15) zu überführen ist,

und in dem Gehäuseinnenraum (36) Mittel (37, 40, 41, 42, 43) angeordnet sind, durch die das Schlüsselteil (35, 35', 35'') bei der Längsverschiebung geführt ist,

dadurch gekennzeichnet,

dass die Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) einen Zug- (50) oder Druckkraftspeicher (60) umfasst, der indirekt über ein Zug- (51) oder Schubmittel (61, 64, 65, 66) an dem Stellglied (47) angreift.

2. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass in dem Gehäuseteil (30, 30', 30'') in Ausschubrichtung (16) des Schlüsselteils (35, 35', 35'') eine Schlüsselöffnung (12) angeordnet ist, die formschlüssig zur Außenkontur des Schlüsselteils (35, 35', 35'') ausgebildet ist.

3. Schlüssel nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass der Gehäuseinnenraum (36) des Gehäuseteils (30, 30', 30'') über ein an der Schlüsselöffnung (12) angeordnetes Verschlussmittel von dem, das Gehäuseteil (30, 30', 30'') umgebenden Außenraum abgeschlossen ist.

4. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, daß die Mittel zur Führung des Schlüsselteils (35, 35', 35'') einen Führungskanal (37) umfassen.

5. Schlüssel nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das, den mechanischen Schlüsselteil (35, 35', 35'') und die Mimik (47 - 47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) beherbergende Gehäuseteil (30, 30', 30'') wenigstens zwei, im wesentlichen parallel zueinander verlaufende Flächenseiten (38, 38', 39, 39'') aufweist, und diese Flächenseiten (38, 38', 39, 39'') zu zwei Seiten die Flächenwände (40, 40', 40'', 41, 41') des Führungskanals (37) bilden.

6. Schlüssel nach einem der Ansprüche 1 und 5, dadurch gekennzeichnet, dass im wesentlichen senkrecht zu den Flächenwänden (40, 40′, 40′′, 41, 41′) zwei im wesentlichen parallel verlaufende Wände (42, 42′, 42′′, 43, 43′, 43′′) den Führungskanal (37) seitlich begrenzen.

7. Schlüssel nach einem der Ansprüche 1 und 6, dadurch gekennzeichnet, dass wenigstens eine Wand (42, 42′, 42′′, 43, 43′, 43′′) des Führungskanals eine Öffnung (44, 44', 44'') aufweist durch den ein, auf das mechanische Schlüsselteil (35, 35′, 35'') einwirkendes Stellglied (47, 47', 47'') der Mimik die Wand (42, 42′, 42′′, 43, 43′, 43′′) durchgreift.

8. Schlüssel nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Öffnung (44, 44'') im wesentlichen linear und parallel zur Ausschiebrichtung (16) des mechanischen Schlüsselteils (35, 35′, 35'') verläuft.

9. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass ein Endanschlag (49, 49'') vorgesehen ist, gegen den eine am Schlüsselteil (35, 35′, 35'') angeordnete Nase (48, 48', 48'') zur Begrenzung des Ausschubwegs aufläuft.

10. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der mechanische Schlüsselteil (35, 35′, 35'') durch Rastmittel (71 - 71′′, 72 - 72′′, 73, 74, 75, 76-76′′) in seiner Ruhe- (11) und in seiner Arbeitsstellung (15) bewegungsstarr gehalten ist.

11. Schlüssel nach einem der Ansprüche 1 und 10, dadurch gekennzeichnet, dass die Rastmittel (71 - 71′′, 72 - 72′′, 73, 74, 75, 76-76′′) durch Betätigung des Auslösemittels (70 - 70′′) freigegeben werden.

12. Schlüssel nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Rastmittel wenigstens einen Hebel (71 - 71'', 73) mit mit wenigstens einem Rasthaken (72 - 72'', 74) umfassen, der in der Arbeits- (15) und/oder Ruhestellung (11) jeweils auf ein Sperrmittel (75 - 75'', 76, 76') einwirkt.

13. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der Zugkraftspeicher (50) über ein Zugmittel (51) an dem Stellglied (47) angreift, wobei der Zugweg des Zugmittels (51) und des Zugkraftspeichers (50) durch Umlenkung des Zugmittels (51) an einem Umlenkteil (52), insbesondere einer Umlenkrolle, vergrößert ist.

14. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der Druckkraftspeicher (60) über Schubmittel (61, 64, 65, 66) an dem Stellglied (47'') angreift.

15. Schlüssel, nach Anspruch 1, dadurch gekennzeichnet, dass zwei in sich abgeschlossene Gehäuseteile (20, 30; 20', 30'; 20'', 30'') aneinander angeordnet sind, wobei das erste Gehäuseteil (20, 20', 20'') eine Schlüsselelektronik (25, 24), und das zweite Gehäuseteil (30; 30'; 30'') einen mechanischen Schlüsselteil (35, 35', 35'') und eine Mimik (47 - 47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) beinhaltet, und bei dem die beiden Gehäuseteile (20, 30; 20', 30', 20'', 30'') entlang einer einzelnen, im wesentlichen planaren Ebene (14) reversibel aneinander festgelegt sind.

16. Schlüssel nach Anspruch 15, dadurch gekennzeichnet, dass im Bereich der planaren Ebene (14) Verbindungsmittel (28, 30) an den Gehäuseteilen 20, 30; 20', 30'; 20'', 30'') angeordnet sind, mittels derer die Gehäuseteile (20, 30; 20', 30'; 20'', 30'') reversibel aneinander festgelegt sind.

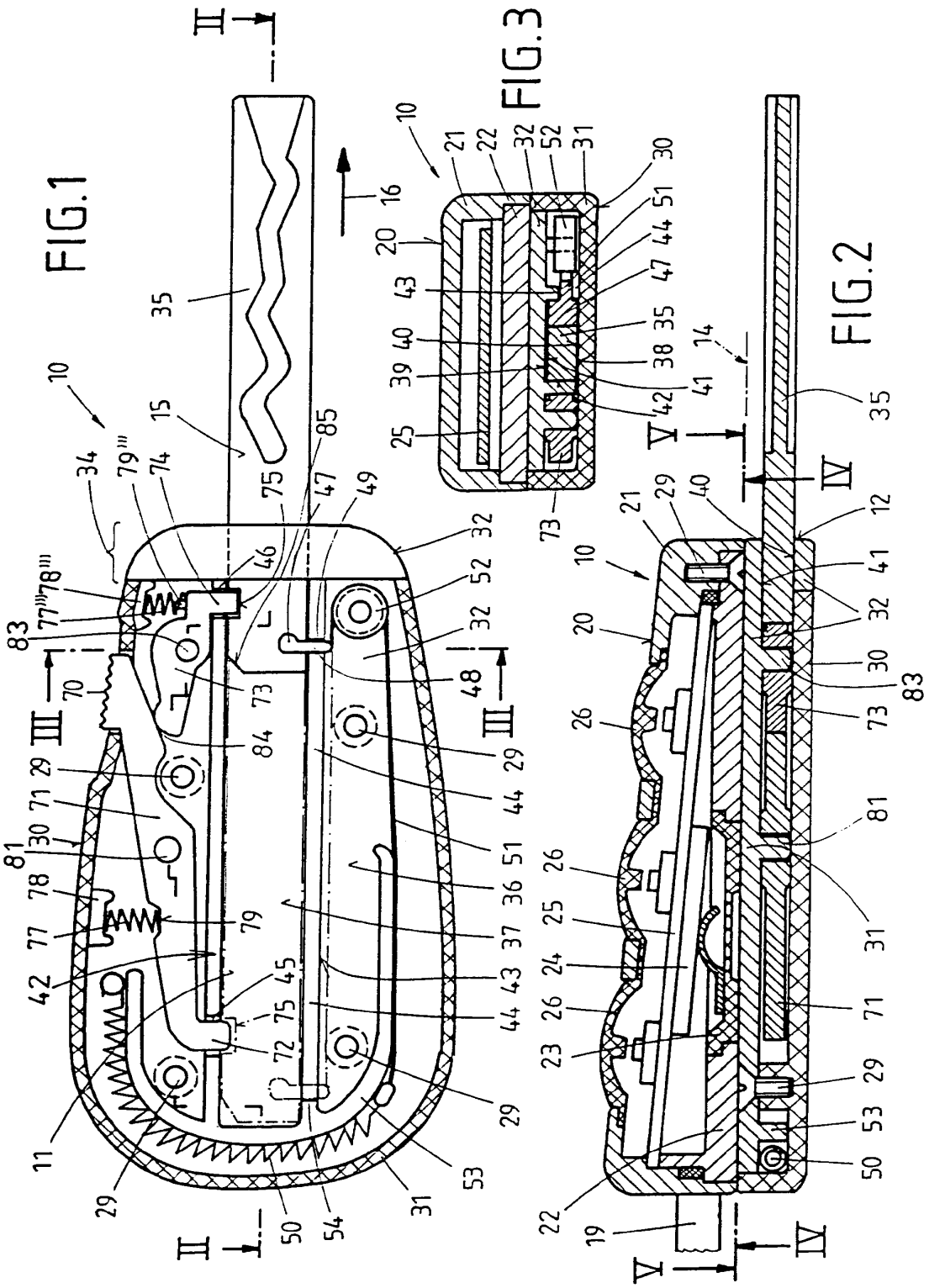


FIG.1
FIG.2
FIG.3
II
III
IV
V

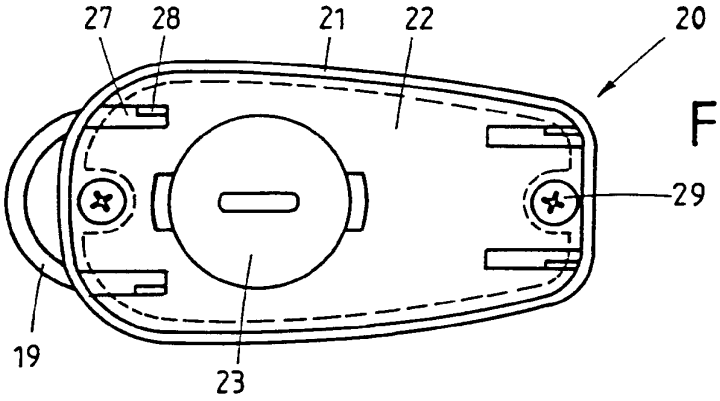


FIG.4

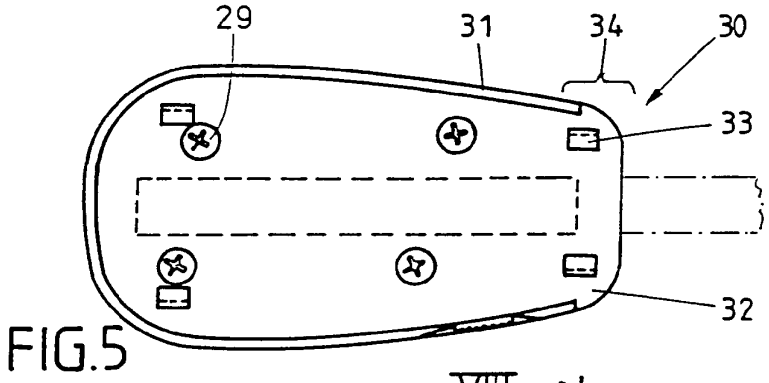


FIG.5

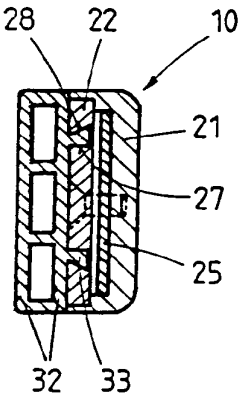


FIG.8

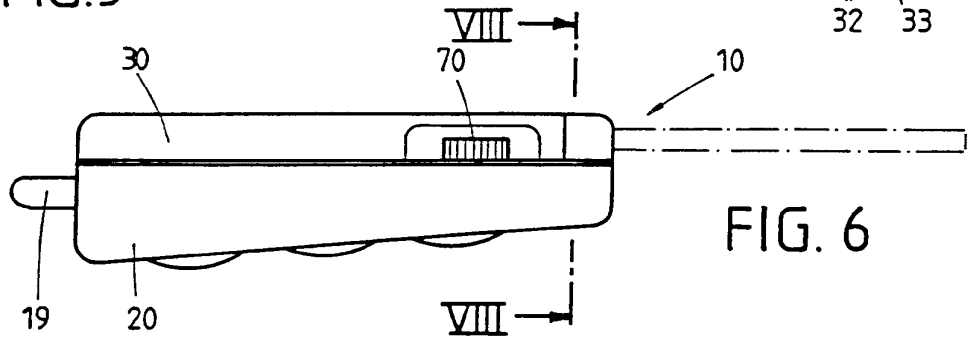


FIG. 6

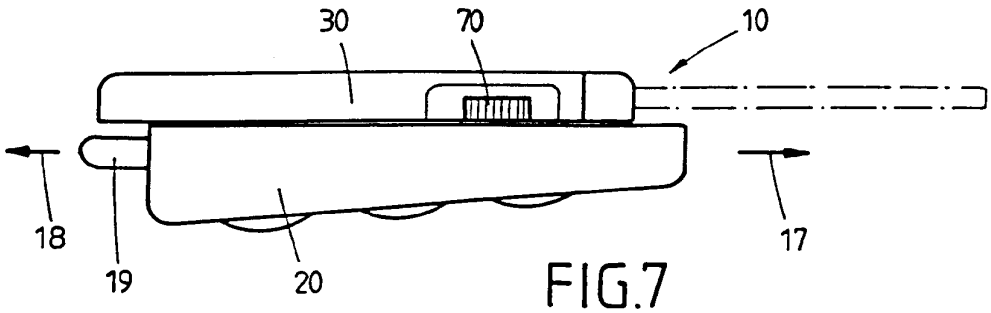


FIG.7

FIG.9

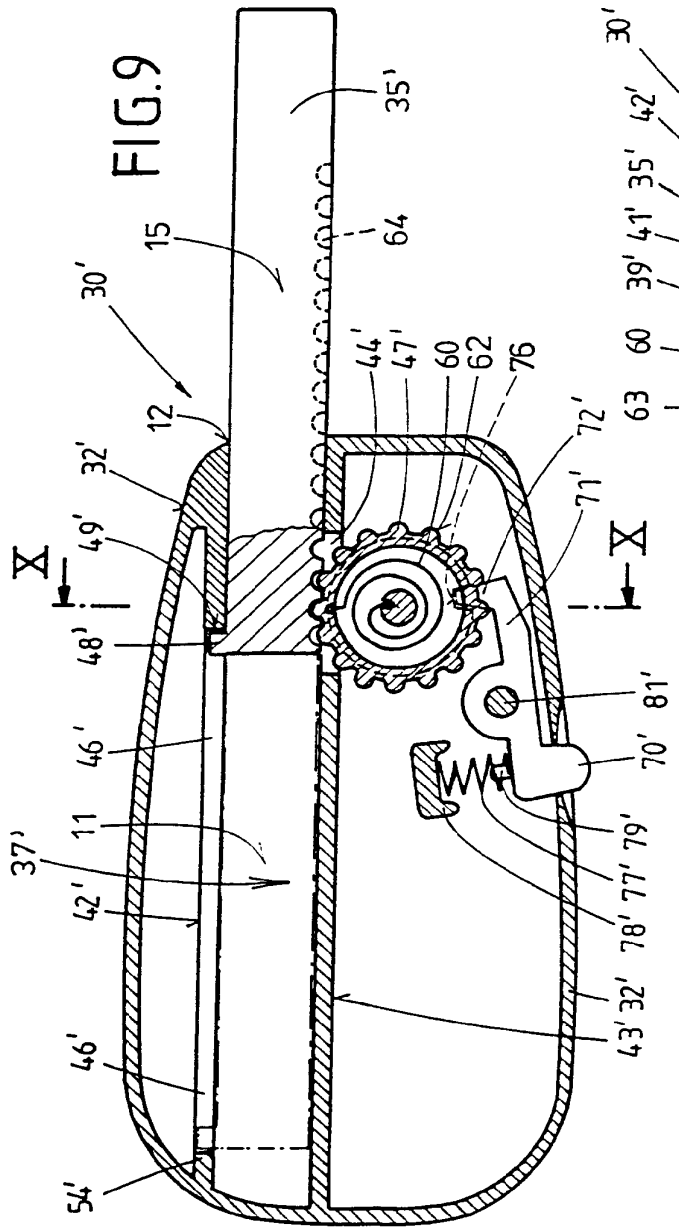
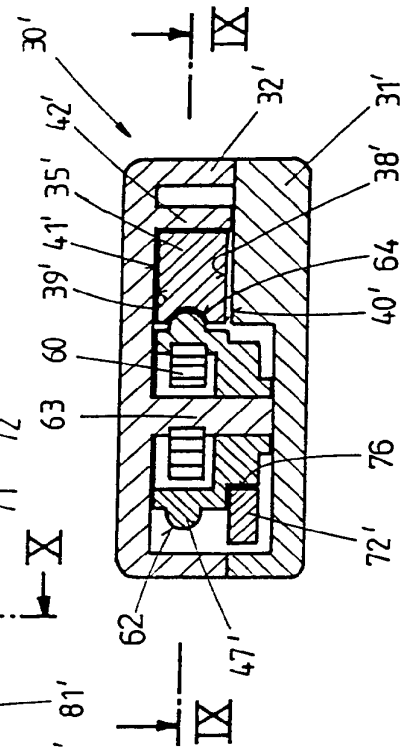

35'
15
64
30'
12
32'
49'
48'
46'
11
37'
42'
46'
54'
44'
47'
60
62
76
72'
71'
81'
70'
79'
77'
78'
43'
32'
X
X

FIG.10


30'
42'
35'
41'
39'
60
63
62
47'
32'
31'
38'
64
40'
76
72'
IX
IX

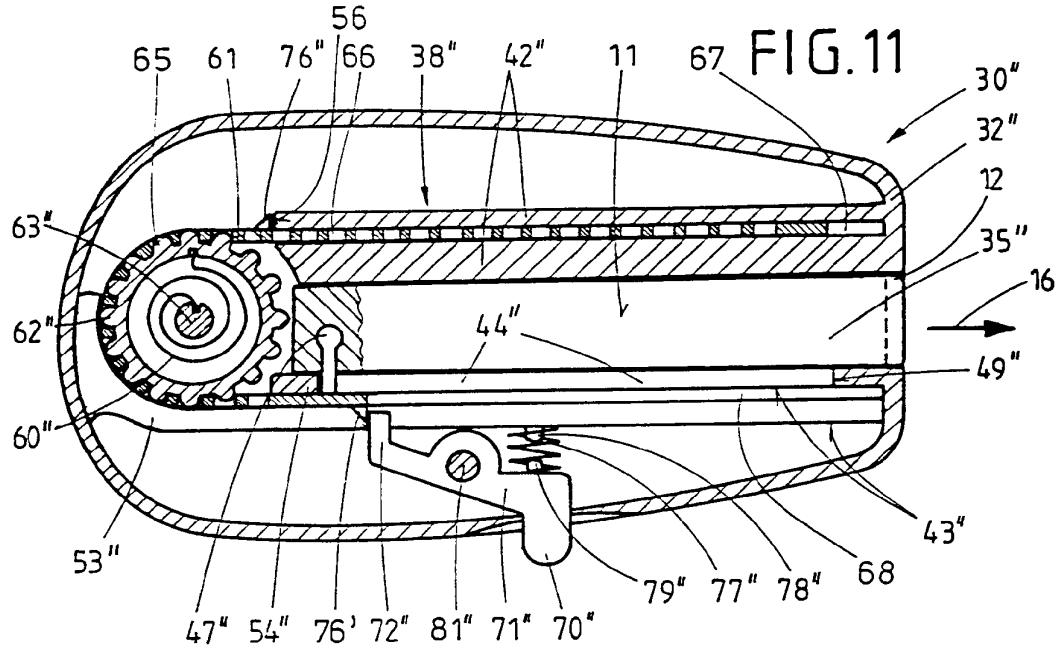

56
65
61
76"
66
38"
42"
11
67
30"
32"
12
35"
16
63"
62"
44"
49"
60"
43"
53"
79"
77"
78"
68
47"
54"
76'
72"
81"
71"
70"

FIG.11

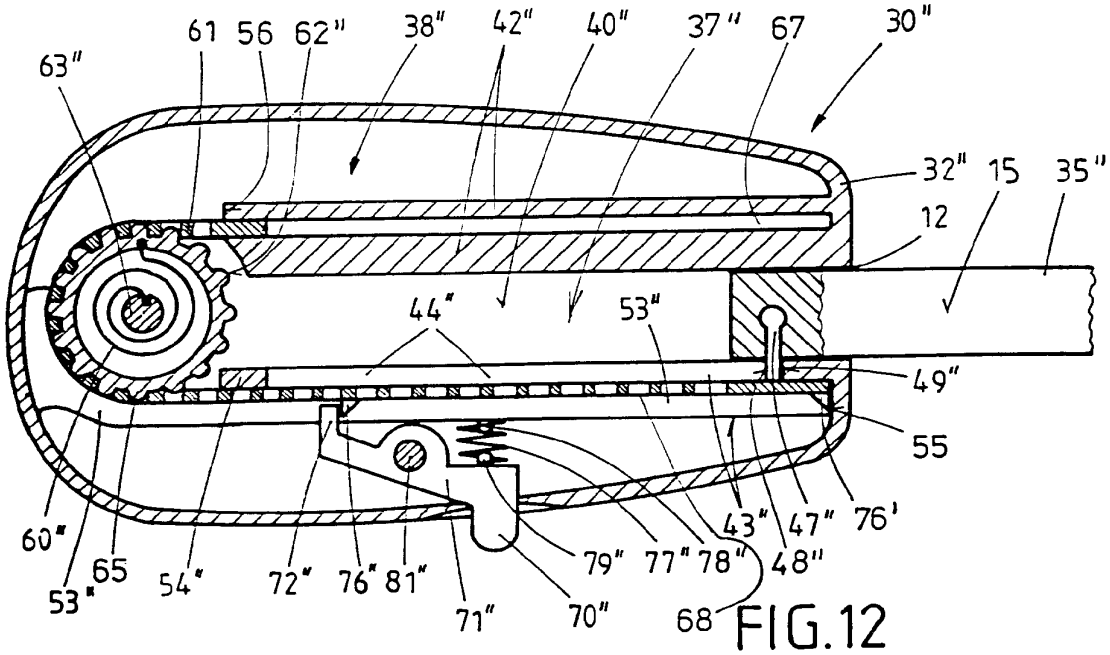

61
56
62"
38"
42"
40"
37"
67
30"
63"
32"
15
35"
12
44"
53"
49"
55
60"
65
54"
72"
76"
81"
79"
77"
78"
48"
43"
47"
76'
53"
71"
70"
68

FIG.12

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/EP 00/11504

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B19/04 A45C11/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 A45C E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	DE 199 12 749 C (VALEO GMBH & CO SCHLIESSYST KG) 2 November 2000 (2000-11-02) column 3, line 35 - line 59; figure	1-5, 7-12, 14-16
X	US 2 690 666 A (MORRIS ENGEL ET AL.) 5 October 1954 (1954-10-05) cited in the application column 4, line 7 - line 51; figure	1,2,4-6, 9-12
X	US 3 328 986 A (THEODORE RALTON) 4 July 1967 (1967-07-04) column 2, line 35 - line 62; figure	1,2,4-6, 9-11,14
A	FR 2 597 537 A (PEUGEOT) 23 October 1987 (1987-10-23) page 3, line 4 - line 24; figures 1,3,4	15

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April 2001	20/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pieracci, A

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr. nal Application No
PCT/EP 00/11504

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19912749 C	02-11-2000	NONE	
US 2690666 A	05-10-1954	NONE	
US 3328986 A	04-07-1967	NONE	
FR 2597537 A	23-10-1987	NONE	

INTERNATIONALER RECHERCHENBERICHT

Intern. nales Aktenzeichen
PCT/EP 00/11504

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B19/04 A45C11/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 A45C E05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	DE 199 12 749 C (VALEO GMBH & CO SCHLIESSYST KG) 2. November 2000 (2000-11-02) Spalte 3, Zeile 35 - Zeile 59; Abbildung	1-5, 7-12, 14-16
X	US 2 690 666 A (MORRIS ENGEL ET AL.) 5. Oktober 1954 (1954-10-05) in der Anmeldung erwähnt Spalte 4, Zeile 7 - Zeile 51; Abbildung	1,2,4-6, 9-12
X	US 3 328 986 A (THEODORE RALTON) 4. Juli 1967 (1967-07-04) Spalte 2, Zeile 35 - Zeile 62; Abbildung	1,2,4-6, 9-11,14
A	FR 2 597 537 A (PEUGEOT) 23. Oktober 1987 (1987-10-23) Seite 3, Zeile 4 - Zeile 24; Abbildungen 1,3,4	15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. April 2001	20/04/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pieracci, A

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internales Aktenzeichen
PCT/EP 00/11504

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19912749	C	02-11-2000	KEINE	
US 2690666	A	05-10-1954	KEINE	
US 3328986	A	04-07-1967	KEINE	
FR 2597537	A	23-10-1987	KEINE	

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 May 2001 (31.05.2001)

PCT

(10) International Publication Number
WO 01/39102 A1

(51) International Patent Classification[7]: G06K 7/00

(21) International Application Number: PCT/IT00/00429

(22) International Filing Date: 25 October 2000 (25.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
TO99A001020 22 November 1999 (22.11.1999) IT

(71) Applicant *(for all designated States except US)*: **EUTRON INFOSECURITY S.R.L.** [IT/IT]; Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CASSIA, Lucio** [IT/IT]; c/o Eutron Infosecurity S.R.L., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT). **LEIDI, Michele** [IT/IT]; c/o Eutron Infosecurity S.R.L., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(74) Agent: **GARAVELLI, Paolo**; c/o A.Bre.Mar. S.r.l., Via Servais, 27, I-10146 Torino (IT).

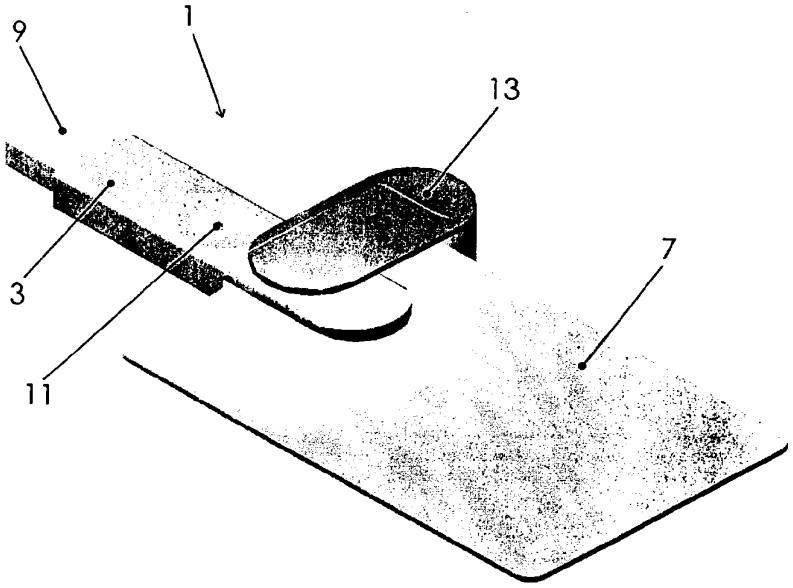
(81) Designated States *(national)*: AE, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, YU, ZA.

(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, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

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.

(54) Title: PORTABLE READER FOR SMART CARDS



(57) Abstract: A portable reader (1) for smart cards (7) is described that comprises: a support body (3) containing at least one slot (5) for inserting and reading a smart card (7); interface means (9) connected to the support body (3); interface means (9) connected to the support body (3); means (13) for keeping and aligning the smart card (7); and a managing microprocessor contained inside the support body (3) and connected to the interface means (9) and the reading means for smart cards (7).

WO 01/39102 A1

PORTABLE READER FOR SMART CARDS

The present invention refers to a portable reader for intelligent cards of the type commonly known as "smart cards".

Smart cards are nowadays rather widespreaded given their practical easiness of use: in fact, they allow, through microprocessors realised on integrated circuit chips obtained therein, to store a very high amount of data and therefore they can be used in applications such as different types of credit cards, cryptographic cards and future applications such as identity cards or electronic health cards.

For the purpose for which they are provided, such smart cards are adapted to communicate (that is, to transmit and receive) data through communication standards that are well-known at world level, such as the 7816 Standard. To realise such communication, the intelligent card is put in contact with a card reading device, which is equipped with suitable slots in which the card is

inserted, such slots containing a certain number of contacts that read the card data and communicate them to the microprocessor managing the card reader. Card readers are currently available on the market that are realised in the shape of boxes whose sizes are about 15 x 10 cm, that are statically connected to different types of data processing and transmitting systems. Such smart card readers are therefore with a relatively high encumbrance and due to their nature they are provided fixed in well-defined positions. On the market, there are currently no smart card readers that are portable and with small sizes.

Object of the present invention is solving the above prior-art problems, by providing a portable reader for smart cards that is of very reduced sizes and therefore can be easily transported and used by end users for any type of application.

A further object of the present invention is providing a portable reader that is equipped with such interface means as to allow it to widely and immediately use all smart cards with which a user can be equipped: for such purpose, the reader is equipped with means allowing it to be connected to a common Universal Serial Bus (USB) port of a

computer.

The above and other objects and advantages of the invention, as will appear from the following description, are obtained by a portable reader for smart cards as claimed in Claim 1. Preferred embodiments and non-trivial variations of the present invention are claimed in the dependent Claims.

The present invention will be better described by some preferred embodiments thereof, given as a non-limiting example, with reference to the enclosed drawings, in which:

- Figure 1 is a perspective view of an embodiment of a portable reader according to the present invention coupled with a smart card in the operating position;
- Figure 2 is a perspective view of the reader in Fig. 1 in the transport position;
- Figure 3 is a top view of the operating configuration in Fig. 1; and
- Figure 4 is a top view of the reader in Fig. 2.

With reference to the Figures, a preferred embodiment of the portable reader 1 for intelligent cards is shown, such cards being commonly known as

"smart cards".

The portable reader 1 for smart cards of the present invention substantially comprises a support body 3 shaped as an elongated box, comprising at one end thereof at least one slot 5 for inserting and reading therein a smart card 7. For such purpose, the slot 5 is equipped with reading means (not shown) for smart cards 7, that are commonly known and are composed of a plurality (usually six) of contacts that carry connection wires to a managing microprocessor (also not shown) contained inside the support body 3.

Such managing microprocessor is preferably realised through an integrated circuit chip and contains inside it all the necessary logics for receiving and transmitting data to the smart card 7 to which it is connected.

In order to communicate with the outside world the data obtained from a connected smart card 7, the portable reader 1 of the invention is further equipped with interface means 9 connected to the support body 3 and to the managing microprocessor; commonly, such interface means 9 are adapted to be connected to a common USB port of a computer, in order to be able to realise a connection with the

most widely known external managing networks (Internet, Intranet, etc.).

Moreover, the portable reader 1 of the invention comprises means 13 for keeping and aligning the smard card 7, that, in the practical embodiment shown, are composed of a bracket shaped as an elongated C and hinged to the support body 3 in order to have:

a) an operating position in which the keeping and aligning means 13 are perpendicular to the support body 3 to keep the card 7 in contact with the reader 1 and to align the card 7 with the reading means (as can be clearly shown in Fig.s 1 and 3; and

b) a rest position in which the keeping and aligning means 13 are aligned with the support body 3 allowing to transport and store the reader 1 (as can be clearly seen in Fig.s 2 and 4).

Finally, the portable reader 1 of the invention can be further equipped with means 11 that enable grasping the support body 3 by means of two fingers of an hand, such as for example the depression 11 shown in the different Figures.

A portable reader 1 has thereby been realised

that can be placed and stored in any suitable place and that can be easily transported and connected to USB ports: in this way, by arranging a reader whose overall sizes are on the order of 3 cm, it is possible to realise a flexible solution wherein each smart card with which a user is equipped can be immediately and easily connected and activated for the outside world to perform flexible and powerful applications.

Some preferred embodiments of the invention have been disclosed, but obviously they are subjected to further modifications and variations within the same inventive idea. For example, the reader 1 of the invention can be realised on a personal identification device like the one marketed by the Assignee of the present invention, containing in a single configuration the functionalities of personal identification, encrypted data transmission and smart cards reading. Otherwise, the reader 1 of the present invention can be pre-arranged in a stand-alone configuration according to application needs, guaranteeing at any rate an efficient solution as regards the practical comfort of the shape and portability of the reader 1 itself.

CLAIMS

1. Portable reader (1) for smart cards (7), characterised in that it comprises:
   - a support body (3) containing at least one slot (5) for inserting and reading a smart card (7), said slot (5) being equipped with reading means for smart cards (7);
   - interface means (9) connected to said support body (3);
   - means (13) for keeping and aligning said smart card (7); and
   - a managing microprocessor contained inside said support body (3) and connected to said interface means (9) and said reading means for smart cards (7).
2. Portable reader (1) according to Claim 1, characterised in that said interface means (9) are adapted to be connected to an USB port.
3. Portable reader (1) according to Claim 1, characterised in that said reading means for smart cards (7) are composed of a plurality of contacts carrying connection wires to said managing microprocessor.
4. Portable reader (1) according to Claim 3,

characterised in that said contacts are equal to six.

5. Portable reader (1) according to Claim 1, characterised in that said keeping and aligning means (13) are composed of an elongated-C-shaped bracket, said bracket being hinged to said support body (3) in order to have:

   a. an operating position in which said keeping and aligning means (13) are perpendicular to said support body (3) to keep the card (7) in contact with said reader (1) and to align the card (7) with said reading means; and

   b. a rest position in which said keeping and aligning means (13) are aligned with said support body (3) allowing to transport and store said reader (1).

6. Portable reader (1) according to Claim 1, characterised in that it is further equipped with means (11) that enable grasping said support body (3) by means of two fingers of an hand.

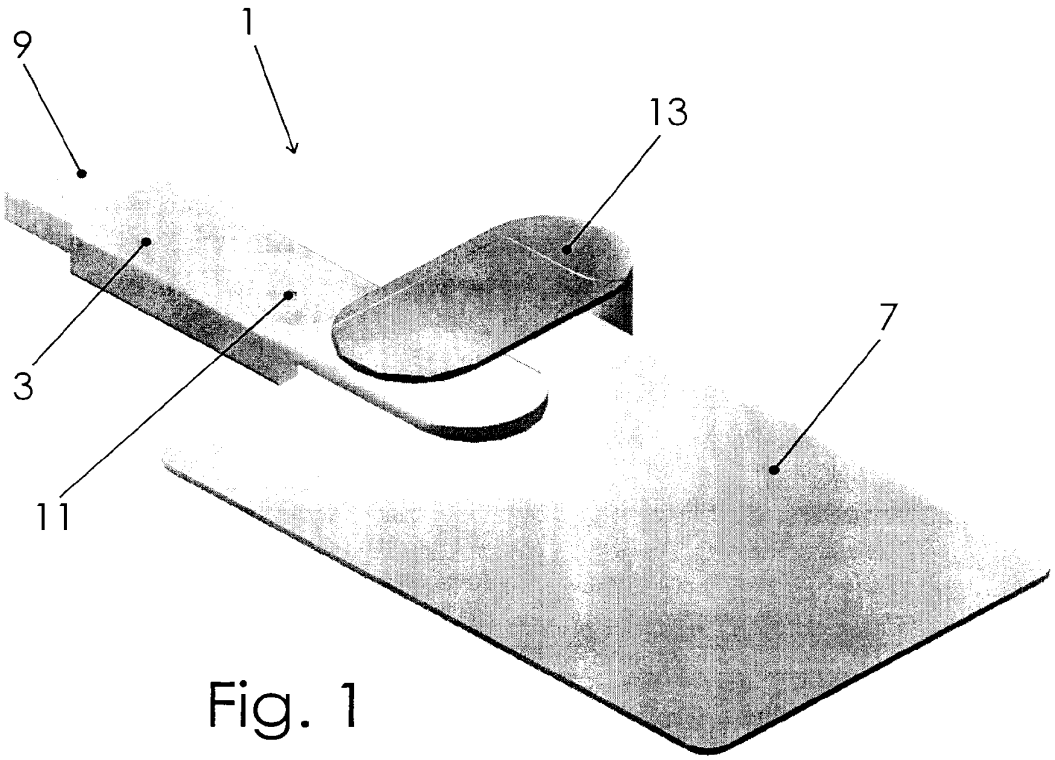


Fig. 1

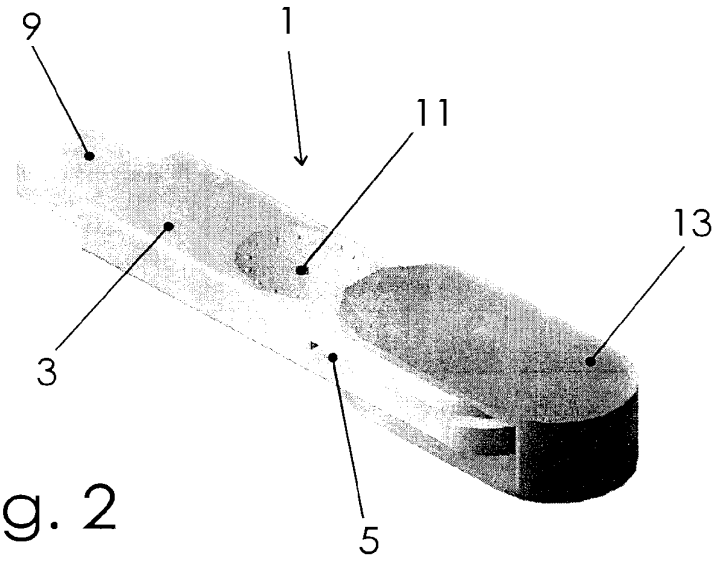


Fig. 2

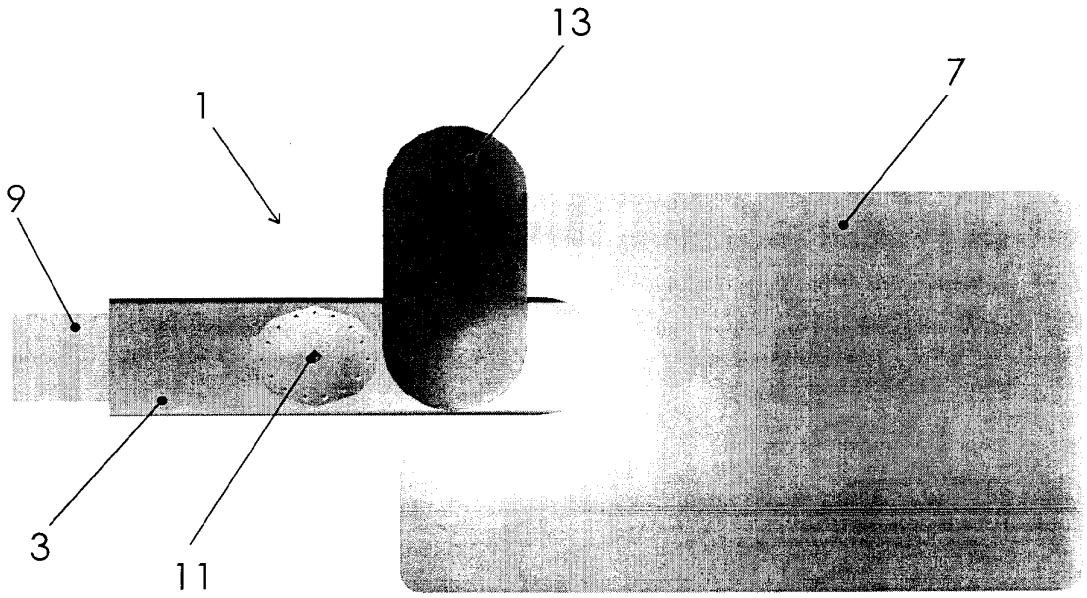


Fig. 3

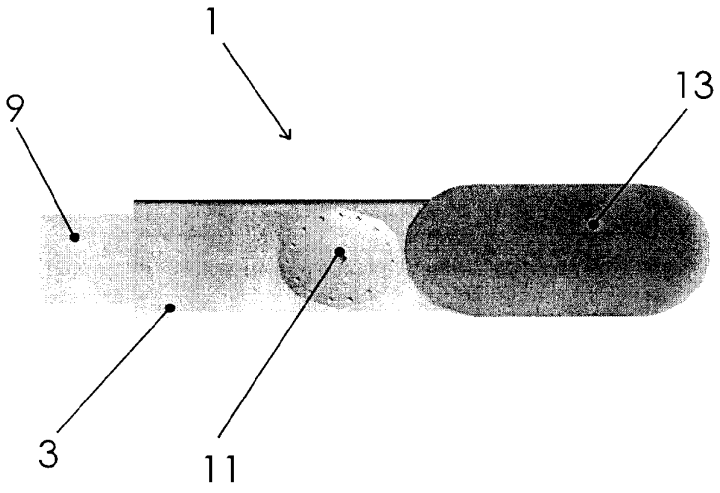


Fig. 4

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/IT 00/00429

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 07448 A (SIRBU CORNEL) 27 February 1997 (1997-02-27) page 9, line 14 -page 11, line 5 figures 1,7	1-4,6
X	US 5 778 071 A (AMORUSO VICTOR P ET AL) 7 July 1998 (1998-07-07) column 2, line 24 - line 47 column 3, line 6 - line 8 column 6, line 62 -column 7, line 20 figure 1C	1,3,4,6
X	US 5 844 497 A (GRAY ROBERT J) 1 December 1998 (1998-12-01) column 3, line 36 -column 5, line 48 figures 1,2	1,3,4,6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 January 2001	06/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Rydman, J

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/IT 00/00429

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 635 701 A (GLOTON JEAN-PIERRE) 3 June 1997 (1997-06-03) column 2, line 57 -column 3, line 13 figures 1,2	1
A	FR 2 774 194 A (SCM SCHNEIDER MICROSYSTEME MIC) 30 July 1999 (1999-07-30) page 2, line 23 -page 3, line 30 figures 5,7	1

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No
PCT/IT 00/00429

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9707448 A	27-02-1997	FR 2738070 A	28-02-1997
		FR 2740885 A	09-05-1997
		AU 720839 B	15-06-2000
		AU 6824096 A	12-03-1997
		BG 102336 A	30-12-1998
		BR 9610236 A	15-06-1999
		CN 1194043 A	23-09-1998
		CZ 9800408 A	16-12-1998
		EP 0870222 A	14-10-1998
		HU 9900499 A	28-06-1999
		JP 11511278 T	28-09-1999
		NO 980728 A	20-04-1998
		PL 325164 A	06-07-1998
		SK 22098 A	07-10-1998
		US 6070796 A	06-06-2000
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 726397 B	09-11-2000
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
US 5844497 A	01-12-1998	US 6087955 A	11-07-2000
US 5635701 A	03-06-1997	FR 2716988 A	08-09-1995
		DE 69518678 D	12-10-2000
		EP 0670556 A	06-09-1995
		JP 7271888 A	20-10-1995
FR 2774194 A	30-07-1999	EP 1050006 A	08-11-2000
		WO 9938104 A	29-07-1999

Form PCT/ISA/210 (patent family annex) (July 1992)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
5. Juli 2001 (05.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/48339 A1

(51) Internationale Patentklassifikation[7]: E05B 19/04, 49/00

(21) Internationales Aktenzeichen: PCT/EP00/11619

(22) Internationales Anmeldedatum:
22. November 2000 (22.11.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 62 975.7 24. Dezember 1999 (24.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **JACOB, Dirk** [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE). **MÜLLER, Ulrich** [DE/DE]; Schneegelskothen 7c, 42549 Velbert (DE). **PLATE, Jeffrey, D.** [US/US]; 9395 North 49th Street, Apt. 201, Brown Deer, WI 53223 (US).

(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

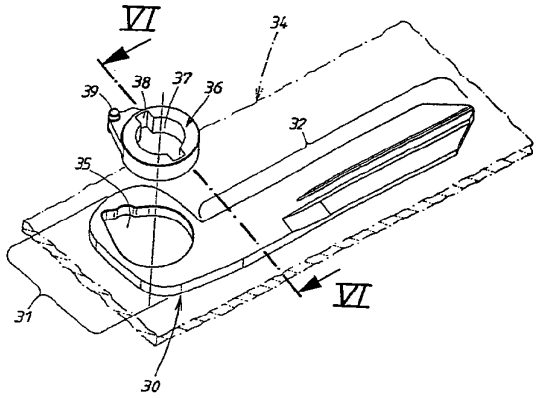
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

[Fortsetzung auf der nächsten Seite]

(54) Title: COMBINED MECHANICAL AND ELECTRONIC KEY, IN PARTICULAR FOR THE LOCKS OF MOTOR VEHICLES

(54) Bezeichnung: KOMBINIERTER MECHANISCHER UND ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR AN FAHRZEUGEN BEFINDLICHE SCHLÖSSER



(57) Abstract: The invention relates to a combined mechanical and electronic key comprising a key housing for electronic components and an L-shaped flat key (30). Said flat key consists of a bearing limb (31) which enables the key to pivot into a storage position and a shank (32) which mechanically operates the lock. The shank (32) of the flat key (30) can be displaced between an inoperative position, retracted into the key housing and an operative position, in which it projects out of the housing. A push-button preferably also acts as the pivoting axis for the flat key (30). The push-button and the housing have profiled sections and the bearing limb has co-operating profiled sections (37, 38, 39), to subject the flat key (30) to a force in the operative position and to lock the key in one of its positions. The invention aims to produce a simple, cost-effective key. To this end, the flat key is configured as a planar plate (34) with an L-shaped outline, the shank (32) sharing the same plane as the bearing limb. The bearing limb (31) has an opening (35) in the plate for receiving, in a rotationally fixed manner, an insert (36) that has the co-operating profiled section (37 to 39).

[Fortsetzung auf der nächsten Seite]

WO 01/48339 A1

— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Bei einem kombinierten mechanischen und elektronischen Schlüssel gibt es sowohl einen Schlüsselbehälter für elektronische Bauteile als auch einen L-förmigen Flachschlüssel (30), der einen zu seiner Schwenklagerung dienenden Lagerschenkel (31) und einen zur mechanischen Betätigung des Schlosses dienenden Schaftschenkel (32) besitzt. Der Flachschlüssel (30) ist mit seinem Schaftschenkel (32) zwischen einer in den Schlüsselbehälter eingeschwenkten Ruhelage und einer herausgeschwenkten Gebrauchslage bewegbar. Ein Druckknopf dient vorzugsweise zugleich als Schwenkachse für den Flachschlüssel (30). Der Druckknopf und der Behälter besitzen Profile und der Lagerschenkel Gegenprofile (37, 38, 39), um den Flachschlüssel (30) in seine Gebrauchslage kraftzubelasten und in einer seiner Lagen zu arretieren. Für eine einfachere und kostengünstigere Herstellung wird vorgeschlagen, den Flachschlüssel als ebene Platte (34) mit L-förmigem Umrissprofil auszubilden, wo der Schaftschenkel (32) in der gleichen Ebene wie der Lagerschenkel angeordnet ist. Dabei besitzt der Lagerschenkel (31) einen Plattendurchbruch (35), der zur drehfesten Aufnahme eines das Gegenprofil (37 bis 39) aufweisenden Einsatzes (36) dient.

Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für an Fahrzeugen befindliche Schlösser

Die Erfindung richtet sich auf einen kombinierten Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Ein solcher Schlüssel erlaubt sowohl eine unmittelbare mechanische Betätigung der Schlösser als auch, alternativ oder ergänzend, eine elektronische Betätigung, z.B. eine Fernbedienung dieses Schlosses bzw. auch anderer Schlösser. Der Schlüsselbehälter ist das Handhabungsmittel sowohl zur mechanischen als auch elektrischen Schlüsselbetätigung. Für die elektronische Betätigung besitzt daher der Schlüsselbehälter an seiner Außenseite Betätigungsstellen, z.B. in Form von elektrischen Druckknöpfen oder nachgiebigen Membranen, die auf im Behälterinneren angeordnete elektrische Schalter od. dgl. einwirken. Der mechanische Flachschlüssel ist L-förmig gestaltet und mit seinem einen L-Schenkel am Vorderende des Behälters schwenkbar gelagert, weshalb der „Lagerschenkel" genannt werden soll. In der Ruhelage befindet sich der Flachschlüssel mit seinem anderen, den Schlüsselschaft bildenden L-Schenkel in einer Einschwenkposition im Behälter. Dieser L-Schenkel soll nachfolgend „Schaftschenkel" bezeichnet werden. Der Flachschlüssel lässt sich mit seinem Schaftschenkel in eine Gebrauchslage herauschwenken. Zur Lagesicherung empfiehlt es sich den Flachschlüssel in beiden Lagen im Schlüsselbehälter zu arretieren.

Bei dem bekannten Schlüssel der im Oberbegriff von Anspruch 1 genannten Art (EP 0 267 429) ist der L-förmige Flachschlüssel mit seinen Schenkeln zweiteilig

ausgebildet; er besitzt ein Kopfstück in Form eines Lagerrings mit einem tangentialen Ansatz, in welchen das Ende einer Klinge einsteckbar und darin lösbar befestigt ist. Das eingesteckte Kupplungsstück der Klinge muss durch eine Schraube oder einen Niet in der Einstecklage gesichert werden, was mühsam und zeitaufwendig ist. Der den Schaftschenkel bildende L-Schenkel des bekannten Flachschlüssels umfasst den Lagerring, den Ansatz und die eingesteckte Klinge. Der Schaftschenkel ist also zweistückig ausgebildet. Der Übergangsbereich zwischen der eingesteckten Klinge und dem Ansatz am Lagerring ist bruchgefährdet. Um einen Bruch auszuschließen muss das den Aufnahmeschlitz für die Klinge umschließende Material im Ansatz des Lagerrings möglichst dick ausgebildet werden, was der Zielsetzung eines raumsparenden Schlüssels entgegenläuft.

Bei einem bekannten Schlüssel (DE 39 02 537 C2) ist im Schwenkachsenbereich des Flachschlüssels ein mechanischer Druckknopf angeordnet, der axial und radial gefedert ist. Der Druckknopf dient als Schwenkachse für den Flachschlüssel. Die doppelte Federung des Druckknopfes hat zwei Aufgaben beim Flachschlüssel zu erfüllen. Die eine Aufgabe besteht darin, den Flachschlüssel in Schwenkrichtung aus seiner Ruhelage in Richtung seiner Gebrauchslage federzubelasten. Die andere Aufgabe liegt darin, möglichst beide Schwenklagen des Flachschlüssels zu arretieren. Dafür benötigt der Druckknopf geeignete Profilierungen und der Flachschlüssel geeignete Gegenprofilierungen. Zwar ist der Flachschlüssel L-förmig ausgebildet, doch muss der Lagerschenkel wegen der Gegenprofile eine beachtliche Bauhöhe aufweisen und wird gesondert als Lagerkörper mit Vierkantprofil vorgefertigt. Um die große Bauhöhe des Lagerkörpers zu nutzen, ordnete man den Schaftschenkel in einer Parallelebene zur Schwenkachse des Flachschlüssels an. Das erfordert eine entsprechend große Höhendimension im Schlüsselbehälter. Der zur Lagerung des mechanischen Druckknopfs dienende Lagerkörper des Flachschlüssels besitzt einen Schlitz zur nachträglichen Anbringung des für sich gefertigten Schlüsselschafts. Der Schlüsselschaft wird in den Schlitz des Lagerkörpers eingesteckt und dort durch einen Stift od. dgl. gesichert. Das ist zeit- und kostenaufwendig.

Es gibt kombinierte Schlüssel (DE 22 26 385 A; DE 38 42 790 C1), die zwar einen flachen L-förmigen Flachschlüssel aufweisen, doch ist ein Druckknopf im

Achsbereich nicht vorgesehen. Die Schwenkachse erzeugt ein unbeweglicher Lagerstift. Weil kein Gegenprofil für einen Druckknopf erforderlich ist, kann der zur Schwenklagerung dienende eine Lagerschenkel des Flachprofils flach ausgebildet sein. Man bildet den Flachschlüssel als eine ebene Platte aus, in welcher auch das Flachprofil des Schaftschenkels liegt. Dieses Schlüsselgehäuse kann zwar flacher gebaut werden, doch gibt es keine Federbelastung, um den Schaftschenkel aus einer in dem Schlüsselbehälter abgesenkten Ruhelage in seine herausgeschwenkte Gebrauchslage zu überführen. Dies erfordert eine mühsame Handhabung. Außerdem gibt es keine raumsparende Möglichkeit, um den Flachschlüssel in diesen Lagen im Behälter zu arretieren. Diese nicht festlegbare Schwenkposition des Flachschlüssels bringt Probleme sowohl beim Tragen in der Hosentasche als auch beim Gebrauch, z.B. während der Drehbetätigung des Schlüsselgehäuses.

Bei Schraubverbindungen an Blechprofilen ist es bekannt, zum Erreichen der nötigen Einschraublänge für die Schraube das Mutterngewinde im Blechprofil durch ein Ansatzstück oder ein eingenietetes Einsatzstück zu vergrößern (U. Richter, R. v. Voss, F. Kozer: Bauelemente der Feinmechanik, Berlin: Verlag Technik, 1954, S. 137). Diese Ausbildung von Mutterngewinden in Blechprofilen steht mit Flachschlüsseln in keinem Zusammenhang. Diese Druckschrift gibt keine Anregungen für den Aufbau eines L-förmigen Flachschlüssels.

Der Erfindung liegt die Aufgabe zugrunde, einen zuverlässigen, raumsparenden Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, der sich einfacherer und kostengünstiger herstellen lässt. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Bei der Erfindung wird zunächst der Schlüssel mit seinen beiden L-Schenkeln einstückig in Form einer ebenen Platte ausgebildet. Man kann den L-förmigen Flachschlüssel aus Plattenmaterial ausstanzen. Durch die einstückige Ausbildung liegt ein stabiler bruchfester Übergang zwischen dem Lagerschenkel und dem Schaftschenkel vor. Trotz der flachen Ausbildung dieses L-förmigen Schlüssels kann im Bereich seines Lagerschenkels der mechanische Druckknopf im Schlüsselbehälter

eingesetzt werden. Dies ist deswegen möglich, weil die für den Druckknopf an sich erforderlichen Gegenprofile einem Einsatz überlassen werden, der in einem Plattendurchbruch des Lagerschenkels drehfest aufgenommen wird. Der Einsatz dient sowohl zur Schwenklagerung als auch zweckmäßigerweise zur Axialführung des Druckknopfs und zur Aufnahme seiner Federmittel. Dadurch ist auch der Aufbau des Schlüsselbehälters vereinfacht. Trotz einer einstückigen, preiswerten L-Plattenform des Flachschlüssels lässt sich seine Arretierung in der Ruhe- und Gebrauchslage über den Druckknopf zuverlässig verwirklichen. Außerdem wird der Schlüssel durch die am Druckknopf und Einsatz vorgesehenen Mitnahmeflächen mittels der auf ihn wirkende Federkraft aus einer Ruhelage in die Gebrauchslage selbsttätig herausgeschwenkt, wenn in der Ruhelage die Arretierung durch Betätigen des Druckknopfs unwirksam gesetzt worden ist.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in einem Ausführungsbeispiel schematisch dargestellt. Es zeigen:

Fig. 1, in perspektivischer Darstellung, den Schlüsselbehälter mit herausragendem mechanischen Flachschlüssel,

Fig. 2, ebenfalls in perspektivischer Darstellung, eine zum Flachschlüssel von Fig. 1 gehörende Steckeinheit, bestehend aus einer die elektronischen Bauteile umschließenden Elektrokapsel,

Fig. 3 ein aus dem Schlüsselbehälter von Fig. 1 und der Steckeinheit von Fig. 2 zusammengestecktes Kombinationsgehäuse, das zur Handhabung bei mechanischer und elektronischer Betätigung des Schlüssels dient,

Fig. 4, in Explosionsdarstellung, einige wesentliche Bestandteile des in Fig. 1 gezeigten Schlüsselbehälters mit dem mechanischen Flachschlüssel, vor deren Zusammenbau,

Fig. 5, in Explosionsdarstellung, die beiden Bestandteile des mechanischen Flachschlüssels vor ihrer Vereinigung,

Fig. 6 einen Querschnitt durch den einen Bestandteil von Fig. 5, längs der dortigen Schnittlinie VI - VI,

Fig. 7 einen Querschnitt durch das zusammengebaute Schlüsselbehälter von Fig. 1 längs der dortigen Schnittlinie VII - VII, wobei ein Druckknopf in seiner eingedrückten Position gezeigt ist,

Fig. 8 einen Axialschnitt durch den in Fig. 1 gezeigten Schlüsselbehälter längs der dortigen Schnittlinie VIII - VIII und

Fig. 9 einen Querschnitt durch das in Fig. 3 gezeigte Kombinationsgehäuse längs der dortigen Schnittlinie IX - IX.

Der kombinierte Schlüssel nach der Erfindung erlaubt sowohl eine mechanische als auch eine elektronische Betätigung eines nicht näher gezeigten Schlosses. Er besteht aus zwei jeweils für sich vorgefertigten Teilen 10, 20, die nachträglich ineinandergefügt werden. Der eine Teil 10 umfasst die mechanischen Schließmittel und besteht aus einem Schlüsselbehälter 10, dessen Bestandteile aus der Explosionsdarstellung von Fig. 4 am besten zu erkennen sind. Der andere Teil 20 ist eine noch näher zu beschreibende Steckeinheit, welche die in ihrem Inneren die im Querschnitt von Fig. 9 angedeuteten elektronischen Bauteile 40 umfasst.

Ausweislich der Fig. 1 und 4 umfasst der mechanische Teil zunächst einen zweischaligen Schlüsselbehälter 10. Während die Oberschale 11, wie Fig. 7 und 8 erkennen lässt, als ebene Platte mit stellenweisen Kupplungsvorsprüngen 13 an ihrer Innenfläche ausgebildet ist, umfasst die Unterschale 12 außer ihrem Schalenboden 15 auch noch Schalenseitenwände 14. In den Schalenseitenwänden 14 befinden sich stellenweise Kupplungsaufnahmen 16 für die vorerwähnten Kupplungsvorsprünge 13 der Oberschale 11. Die Oberschale 11 erstreckt sich nur über einen vorderen Bereich

des Schlüsselbehälters 10 und weist im hinteren Bereich einen Ausbruch 17 auf, der zum Schaleninneren 18 hin einen von außen zugänglichen Freiraum erzeugt. Das ist für das noch näher zu beschreibende Einstecken bzw. Herausziehen der Steckeinheit 20 bedeutungsvoll.

Zum Schlüsselbehälter 10 gehört, wie Fig. 4 zeigt, ein mechanischer Flachschlüssel 30 der beweglich angeordnet ist, um aus einer nicht näher gezeigten versenkten Ruhelage im Behälter 10 in eine aus dem Behälter herausragenden, in Fig. 1 bis 4 ersichtliche Gebrauchslage überführt zu werden. Der Flachschlüssel 30 besteht aus metallischem Werkstoff. Obwohl auch andere Bewegungen denkbar wären, ist dieser Flachschlüssel 30 um die strichpunktiert in den Fig. 1, 3 und 4 angedeuteten Schwenkachsen 33 schwenkbeweglich. Dabei ist der Flachschlüssel 30 als ein Stanzling aus einer in Fig. 4 strichpunktiert verdeutlichten ebenen Platte 34 ausgebildet, wobei der Stanzling ein L-förmiges Umrissprofil aus zwei Schenkeln 31, 32 besitzt. Der eine L-Schenkel ist kurz ausgebildet und dient zur Schwenklagerung des Flachschlüssels 30 am Vorderende des Schlüsselbehälters 10 und wird daher nachfolgend kurz „Lagerschenkel" genannt. Der andere L-Schenkel 32 umfasst das eigentliche Flachprofil des Schlüsselschafts, weshalb er nachfolgend als „Schaftschenkel" bezeichnet werden soll. Beide Schenkel 31, 32 liegen also in einer gemeinsamen, durch den erwähnten Plattenverlauf 34 bestimmten Ebene, die im fertig montierten Zustand des Schlüsselbehälters 10 senkrecht zur Schwenkachse 33 verläuft. Ausweislich der Fig. 5 ist der Lagerschenkel 31 mit einem unrunden Plattendurchbruch 35 versehen, der zur Aufnahme eines besonderen Einsatzes 36 dient.

Der Druckknopf 40 ist sowohl axial als auch radial federbelastet und besitzt mit dem Behälter 10 übereinstimmend ausgebildete Profile 19, 48, 28. Der Einsatz 36 besteht aus relativ nachgiebigem Material, vorzugsweise Kunststoff und besitzt ein besonderes Gegenprofil 37, 38, 39 für einen die Lage der Schwenkachse 33 bestimmenden Druckknopf 40. Die Federwirkung übernimmt eine kombinierte Druck-Dreh-Feder 41, die, ausweislich der Fig. 7, in einer Axialbohrung 45 des Druckknopfs 40 aufgenommen ist. Die Feder 41 ist mit ihrem einen Federende 42 drehfest mit dem Druckknopf 40 verbunden, während ihr anderes Federende 43 in der

Unterschale 12 des Behälters 10 festgehalten wird. Die Feder 41 ist wendelförmig ausgebildet. Im Montagefall greift ein an der bodenseitigen Innenfläche der Unterschale 12 sitzender Dorn 44 sowohl ins Wendelinnere hinein, als auch in den Einsatz 36 ein.

Gemäß Fig. 5 wird zunächst der Flachschlüssel 30 mit seinem Plattendurchbruch 35 durch Stanzen erzeugt und dann, nachträglich, der Einsatz 36 in den Plattendurchbruch 35 vertikal eingesteckt. Nach diesem Einstecken ragt, wie Fig. 4 und 7 zeigen, über die beiden Plattenflächen des Flachschlüssels heraus. Dazu gehören zylindrische Ansätze 47, gemäß Fig. 6, aber auch ein Anschlagzapfen 39 an beiden Flächenseiten, der in ein Ringnutsegment 19 der beiden Schalen 11 und 12 hineinragt, wie aus Fig. 8 zu entnehmen ist. In der in Fig. 8 ausgezogen gezeichneten Position des Anschlagnockens 39 liegt die bereits eingangs erwähnte, aus dem Behälter 10 herausgeschwenkte Gebrauchslage vor. Dann erstreckt sich der vorbeschriebene Schaftschenkel 32 des Flachschlüssels 30 in Richtung der in Fig. 8 strichpunktiert angedeuteten Hilfslinie 30.1, welche die in den übrigen Fig. dargestellte Gebrauchslage des Flachschlüssels 30 kennzeichnet. In dieser Gebrauchslage 30.1 ist der Flachschlüssel durch den Druckknopf 40 arretiert. Dann greifen am Druckknopf 40 vorgesehene, hier diametral angeordnete Mitnahmeflügel 48 in zugehörige Radialnuten 28 an der Innenfläche der Oberschale 11 hinein und sichern so die Ausschwenklage des Flachschlüssels 30.

Die Mitnahmeflügel 48 besitzen, als Gegenprofil, im Einsatz 36 Axialnuten 48, die eine Eindruckbewegung im Sinne des aus Fig. 7 erkennbaren Kraftpfeils 46 zulassen. Diese Eindruckbewegung 46, die in Fig. 7 vollzogen ist, führt zu einer axialen Absenkung des Druckknopfs 40, wodurch die Mitnahmeflügel 48 die Radialnuten 28 freigeben. Die Eindruckbewegung 46 erfolgt gegen die axiale Kraftwirkung der Feder 41. Die Arretierung der Gebrauchslage 30.1 ist dann aufgehoben. Der Flachschlüssel kann dann im Sinne des Bewegungspfeils 29 von Fig. 8 gegen die durch den Kraftpfeil 49 in Fig. 8 verdeutlichte Drehkraft der Feder 41 in seine Ruhelage im Gehäuse zurückgeschwenkt werden. Dann liegt der Schaftschenkel 32 des Flachschlüssels 30, in Fig. 8 gesehen, an der dort mit 30.2 gekennzeichneten Strichpunktlinie. In dieser Ruhelage 30.2 verschwindet der Schaftschenkel 32 in

einem aus Fig. 3 erkennbaren seitlichen Spalt 24 eines noch näher zu beschreibenden Gesamtgehäuses 50, welches aus dem Schlüsselbehälter 10 und der darin eingeschobenen Steckeinheit 20 entsteht. Dann sind die Mitnahmeflügel 48 wieder in axialer Ausrichtung mit den gehäuseseitigen Radialnuten 28, wo sie durch die Rückstellkraft der Feder 41 einschnappen und so auch diese Ruhelage 30.2 des Flachschlüssels 30 im Schlüsselbehälter 10 arretieren.

Bei der Schwenkbewegung 29 dient der Druckknopf 40 auch als Schwenklager. Dazu ist in der Oberschale 11 des Behälters 10 eine aus Fig. 4 erkennbare Lagerbohrung 25 vorgesehen. Diese ist in axialer Ausrichtung mit einer in Fig. 5 und 6 gezeigten Axialbohrung 37 des Einsatzes 36 und mit dem bereits mehrfach erwähnten Dorn 44 der Unterschale 12. Der Druckknopf 40 bestimmt die Schwenkachse 33 des Flachschlüssels 30. Der Anschlagzapfen 39 vom Einsatz 36 einerseits und das ihm gehäuseseitig zugeordnete Ringnutsegment 19 andererseits können auch Drehführungsfunktionen bei der Schwenkbewegung 29 übernehmen. Außerdem können Drehanschläge durch das Umrissprofil des Schlüssels 30 einerseits und Innenflächen an den beiden Schalen 11, 12 andererseits verwirklicht sein.

Statt einer Vorfertigung des Einsatzes 36 könnte man den Einsatz 36 durch eine Spritzgusstechnik nachfertigen. Dazu wird der beschriebene Flachschlüssel 30 in eine Spritzgussform eingebracht, in welcher dann der Einsatz 36 im Plattendurchbruch 35 durch Gießen gebildet wird. Die erwähnte Gegenprofilierung 37, 38, 39, 47 liegt dann in ähnlicher Form vor.

In manchen Anwendungsfällen ist bei dem eingangs erwähnten kombinierten Schlüssel für die elektronische Betätigung auch ein sogenannter Transponder 26 erwünscht. Dieser Transponder 26 soll bereits zur elektronischen Individualisierung dieses kombinierten Schlüssels sorgen. Wird dieser Schlüssel in das zugehörige Schloss eingesteckt, so findet zwischen dem Transponder 26 und dem Schloss eine Kommunikation statt, die bei Übereinstimmung von Schloss und Schlüssel bereits Schlossfunktionen auslöst. Deswegen werden bei der Erfindung derartige Transponder 26 im vorderen Bereich des Schlüsselbehälters 10 untergebracht. Dazu besitzt die Unterschale 12 eine Kammer 27, in welche der bzw. die Transponder 26

eingeklebt werden können. Weil eine elektronische Energieversorgung der Transponder 26 nicht erforderlich ist, braucht der fertig montierte Schlüsselbehälter 10 von Fig. 1 nicht mehr in seine Schalen 11, 12 zerlegt zu werden, um dort einen Batteriewechsel od. dgl. vorzunehmen. Die Transponder 26 sind also in der Kammer 27 permanent geschützt. Das gilt auch für die bereits eingangs erwähnten weiteren elektronischen Bauteile 21, welche innerer Bestandteil der bereits erwähnten lösbaren Steckeinheit 20 des Gesamtgehäuses 50 sind.

Wie am besten aus Fig. 9 zu ersehen ist, gehören zur Steckeinheit 20 eine gehäuseartige Kapsel 22, in deren Innenraum 23 die Bauteile 21 angeordnet und so nach außen allseitig abgeschlossen sind. Im Kapselinneren 23 können auch die Schaltungen der Bauelemente und gegebenenfalls die elektrische Störung angeordnet sein. Diese Baueinheit 21, 22, die als Steckeinheit mit dem Schlüsselbehälter 10 fungiert, wird komplett vorgefertigt und soll nachfolgend „Elektrokapsel" genannt werden. Dazu ist der Schlüsselbehälter 10 profilmäßig in folgender Weise angepasst.

Der eingangs erwähnte Ausbruch 17 im Schlüsselbehälter 10 erfolgt einfach dadurch, dass die Oberschale 11, gemäß Fig. 1, nur den Vorderabschnitt 51 des Schlüsselbehälters 10 überdeckt. Dadurch ist ein von außen zugänglicher Freiraum ins Schaleninnere 18 erzeugt. Dieser Freiraum 17 besitzt nicht nur eine nach oben weisende Oberöffnung 52, sondern erstreckt sich auch in eine vom Hinterende 54 zugängliche Seitenöffnung 53. Diese entsteht, weil nicht nur der hintere Abschnitt der Oberschale 11 fehlt, sondern auch, wie Fig. 1 zeigt, die Seitenwand 14 der Unterschale 12 am Hinterende 54 des Behälters 10 weggefallen ist. Die Elektrokapsel 20 wird durch diese Seitenöffnung 53 in den Freiraum 17 des Schlüsselbehälters 10 gemäß dem Bewegungspfeil 55 von Fig. 1 eingeschoben. In ihrer Einschublage, gemäß Fig. 3, verschließt die Elektrokapsel 20 die Oberöffnung 52. Die Einschubbewegung 55 ist in einer Parallelebene zu der oben erwähnten Schwenkbewegung 29 angeordnet. Dabei sind folgende Führungsmittel 61, 62 zum gezielten Einstecken und Verschieben 55 der Elektrokapsel 20 vorgesehen.

An der Innenfläche des Schalenbodens 15 der Unterschale 12 befinden sich zwei parallele Führungsleisten 61, die zur Seitenöffnung 53 hin gerichtet sind. Sie sind

hinterschnitten und besitzen vorzugsweise ein schwalbenschwanzförmiges Profil. Ihnen sind angepasste Führungsnuten 62 an der Unterseite des Gehäuses der Elektrokapsel 20 zugeordnet. Die Eingriffslage dieser Führungsmittel 61, 62 ist im Schnitt von Fig. 9 zu erkennen. Dabei ist die eine Längsseite vom Kapselgehäuse 22 gemäß Fig. 9 bei 58 gestuft, so dass mit einer entsprechenden Stufung 59 in der Unterschale 12, gemäß Fig. 4, in der Einschublage der seitliche Spalt 24 für den Schaftschenkel 32 des Flachschlüssels 30 entsteht. In der Einschublage gemäß Fig. 3 und 9 gehen die sichtbar bleibenden Außenflächen der Elektrokapsel 20 einerseits und des Schlüsselbehälters 10 andererseits ineinander bündig über. Beide Teile 10, 20 bilden dann das bereits erwähnte Kombinationsgehäuse 50, welches beim Handhaben des Schlüssels mit der Hand gemeinsam umgriffen wird und daher „Kombinationsgehäuse" genannt werden soll. Dies gilt sowohl bei einer mechanischen Betätigung des zugehörigen Schlosses, wo der herausgeschwenkte Schaftschenkel 32 mittels des Kombigehäuses 50 gedreht wird, als auch bei der elektronischen Betätigung. Dafür sind Betätigungsstellen 60 an die sichtbar bleibende Außenfläche der Elektrokapsel 20 im gemeinsamen Kombinationsgehäuse 50 vorgesehen. Diese können aus Druckschaltern oder membranartigen Betätigungsstellen entstehen. Diese Betätigungsstellen können mit weiteren membranartigen Überdeckungen im Bereich des vorerwähnten Druckknopfs 40 vorgesehen sein, dem noch folgende besondere Bedeutung zukommt.

Die in Fig. 3 und 9 gezeigte Einstecklage der Elektrokapsel 20 im Schlüsselbehälter 10 ist nicht nur durch Anschlagmittel begrenzt, sondern auch durch Rastmittel gesichert. Diese Funktion kann in vorteilhafterweise auch vom Druckknopf 40 übernommen werden. Dazu ist die Elektrokapsel 20, gemäß Fig. 2, vorderendig mit einem Lappen 56 verlängert, der in der Einschublage von Fig. 3 den verbliebenen Vorderabschnitt 51 der Oberschale 11 vom Schlüsselbehälter 10 überdeckt. Der Lappen 56 besitzt eine Ausnehmung 57, in welche der axial federnde Druckknopf 40 in der Einschublage der Elektrokapsel 20 gemäß Fig. 3 einschnappt. Dadurch ist der Zusammenhalt des Schlüsselbehälters mit der Elektrokapsel 20 sichergestellt. Die Ausnehmung 57 durchsetzt den Lappen 56, weshalb im Eingriffsfall gemäß Fig. 3 der Druckknopf 40 mit einem zu seiner Betätigung ausreichenden Längenstück aus dem Lappen 56 herausragt. Zur Demontage des Kombinationsgehäuses 50 in seine

Bestandteile 10, 20 wird der Druckknopf 40, wie Fig. 7 zeigt, soweit im Sinne des Pfeils 46 eingedrückt, dass er die Ausnehmung 57 im Lappen 56 freigibt.

Der Druckknopf 40 kann durch eine Membran im Bereich des Lappens 56 überdeckt sein, welche in ähnlicher Weise wie die Betätigungsstellen 61 fungiert. Diese Membrane dieser Betätigungsstellen 61 können mit der vorgenannten Membran im Bereich des Druckknopfs 40 kombiniert sein.

Bezugszeichenliste :

10	erster Schlüsselteil, Schlüsselbehälter
11	Oberschale von 10
12	Unterschale von 10
13	Kupplungsvorsprung an 11
14	Schalenseitenwand von 12
15	Schalenboden von 12
16	Kupplungsaufnahme von 12
17	Ausbruch von 11, Freiraum in 18
18	Schaleninneres
19	Profil in 11, 12 für 39, Ringnutsegment
20	zweiter Schlüsselteil, Steckeinheit, Elektrokapsel
21	elektronischer Bauteil
22	gehäuseartige Kapsel für 21
23	Kapselinneres für 22 in 21
24	seitlicher Spalt in 50 für 32 (Fig. 3, 9)
25	Lagerbohrung in 11 für 40 (Fig. 4)
26	Transponder
27	Kammer in 11 für 26 (Fig. 4)
28	Profil in 11 für 48 von 40, Radialnut (Fig. 7)
29	Schwenkbewegungspfeil für 30 (Fig. 8)
30	mechanischer Flachschlüssel für 10, Stanzling
30.1	Gebrauchslage von 32 (Fig. 8)
30.2	Ruhelage von 32 (Fig. 8)
31	erster L-Schenkel von 30, Lagerschenkel
32	zweiter L-Schenkel von 30, Schaftschenkel
33	Schwenkachse für 30
34	ebene Platte für 30
35	Plattendurchbruch
36	Einsatz in 35
37	Gegenprofil in 36, Axialbohrung (Fig. 5, 6)

38 Gegenprofil von 36, Axialnut in 36 für 48 (Fig. 5, 8)
39 Gegenprofil von 36, Führungs- bzw. Anschlagzapfen (Fig. 5, 6)
40 Druckknopf
41 Druck-Dreh-Feder von 40
42 erstes Federende von 41 (Fig. 7)
43 zweites Federende von 41 (Fig. 7)
44 Dorn an 12 für 41 (Fig. 4)
45 Axialbohrung in 40 für 41
46 Pfeil der Eindruckbewegung von 40 (Fig. 7)
47 Gegenprofil an 36, zylindrischer Ansatz an 36 (Fig. 5)
48 Profil, Mitnahmeflügel an 40
49 Pfeil der Ausschwenkkraft von 41 für 30 (Fig. 8)
50 Gesamtgehäuse aus 10, 20, Kombinationsgehäuse
51 Vorderabschnitt von 10
52 Oberöffnung von 10 bei 17 (Fig. 1)
53 Seitenöffnung von 11 (Fig. 1)
54 Hinterende von 10
55 Pfeil der Einschubbewegung von 20 in 10 (Fig. 1)
56 Lappen an 20 (Fig. 2)
57 Ausnehmung in 56 für 40 (Fig. 2)
58 Innenstufung von 22 für 24 (Fig. 2, 9)
59 Stufe von 12 für 24 (Fig. 4)
60 Betätigungsstelle an 20 (Fig. 1)
61 Führungsmittel an 12, Führungsleiste
62 Führungsmittel an 20, Führungsnut

Patentansprüche :

1.) Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für in Fahrzeugen befindliche Schlösser,

mit einem gemeinsamen, bei der Schlüsselbetätigung zu handhabenden Schlüsselbehälter (10) sowohl für elektronische Bauteile (21) zur elektronischen Betätigung des Schlosses als auch für einen L-förmigen Flachschlüssel (30) zur mechanischen Betätigung des Schlosses,

wobei der Flachschlüssel (30) mit seinem einen L-Schenkel, dem Lagerschenkel (31), am Vorderende (51) des Behälters (10) schwenkgelagert (33) ist,

wobei sein anderer, den eigentlichen Schlüsselschaft mit Flachprofil bildender L-Schenkel, der Schaftschenkel (32), aus einer im Behälter (10) eingeschwenkten Ruhelage (30.2) in eine herausgeschwenkte Gebrauchslage (30.1) bewegbar ist,

mit einer axial und radial wirksamen Federbelastung (41)

und mit einem Druckknopf (40), der vorzugsweise zugleich die Schwenkachse (33) des Flachschlüssels (30) im Schlüsselbehälter (10) bestimmt,

wobei der Druckknopf (40) und der Behälter (10) Profile (48, 28) aufweisen und der Lagerschenkel (31) Gegenprofile (37, 38, 39, 47) besitzt, durch die der Flachschlüssel (30) einerseits in seine Gebrauchslage (30.1) kraftbelastet und andererseits in wenigstens einer seiner Lagen (30.1; 30.2) arretiert wird,

und der Schaftschenkel (32) in der gleichen, senkrecht zur Schwenkachse (33) verlaufenden Ebene angeordnet ist, wie der mit dem Druckknopf (44) zusammenwirkende Lagerschenkel (31),

dadurch gekennzeichnet,

dass der L-förmige Flachschlüssel (30) mit seinen beiden Schenkelenden (31, 32) als einstückige ebene Platte ausgebildet ist,

dass der Lagerschenkel (31) einen unrunden Plattendurchbruch (35) besitzt

und dass der Plattendurchbruch (35) zur drehfesten Aufnahme eines Einsatzes (36) dient, der ein Gegenprofil (37, 38, 39, 47) aufweist.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der L-förmige Flachschlüssel (30) und sein unrunder Plattendurchbruch (35) durch Stanzen aus dem Plattenmaterial (34) erzeugt sind und einen Stanzling bildet.

3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Einsatz (36) mit seinem Gegenprofil (37, 38, 39, 47) als Vorprodukt herstellbar ist und einen unrunden Umriss aufweist,

und dass der Einsatz (36) nachträglich in den Plattendurchbruch (35) eingesteckt und dort kraft- und/oder formschlüssig festgehalten ist.

4.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Flachschlüssel (30) aus einem relativ formfesten, metallischen Material gebildet ist und der Einsatz (36) aus relativ nachgiebigem Material, vorzugsweise Kunststoff besteht.

5.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Einsatz (36) mindestens eine der beiden Plattenflächen des Flachschlüssels (30) wenigstens bereichsweise überragt.

6.) Schlüssel nach Anspruch 1, 2 oder 4, dadurch gekennzeichnet, dass der Einsatz (36) im Bereich des Plattendurchbruchs (35) durch Spritzgusstechnik angeformt und mit dem Flachschlüssel (30) spritzgusstechnisch verbunden ist.

7.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Gegenprofil vom Einsatz (36) ein axial abragendes Drehanschlag- und/oder Drehführungs-Element (39) aufweist

und dass das Drehanschlag- und/oder Drehführungs-Element im Montagefall in ein Ringnut-Segment (19) an der Innenfläche des Schlüsselgehäuses (10) hineinragt.

8.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass das Gegenprofil des Einsatzes (36) eine Axialbohrung (37) mit wenigstens einer davon radial abragenden Axialnut (38) umfasst, in welche der Druckknopf (40) mit mindestens einem abgesetzten Mitnahmeflügel (48) zeitweise und/oder bereichsweise eingreift.

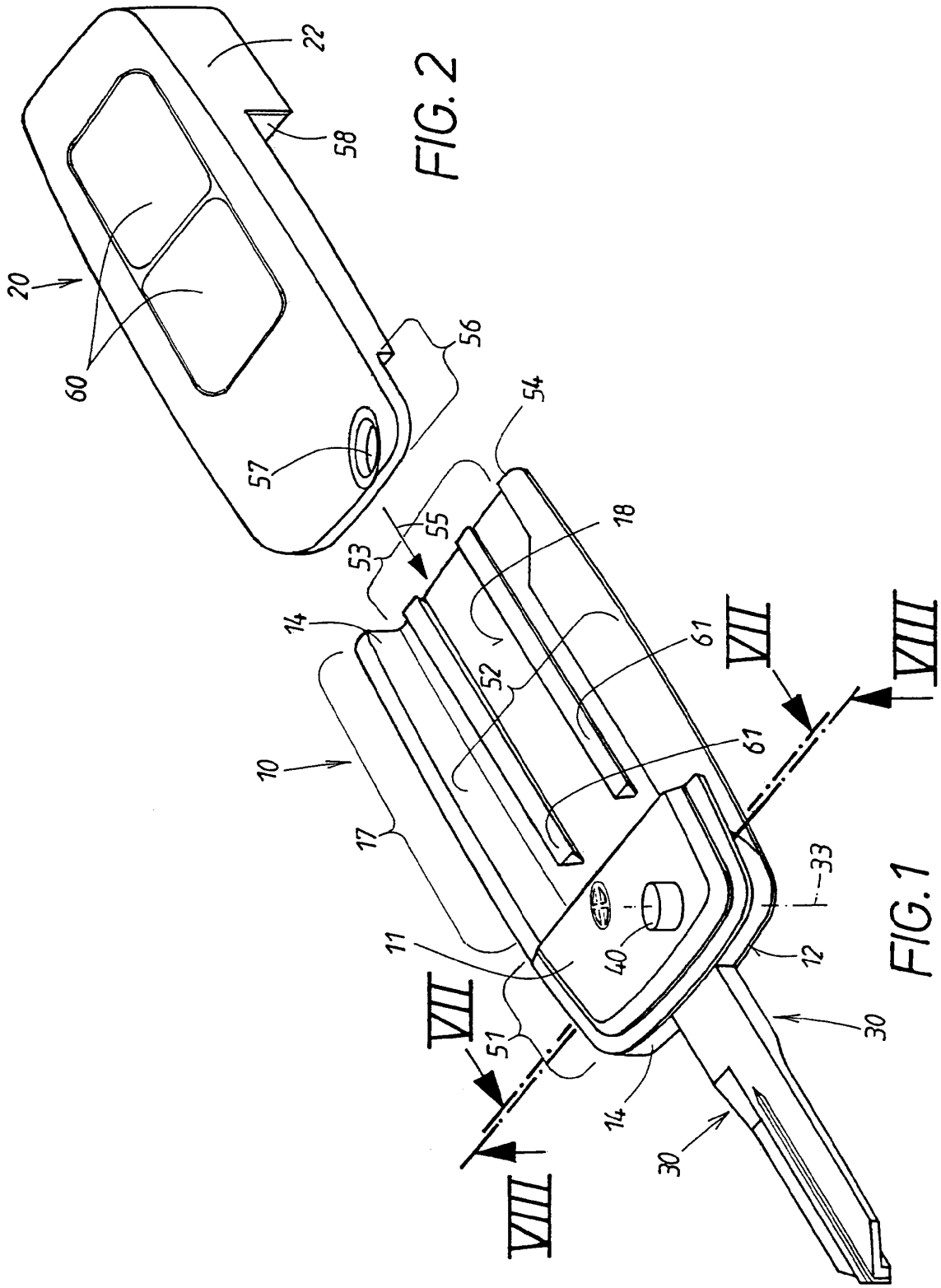


FIG. 2

FIG. 1

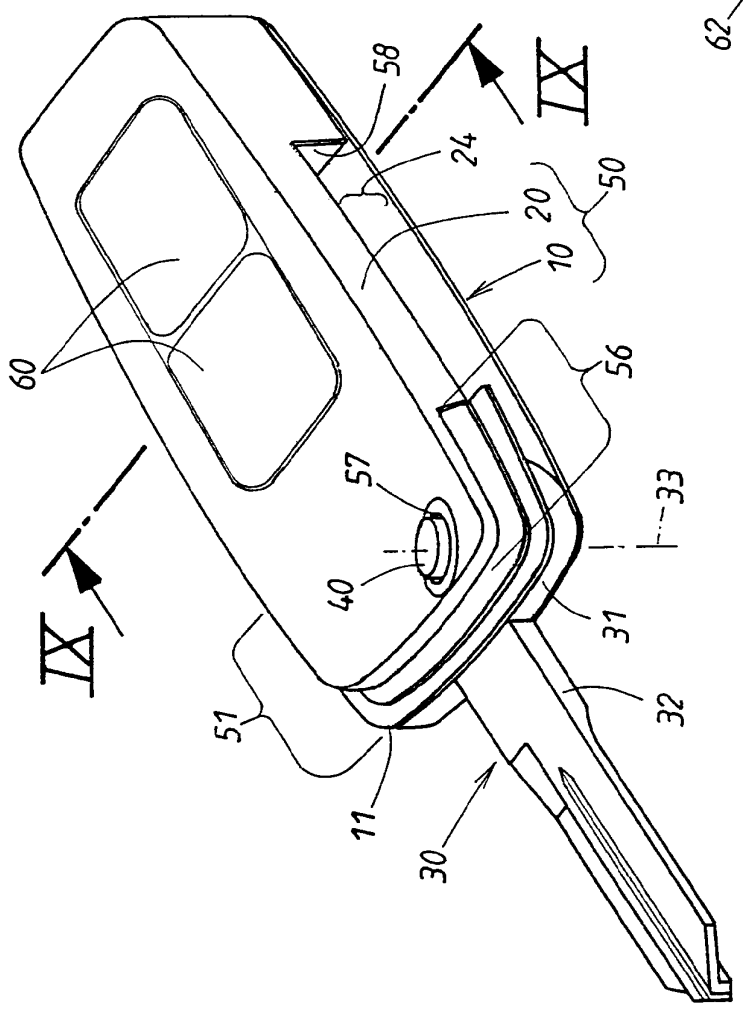

IX
IX
58
24
20
50
10
60
56
57
33
40
31
51
32
11
30

FIG. 3

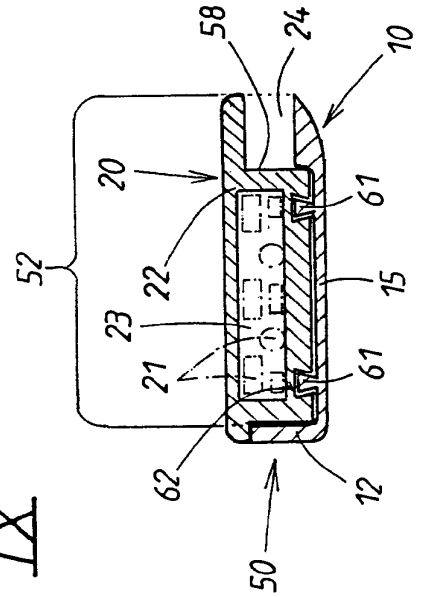

58
24
10
20
61
52
22
15
23
21
61
62
12
50

FIG. 9

315

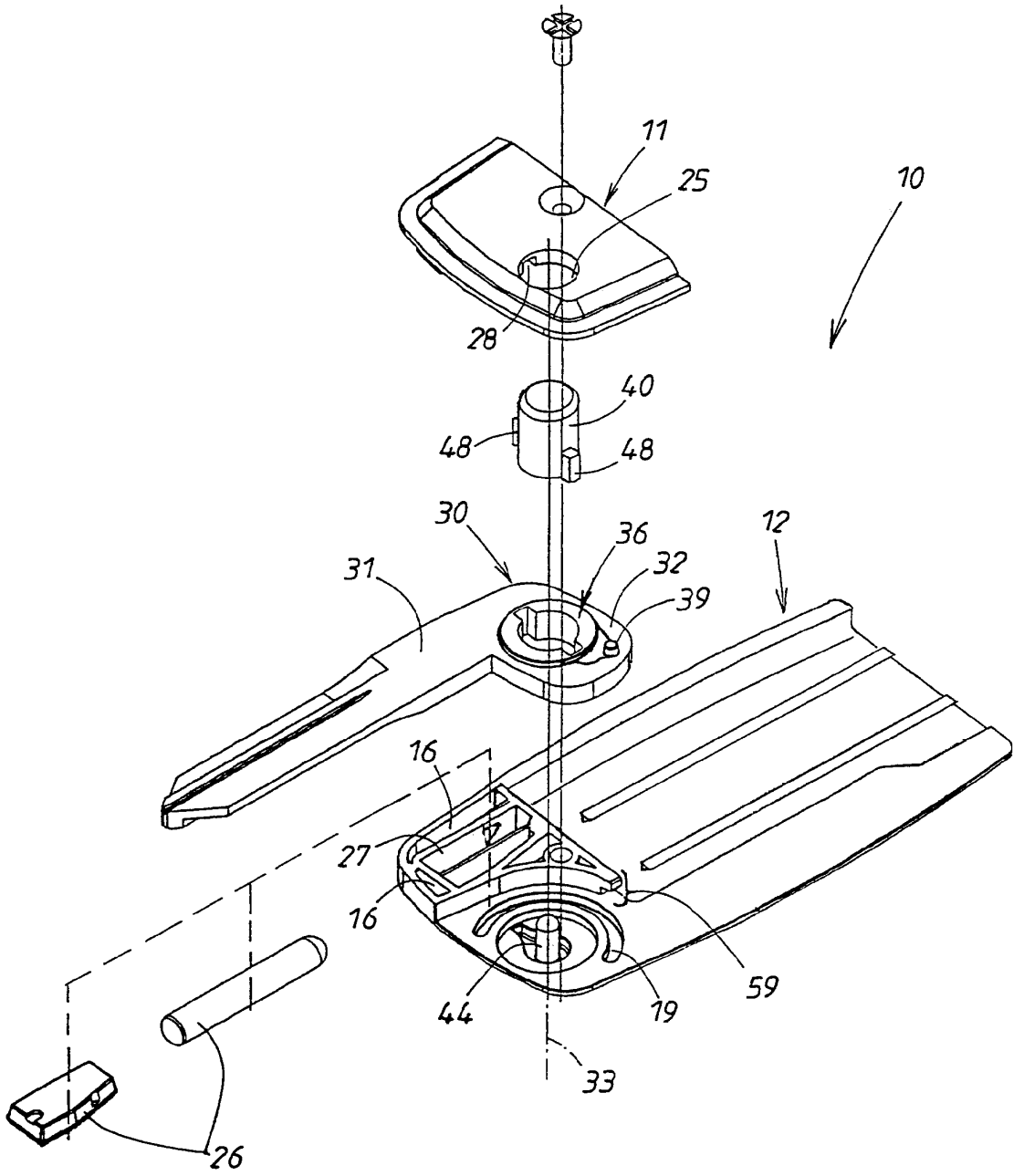


FIG. 4

415

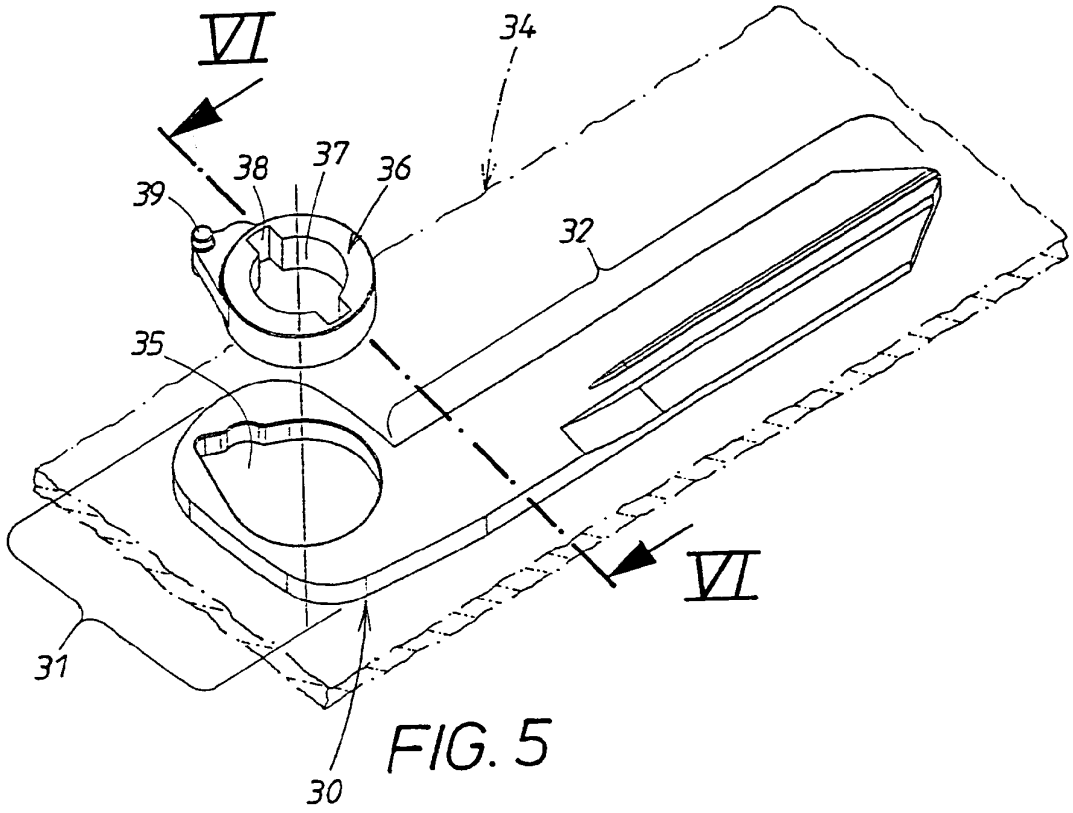


FIG. 5

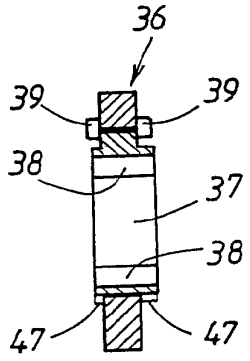


FIG. 6

515

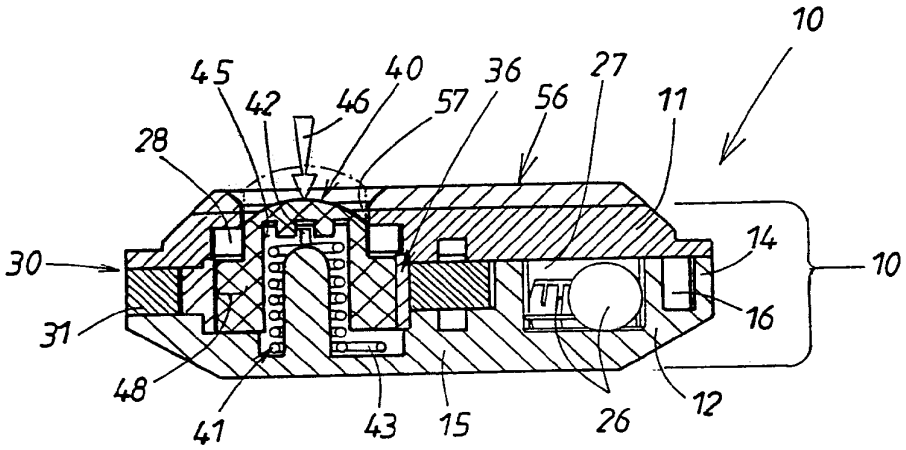


FIG. 7

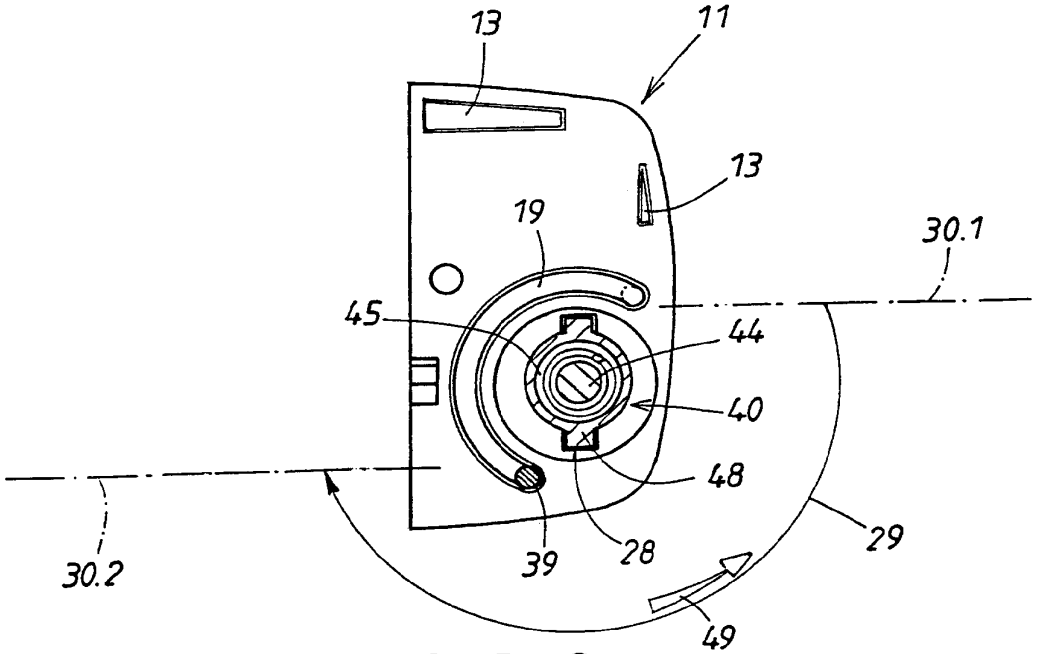


FIG. 8

INTERNATIONAL SEARCH REPORT

Internatic Application No
PCT/EP 00/11619

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B19/04 E05B49/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 42 26 579 A (MERCEDES-BENZ AG) 17 February 1994 (1994-02-17) column 4, line 38 -column 4, line 67; figures	1
A	WO 97 17863 A (POWELL) 22 May 1997 (1997-05-22) page 8, line 30 -page 11, line 14; figures	1
P,A	EP 0 985 788 A (VALEO ELECTRONIQUE) 15 March 2000 (2000-03-15) abstract; figures	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 May 2001	29/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Vacca, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatic ' Application No
PCT/EP 00/11619

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4226579 A	17-02-1994	NONE	
WO 9717863 A	22-05-1997	AU 7579796 A	05-06-1997
EP 985788 A	15-03-2000	FR 2783011 A	10-03-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Internatic ›s Aktenzeichen
PCT/EP 00/11619

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B19/04 E05B49/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 42 26 579 A (MERCEDES-BENZ AG) 17. Februar 1994 (1994-02-17) Spalte 4, Zeile 38 -Spalte 4, Zeile 67; Abbildungen	1
A	WO 97 17863 A (POWELL) 22. Mai 1997 (1997-05-22) Seite 8, Zeile 30 -Seite 11, Zeile 14; Abbildungen	1
P,A	EP 0 985 788 A (VALEO ELECTRONIQUE) 15. März 2000 (2000-03-15) Zusammenfassung; Abbildungen	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
17. Mai 2001	29/05/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Vacca, R

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internatio s Aktenzeichen
PCT/EP 00/11619

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4226579 A	17-02-1994	KEINE	
WO 9717863 A	22-05-1997	AU 7579796 A	05-06-1997
EP 985788 A	15-03-2000	FR 2783011 A	10-03-2000

Formblatt PCT/ISA/210 (Anhang Patentfamilie)(Juli 1992)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
5. Juli 2001 (05.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/48342 A1

(51) Internationale Patentklassifikation[7]: E05B 49/00, 19/00, 19/04

(21) Internationales Aktenzeichen: PCT/EP00/12431

(22) Internationales Anmeldedatum:
8. Dezember 2000 (08.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 62 976.5 24. Dezember 1999 (24.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **JACOB, Dirk** [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE). **MÜLLER, Ulrich** [DE/DE]; Schnegelskothen 7C, 42549 Velbert (DE).

(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

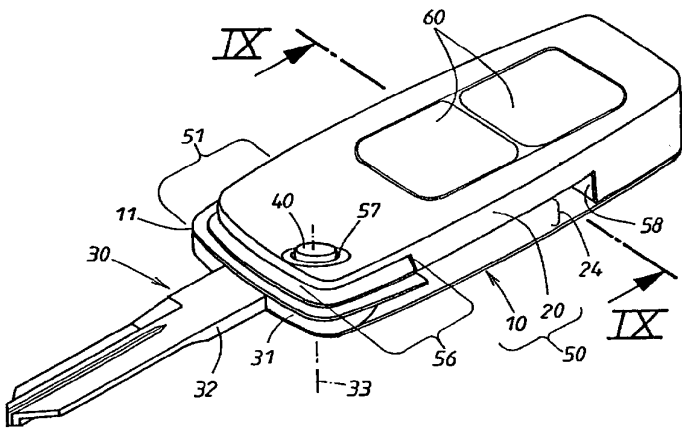
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

[Fortsetzung auf der nächsten Seite]

(54) Title: COMBINED MECHANICAL AND ELECTRONIC KEY, IN PARTICULAR FOR LOCKS IN A VEHICLE

(54) Bezeichnung: KOMBINIERTER MECHANISCHER UND ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR AN FAHRZEUGEN BEFINDLICHE SCHLÖSSER



(57) Abstract: In a combined mechanical and electronic key, electronic components and mechanical flat keys (30) are normally housed in a common key holder (10). In order to place the flat key (30) between a lowered rest position in a holder (10) and a projecting in-use position, the flat key (30) is movably located in a container (10) and secured in at least one of said positions by a push button (40). The key container is assembled from an upper and a lower shell. In order to avoid sealing problems between both shells, according to the invention, the upper shell (11) is provided with an outbreak in a region pertaining thereto which lies outwith the push button.The outbreak creates a void chamber which can be accessed from the outside and is located on the inside of the shell interior. Said electronic components are enclosed by a housing-like capsule and form therewith a prefabricated electrocapsule (20). The electrocapsule (20) forms a socket unit, which can be inserted thereafter in the void chamber pertaining to the pre-assembled key container (10). The electrocapsules (10) are secured in the key container (10) when inserted in said socket. The push button (40) is used to advantage for securing.

[Fortsetzung auf der nächsten Seite]

WO 01/48342 A1

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Bei einem kombinierten mechanischen und elektronischen Schlüssel sind normalerweise die elektronischen Bauteile und der mechanische Flachschlüssel (30) in einem gemeinsamen Schlüsselbehälter (10) untergebracht. Um den Flachschlüssel (30) zwischen einen im Behälter (10) versenkten Ruhelage und einer herausragenden Gebrauchslage zu überführen, ist der Flachschlüssel (30) im Behälter (10) beweglich aufgenommen und in wenigstens einer dieser Lagen durch eine Druckknopf (40) arretiert. Der Schlüsselbehälter wird aus einer Ober- und Unterschale montiert. Um Dichtungsprobleme zwischen den beiden Schalen zu vermeiden, schlägt die Erfindung vor, die Oberschale (11) in ihrem ausserhalb des Druckknopfs (40) liegenden Bereich mit einem Ausbruch zu versehen. Der Ausbruch erzeugt einen von aussen zugänglichen Freiraum im Schaleninneren. Die elektronischen Bauteile sind von einer gehäuseartigen Kapsel umschlossen und bilden mit dieser eine vorgefertigte Elektrokapsel (20). Die Elektrokapsel (20) bildet eine Steckeinheit, welche nachträglich in den Freiraum des fertig montierten Schlüsselbehälters (10) einsteckbar ist. Im Einsteckfall ist die Elektrokapsel (10) im Schlüsselbehälter (10) gesichert. Vorteilhaft nutzt man den Druckknopf (40) für diese Sicherung aus.

Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für an Fahrzeugen befindliche Schlösser

Die Erfindung richtet sich auf einen kombinierten Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Ein solcher Schlüssel erlaubt sowohl eine unmittelbare mechanische Betätigung der Schlösser als auch, alternativ oder ergänzend, eine elektronische Betätigung, z.B. eine Fernbedienung dieses Schlosses bzw. auch anderer Schlösser. Der Schlüsselbehälter ist das Handhabungsmittel sowohl zur mechanischen als auch elektrischen Schlüsselbetätigung. Für die elektronische Betätigung besitzt daher der Schlüsselbehälter an seiner Außenseite Betätigungsstellen, z.B. in Form von elektrischen Druckknöpfen oder nachgiebigen Membranen, die auf im Behälterinneren angeordnete elektrische Schalter od. dgl. einwirken. Der mechanische Flachschlüssel ist im Behälter beweglich aufgenommen und kann aus einer im Behälter versenkten Ruhelage in einer aus dem Behälter herausragenden Gebrauchslage überführt werden. Zur Lagesicherung empfiehlt es sich den Flachschlüssel in beiden Lagen durch einen im Behälter angeordneten axial gefederten Druckknopf zu arretieren.

Bei dem bekannten Schlüssel dieser Art (DE 39 02 537 C2) sind im Inneren des Schlüsselbehälters nicht nur der mechanische Flachschlüssel sondern auch die elektronischen Bauteile für die elektronische Betätigung unmittelbar angeordnet. Die elektronischen Bauteile umfassen auch die zur Energieversorgung dienenden Batterien, die nach längerem Gebrauch ausgewechselt werden müssen. Deswegen wird der Schlüsselbehälter aus einer Oberschale und aus einer Unterschale gebildet, die bedarfsweise voneinander gelöst werden müssen. Die Zerlegung und der Zusammenbau der Schalenteile sind schwierig und zeitaufwendig. Um den Flachschlüssel in der Ruhelage im Behälterinneren versteckt anzuordnen, ist eine seitliche Ausnehmung im Schlüsselbehälter vorgesehen, aus welcher der mechanische Flachschlüssel in seiner Gebrauchslage herausfährt. Durch die Fuge zwischen der Ober- und Unterschale können Schmutz und Feuchtigkeit ins Behälterinnere gelangen, weshalb es dort auf eine gute Dichtung ankommt. Diese Abdichtung ist aber nach längerer Gebrauchsdauer nicht immer gewährleistet, zumal wenn elektronische Bauteile oder Batterien ausgetauscht werden. Der Ausbau und das Einbringen der elektronischen Bauteile und der Batterien im Gehäuseinneren ist mühsam und zeitaufwendig. Bei der Zerlegung und dem Zusammenbau des Schlüsselbehälters mit seinen beiden Schalen besteht die Gefahr, dass die Dichtung nicht mehr ordnungsgemäß plaziert bzw. dabei beschädigt wird. Eine ähnliche Lösung mit den gleichen Nachteilen beschreibt die EP 0 267 429 A1.

Des Weiteren ist aus der GB 2 080 386 A bekannt, einen mechanischen Schlüssel mit einer aufsteckbaren Kassette zu versehen. Die aus zwei Schalen bestehende Kassette, die eine Lichtquelle enthält, bildet eine gehäuseartige Kapsel und kann als Steckeinheit nachträglich eingesteckt oder festgelegt werden. Der Schlüsselgriff besitzt dazu eine Ausnehmung, welche einen von außen zugänglichen Freiraum bildet. Nachteilig bei dieser Anordnung ist, dass die Steckeinheit in Einsteckposition nicht gesichert ist und sich einfach aus der Steckverbindung lösen kann.

Der Erfindung liegt die Aufgabe zugrunde, einen zuverlässigen, raumsparenden Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, bei dem es keine Dichtungsprobleme gibt und bei dem der Austausch von elektronischen Bauteilen und gegebenenfalls Batterien umproblematisch sind. Dies wird erfindungsgemäß durch die im Kennzeichen von Anspruch 1 erwähnten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Erfindung braucht sich mit dem Dichtungsproblem zwischen der Ober- und Unterschale des Schlüsselbehälters nicht zu befassen, weil die auf Schmutz und Feuchtigkeit sehr empfindlichen elektronischen Bauteile, zu denen gegebenenfalls elektrische Batterien gehören, von einer gehäuseartigen Kapsel umschlossen sind, mit der sie eine vorgefertigte Baueinheit bildet, die nachfolgend kurz „Elektrokapsel" bezeichnet werden soll. Die in der Elektrokapsel befindlichen Elemente sind allseitig versiegelt. Bedarfsweise können die elektronischen Bauteile in der Elektrokapsel eingegossen sein. Diese Elektrokapsel ist dichtungsmäßig autark und bringt daher keine Dichtungsprobleme im Schlüsselbehälter. Die elektronischen Bauteile und ihre elektrischen Batterien sind im Inneren der Elektrokapsel nach außen geschützt untergebracht. Die Elektrokapsel wird ohne den zweischaligen Schlüsselbehälter zerlegen zu müssen, schnell und bequem in den Freiraum des Schlüsselbehälters eingesteckt und wieder entnommen werden. Die Elektrokapsel kann als eigenständiges Handelsprodukt in Verkehr gebracht werden, der vom Besitzer des Schlüssels erworben und mit dem stets geschlossen bleibenden Schlüsselbehälter zusammengesteckt werden kann.

Sowohl der Schlüsselbehälter mit seinem Ausbruch einerseits als auch die Elektrokapsel andererseits werden für sich vorgefertigt und sind jederzeit miteinander montierbar bzw. voneinander demontierbar. Weil der Schlüsselbehälter nicht in seine beiden Schalen zerlegt zu werden braucht, treten dort keine Dichtungsprobleme auf. Im übrigen ist es unmaßgeblich, ob bei eingesteckter Elektrokapsel der Schlüsselbehälter abgedichtet ist, denn dort

befinden sich nur die hinsichtlich Schmutz und Feuchtigkeit unempfindlichen Bauteile, wie der mechanische Flachschlüssel. Der Ausbruch im Schlüsselbehälter wird von der eingesteckten Elektrokapsel verschlossen. Die Elektrokapsel vervollständigt den Schlüsselbehälter zu einem bei der Schlüsselbetätigung gemeinsam zu handhabenden Kombinationsgehäuse. Die zur Handhabung dienende Fläche des Kombinationsgehäuses wird also teils vom Schlüsselbehälter des mechanischen Flachschlüssels und teils von der freibleibenden Umfangsfläche der Elektrokapsel gebildet. An den Übergangsstellen wird man für einen bündigen Übergang sorgen.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in einem Ausführungsbeispiel schematisch dargestellt. Es zeigen:

Fig. 1, in perspektivischer Darstellung, den Schlüsselbehälter mit herausragendem mechanischen Flachschlüssel,

Fig. 2, ebenfalls in perspektivischer Darstellung, eine zum Flachschlüssel von Fig. 1 gehörende Steckeinheit, bestehend aus einer die elektronischen Bauteile umschließenden Elektrokapsel,

Fig. 3 ein aus dem Schlüsselbehälter von Fig. 1 und der Steckeinheit von Fig. 2 zusammengestecktes Kombinationsgehäuse, das zur Handhabung bei mechanischer und elektronischer Betätigung des Schlüssels dient,

Fig. 4, in Explosionsdarstellung, einige wesentliche Bestandteile des in Fig. 1 gezeigten Schlüsselbehälters mit dem mechanischen Flachschlüssel, vor deren Zusammenbau,

Fig. 5, in Explosionsdarstellung, die beiden Bestandteile des mechanischen Flachschlüssels vor ihrer Vereinigung,

Fig. 6 einen Querschnitt durch den einen Bestandteil von Fig. 5, längs der dortigen Schnittlinie VI - VI,

Fig. 7 einen Querschnitt durch das zusammengebaute Schlüsselbehälter von Fig. 1 längs der dortigen Schnittlinie VII - VII, wobei ein Druckknopf in seiner eingedrückten Position gezeigt ist,

Fig. 8 einen Axialschnitt durch den in Fig. 1 gezeigten Schlüsselbehälter längs der dortigen Schnittlinie VIII - VIII und

Fig. 9 einen Querschnitt durch das in Fig. 3 gezeigte Kombinationsgehäuse längs der dortigen Schnittlinie IX - IX.

Der kombinierte Schlüssel nach der Erfindung erlaubt sowohl eine mechanische als auch eine elektronische Betätigung eines nicht näher gezeigten Schlosses. Er besteht aus zwei jeweils für sich vorgefertigten Teilen 10, 20, die nachträglich ineinandergefügt werden. Der eine Teil 10 umfasst die mechanischen Schließmittel und besteht aus einem Schlüsselbehälter 10, dessen Bestandteile aus der Explosionsdarstellung von Fig. 4 am besten zu erkennen sind. Der andere Teil 20 ist eine noch näher zu beschreibende Steckeinheit, welche die in ihrem Inneren die im Querschnitt von Fig. 9 angedeuteten elektronischen Bauteile 40 umfasst.

Ausweislich der Fig. 1 und 4 umfasst der mechanische Teil zunächst einen zweischaligen Schlüsselbehälter 10. Während die Oberschale 11, wie Fig. 7 und 8 erkennen lässt, als ebene Platte mit stellenweisen Kupplungsvorsprüngen 13 an

ihrer Innenfläche ausgebildet ist, umfasst die Unterschale 12 außer ihrem Schalenboden 15 auch noch Schalenseitenwände 14. In den Schalenseitenwänden 14 befinden sich stellenweise Kupplungsaufnahmen 16 für die vorerwähnten Kupplungsvorsprünge 13 der Oberschale 11. Die Oberschale 11 erstreckt sich nur über einen vorderen Bereich des Schlüsselbehälters 10 und weist im hinteren Bereich einen Ausbruch 17 auf, der zum Schaleninneren 18 hin einen von außen zugänglichen Freiraum erzeugt. Das ist für das noch näher zu beschreibende Einstecken bzw. Herausziehen der Steckeinheit 20 bedeutungsvoll.

Zum Schlüsselbehälter 10 gehört, wie Fig. 4 zeigt, ein mechanischer Flachschlüssel 30 der beweglich angeordnet ist, um aus einer nicht näher gezeigten versenkten Ruhelage im Behälter 10 in eine aus dem Behälter herausragenden, in Fig. 1 bis 4 ersichtliche Gebrauchslage überführt zu werden. Der Flachschlüssel 30 besteht aus metallischem Werkstoff. Obwohl auch andere Bewegungen denkbar wären, ist dieser Flachschlüssel 30 um die strichpunktiert in den Fig. 1, 3 und 4 angedeuteten Schwenkachsen 33 schwenkbeweglich. Dabei ist der Flachschlüssel 30 als ein Stanzling aus einer in Fig. 4 strichpunktiert verdeutlichten ebenen Platte 34 ausgebildet, wobei der Stanzling ein L-förmiges Umrissprofil aus zwei Schenkeln 31, 32 besitzt. Der eine L-Schenkel ist kurz ausgebildet und dient zur Schwenklagerung des Flachschlüssels 30 am Vorderende des Schlüsselbehälters 10 und wird daher nachfolgend kurz „Lagerschenkel" genannt. Der andere L-Schenkel 32 umfasst das eigentliche Flachprofil des Schlüsselschafts, weshalb er nachfolgend als „Schaftschenkel" bezeichnet werden soll. Beide Schenkel 31, 32 liegen also in einer gemeinsamen, durch den erwähnten Plattenverlauf 34 bestimmten Ebene, die im fertig montierten Zustand des Schlüsselbehälters 10 senkrecht zur Schwenkachse 33 verläuft. Ausweislich der Fig. 5 ist der Lagerschenkel 31 mit einem unrunden Plattendurchbruch 35 versehen, der zur Aufnahme eines besonderen Einsatzes 36 dient.

Der Druckknopf 40 ist sowohl axial als auch radial federbelastet und besitzt mit dem Behälter 10 übereinstimmend ausgebildete Profile 19, 48, 28. Der Einsatz 36

besteht aus relativ nachgiebigem Material, vorzugsweise Kunststoff und besitzt ein besonderes Gegenprofil 37, 38, 39 für einen die Lage der Schwenkachse 33 bestimmenden Druckknopf 40. Die Federwirkung übernimmt eine kombinierte Druck-Dreh-Feder 41, die, ausweislich der Fig. 7, in einer Axialbohrung 45 des Druckknopfs 40 aufgenommen ist. Die Feder 41 ist mit ihrem einen Federende 42 drehfest mit dem Druckknopf 40 verbunden, während ihr anderes Federende 43 in der Unterschale 12 des Behälters 10 festgehalten wird. Die Feder 41 ist wendelförmig ausgebildet. Im Montagefall greift ein an der bodenseitigen Innenfläche der Unterschale 12 sitzender Dorn 44 sowohl ins Wendelinnere hinein, als auch in den Einsatz 36 ein.

Gemäß Fig. 5 wird zunächst der Flachschlüssel 30 mit seinem Plattendurchbruch 35 durch Stanzen erzeugt und dann, nachträglich, der Einsatz 36 in den Plattendurchbruch 35 vertikal eingesteckt. Nach diesem Einstecken ragt, wie Fig. 4 und 7 zeigen, über die beiden Plattenflächen des Flachschlüssels heraus. Dazu gehören zylindrische Ansätze 47, gemäß Fig. 6, aber auch ein Anschlagzapfen 39 an beiden Flächenseiten, der in ein Ringnutsegment 19 der beiden Schalen 11 und 12 hineinragt, wie aus Fig. 8 zu entnehmen ist. In der in Fig. 8 ausgezogen gezeichneten Position des Anschlagnockens 39 liegt die bereits eingangs erwähnte, aus dem Behälter 10 herausgeschwenkte Gebrauchslage vor. Dann erstreckt sich der vorbeschriebene Schaftschenkel 32 des Flachschlüssels 30 in Richtung der in Fig. 8 strichpunktiert angedeuteten Hilfslinie 30.1, welche die in den übrigen Fig. dargestellte Gebrauchslage des Flachschlüssels 30 kennzeichnet. In dieser Gebrauchslage 30.1 ist der Flachschlüssel durch den Druckknopf 40 arretiert. Dann greifen am Druckknopf 40 vorgesehene, hier diametral angeordnete Mitnahmeflügel 48 in zugehörige Radialnuten 28 an der Innenfläche der Oberschale 11 hinein und sichern so die Ausschwenklage des Flachschlüssels 30.

Die Mitnahmeflügel 48 besitzen, als Gegenprofil, im Einsatz 36 Axialnuten 48, die eine Eindruckbewegung im Sinne des aus Fig. 7 erkennbaren Kraftpfeils 46 zulassen. Diese Eindruckbewegung 46, die in Fig. 7 vollzogen ist, führt zu einer

axialen Absenkung des Druckknopfs 40, wodurch die Mitnahmeflügel 48 die Radialnuten 28 freigeben. Die Eindruckbewegung 46 erfolgt gegen die axiale Kraftwirkung der Feder 41. Die Arretierung der Gebrauchslage 30.1 ist dann aufgehoben. Der Flachschlüssel kann dann im Sinne des Bewegungspfeils 29 von Fig. 8 gegen die durch den Kraftpfeil 49 in Fig. 8 verdeutlichte Drehkraft der Feder 41 in seine Ruhelage im Gehäuse zurückgeschwenkt werden. Dann liegt der Schaftschenkel 32 des Flachschlüssels 30, in Fig. 8 gesehen, an der dort mit 30.2 gekennzeichneten Strichpunktlinie. In dieser Ruhelage 30.2 verschwindet der Schaftschenkel 32 in einem aus Fig. 3 erkennbaren seitlichen Spalt 24 eines noch näher zu beschreibenden Gesamtgehäuses 50, welches aus dem Schlüsselbehälter 10 und der darin eingeschobenen Steckeinheit 20 entsteht. Dann sind die Mitnahmeflügel 48 wieder in axialer Ausrichtung mit den gehäuseseitigen Radialnuten 28, wo sie durch die Rückstellkraft der Feder 41 einschnappen und so auch diese Ruhelage 30.2 des Flachschlüssels 30 im Schlüsselbehälter 10 arretieren.

Bei der Schwenkbewegung 29 dient der Druckknopf 40 auch als Schwenklager. Dazu ist in der Oberschale 11 des Behälters 10 eine aus Fig. 4 erkennbare Lagerbohrung 25 vorgesehen. Diese ist in axialer Ausrichtung mit einer in Fig. 5 und 6 gezeigten Axialbohrung 37 des Einsatzes 36 und mit dem bereits mehrfach erwähnten Dorn 44 der Unterschale 12. Der Druckknopf 40 bestimmt die Schwenkachse 33 des Flachschlüssels 30. Der Anschlagzapfen 39 vom Einsatz 36 einerseits und das ihm gehäuseseitig zugeordnete Ringnutsegment 19 andererseits können auch Drehführungsfunktionen bei der Schwenkbewegung 29 übernehmen. Außerdem können Drehanschläge durch das Umrissprofil des Schlüssels 30 einerseits und Innenflächen an den beiden Schalen 11, 12 andererseits verwirklicht sein.

Statt einer Vorfertigung des Einsatzes 36 könnte man den Einsatz 36 durch eine Spritzgusstechnik nachfertigen. Dazu wird der beschriebene Flachschlüssel 30 in eine Spritzgussform eingebracht, in welcher dann der Einsatz 36 im

Plattendurchbruch 35 durch Gießen gebildet wird. Die erwähnte Gegenprofilierung 37, 38, 39, 47 liegt dann in ähnlicher Form vor.

In manchen Anwendungsfällen ist bei dem eingangs erwähnten kombinierten Schlüssel für die elektronische Betätigung auch ein sogenannter Transponder 26 erwünscht. Dieser Transponder 26 soll bereits zur elektronischen Individualisierung dieses kombinierten Schlüssels sorgen. Wird dieser Schlüssel in das zugehörige Schloss eingesteckt, so findet zwischen dem Transponder 26 und dem Schloss eine Kommunikation statt, die bei Übereinstimmung von Schloss und Schlüssel bereits Schlossfunktionen auslöst. Deswegen werden bei der Erfindung derartige Transponder 26 im vorderen Bereich des Schlüsselbehälters 10 untergebracht. Dazu besitzt die Unterschale 12 eine Kammer 27, in welche der bzw. die Transponder 26 eingeklebt werden können. Weil eine elektronische Energieversorgung der Transponder 26 nicht erforderlich ist, braucht der fertig montierte Schlüsselbehälter 10 von Fig. 1 nicht mehr in seine Schalen 11, 12 zerlegt zu werden, um dort einen Batteriewechsel od. dgl. vorzunehmen. Die Transponder 26 sind also in der Kammer 27 permanent geschützt. Das gilt auch für die bereits eingangs erwähnten weiteren elektronischen Bauteile 21, welche innerer Bestandteil der bereits erwähnten lösbaren Steckeinheit 20 des Gesamtgehäuses 50 sind.

Wie am besten aus Fig. 9 zu ersehen ist, gehören zur Steckeinheit 20 eine gehäuseartige Kapsel 22, in deren Innenraum 23 die Bauteile 21 angeordnet und so nach außen allseitig abgeschlossen sind. Im Kapselinneren 23 können auch die Schaltungen der Bauelemente und gegebenenfalls die elektrische Störung angeordnet sein. Diese Baueinheit 21, 22, die als Steckeinheit mit dem Schlüsselbehälter 10 fungiert, wird komplett vorgefertigt und soll nachfolgend „Elektrokapsel“ genannt werden. Dazu ist der Schlüsselbehälter 10 profilmäßig in folgender Weise angepasst.

Der eingangs erwähnte Ausbruch 17 im Schlüsselbehälter 10 erfolgt einfach dadurch, dass die Oberschale 11, gemäß Fig. 1, nur den Vorderabschnitt 51 des Schlüsselbehälters 10 überdeckt. Dadurch ist ein von außen zugänglicher Freiraum ins Schaleninnere 18 erzeugt. Dieser Freiraum 17 besitzt nicht nur eine nach oben weisende Oberöffnung 52, sondern erstreckt sich auch in eine vom Hinterende 54 zugängliche Seitenöffnung 53. Diese entsteht, weil nicht nur der hintere Abschnitt der Oberschale 11 fehlt, sondern auch, wie Fig. 1 zeigt, die Seitenwand 14 der Unterschale 12 am Hinterende 54 des Behälters 10 weggefallen ist. Die Elektrokapsel 20 wird durch diese Seitenöffnung 53 in den Freiraum 17 des Schlüsselbehälters 10 gemäß dem Bewegungspfeil 55 von Fig. 1 eingeschoben. In ihrer Einschublage, gemäß Fig. 3, verschließt die Elektrokapsel 20 die Oberöffnung 52. Die Einschubbewegung 55 ist in einer Parallelebene zu der oben erwähnten Schwenkbewegung 29 angeordnet. Dabei sind folgende Führungsmittel 61, 62 zum gezielten Einstecken und Verschieben 55 der Elektrokapsel 20 vorgesehen.

An der Innenfläche des Schalenbodens 15 der Unterschale 12 befinden sich zwei parallele Führungsleisten 61, die zur Seitenöffnung 53 hin gerichtet sind. Sie sind hinterschnitten und besitzen vorzugsweise ein schwalbenschwanzförmiges Profil. Ihnen sind angepasste Führungsnuten 62 an der Unterseite des Gehäuses der Elektrokapsel 20 zugeordnet. Die Eingriffslage dieser Führungsmittel 61, 62 ist im Schnitt von Fig. 9 zu erkennen. Dabei ist die eine Längsseite vom Kapselgehäuse 22 gemäß Fig. 9 bei 58 gestuft, so dass mit einer entsprechenden Stufung 59 in der Unterschale 12, gemäß Fig. 4, in der Einschublage der seitliche Spalt 24 für den Schaftschenkel 32 des Flachschlüssels 30 entsteht. In der Einschublage gemäß Fig. 3 und 9 gehen die sichtbar bleibenden Außenflächen der Elektrokapsel 20 einerseits und des Schlüsselbehälters 10 andererseits ineinander bündig über. Beide Teile 10, 20 bilden dann das bereits erwähnte Kombinationsgehäuse 50, welches beim Handhaben des Schlüssels mit der Hand gemeinsam umgriffen wird und daher „Kombinationsgehäuse“ genannt werden soll. Dies gilt sowohl bei einer mechanischen Betätigung des zugehörigen Schlosses, wo der herausgeschwenkte

Schaftschenkel 32 mittels des Kombigehäuses 50 gedreht wird, als auch bei der elektronischen Betätigung. Dafür sind Betätigungsstellen 60 an die sichtbar bleibende Außenfläche der Elektrokapsel 20 im gemeinsamen Kombinationsgehäuse 50 vorgesehen. Diese können aus Druckschaltern oder membranartigen Betätigungsstellen entstehen. Diese Betätigungsstellen können mit weiteren membranartigen Überdeckungen im Bereich des vorerwähnten Druckknopfs 40 vorgesehen sein, dem noch folgende besondere Bedeutung zukommt.

Die in Fig. 3 und 9 gezeigte Einstecklage der Elektrokapsel 20 im Schlüsselbehälter 10 ist nicht nur durch Anschlagmittel begrenzt, sondern auch durch Rastmittel gesichert. Diese Funktion kann in vorteilhafterweise auch vom Druckknopf 40 übernommen werden. Dazu ist die Elektrokapsel 20, gemäß Fig. 2, vorderendig mit einem Lappen 56 verlängert, der in der Einschublage von Fig. 3 den verbliebenen Vorderabschnitt 51 der Oberschale 11 vom Schlüsselbehälter 10 überdeckt. Der Lappen 56 besitzt eine Ausnehmung 57, in welche der axial federnde Druckknopf 40 in der Einschublage der Elektrokapsel 20 gemäß Fig. 3 einschnappt. Dadurch ist der Zusammenhalt des Schlüsselbehälters mit der Elektrokapsel 20 sichergestellt. Die Ausnehmung 57 durchsetzt den Lappen 56, weshalb im Eingriffsfall gemäß Fig. 3 der Druckknopf 40 mit einem zu seiner Betätigung ausreichenden Längenstück aus dem Lappen 56 herausragt. Zur Demontage des Kombinationsgehäuses 50 in seine Bestandteile 10, 20 wird der Druckknopf 40, wie Fig. 7 zeigt, soweit im Sinne des Pfeils 46 eingedrückt, dass er die Ausnehmung 57 im Lappen 56 freigibt.

Der Druckknopf 40 kann durch eine Membran im Bereich des Lappens 56 überdeckt sein, welche in ähnlicher Weise wie die Betätigungsstellen 61 fungiert. Diese Membrane dieser Betätigungsstellen 61 können mit der vorgenannten Membran im Bereich des Druckknopfs 40 kombiniert sein.

Bezugszeichenliste :

10	erster Schlüsselteil, Schlüsselbehälter
11	Oberschale von 10
12	Unterschale von 10
13	Kupplungsvorsprung an 11
14	Schalenseitenwand von 12
15	Schalenboden von 12
16	Kupplungsaufnahme von 12
17	Ausbruch von 11, Freiraum in 18
18	Schaleninneres
19	Profil in 11, 12 für 39, Ringnutsegment
20	zweiter Schlüsselteil, Steckeinheit, Elektrokapsel
21	elektronischer Bauteil
22	gehäuseartige Kapsel für 21
23	Kapselinneres für 22 in 21
24	seitlicher Spalt in 50 für 32 (Fig. 3, 9)
25	Lagerbohrung in 11 für 40 (Fig. 4)
26	Transponder
27	Kammer in 11 für 26 (Fig. 4)
28	Profil in 11 für 48 von 40, Radialnut (Fig. 7)
29	Schwenkbewegungspfeil für 30 (Fig. 8)
30	mechanischer Flachschlüssel für 10, Stanzling
30.1	Gebrauchslage von 32 (Fig. 8)
30.2	Ruhelage von 32 (Fig. 8)
31	erster L-Schenkel von 30, Lagerschenkel
32	zweiter L-Schenkel von 30, Schaftschenkel
33	Schwenkachse für 30
34	ebene Platte für 30
35	Plattendurchbruch

36 Einsatz in 35

37 Gegenprofil in 36, Axialbohrung (Fig. 5, 6)

38 Gegenprofil von 36, Axialnut in 36 für 48 (Fig. 5, 8)

39 Gegenprofil von 36, Führungs- bzw. Anschlagzapfen (Fig. 5, 6)

40 Druckknopf

41 Druck-Dreh-Feder von 40

42 erstes Federende von 41 (Fig. 7)

43 zweites Federende von 41 (Fig. 7)

44 Dorn an 12 für 41 (Fig. 4)

45 Axialbohrung in 40 für 41

46 Pfeil der Eindruckbewegung von 40 (Fig. 7)

47 Gegenprofil an 36, zylindrischer Ansatz an 36 (Fig. 5)

48 Profil, Mitnahmeflügel an 40

49 Pfeil der Ausschwenkkraft von 41 für 30 (Fig. 8)

50 Gesamtgehäuse aus 10, 20, Kombinationsgehäuse

51 Vorderabschnitt von 10

52 Oberöffnung von 10 bei 17 (Fig. 1)

53 Seitenöffnung von 11 (Fig. 1)

54 Hinterende von 10

55 Pfeil der Einschubbewegung von 20 in 10 (Fig. 1)

56 Lappen an 20 (Fig. 2)

57 Ausnehmung in 56 für 40 (Fig. 2)

58 Innenstufung von 22 für 24 (Fig. 2, 9)

59 Stufe von 12 für 24 (Fig. 4)

60 Betätigungsstelle an 20 (Fig. 1)

61 Führungsmittel an 12, Führungsleiste

62 Führungsmittel an 20, Führungsnut

P a t e n t a n s p r ü c h e :

1.) Kombinierter mechnischer und elektronischer Schlüssel, insbesondere für in Fahrzeugen befindliche Schlösser,

mit einem gemeinsamen, bei der Schlüsselbetätigung zu handhabenden Schlüsselbehälter (10) sowohl für elektronische Bauteile (21) zur elektronischen Betätigung als auch für einen Flachschlüssel (30) zur mechanischen Betätigung des Schlosses,

wobei der Flachschlüssel (30) im Behälter beweglich (29) aufgenommen ist und aus einer im Behälter (10) versenkten Ruhelage (30.2) in eine aus dem Behälter (10) herausragende Gebrauchslage (30.1) überführbar ist,

und mit einem im Behälter (10) angeordneten axial gefederten (41) Druckknopf (40), der den Schlüssel (30) in wenigstens einer dieser Lagen (30.1; 30.2) arretiert,

wobei der Schlüsselbehälter (10) aus einer Ober- und Unterschale (11, 12) besteht, die wenigstens bereichsweise aneinander befestigt sind,

d a d u r c h g e k e n n z e i c h n e t ,

daß die Oberschale (11) in ihrem außerhalb des Druckknopfs (40) liegenden Bereich einen Ausbruch (17) aufweist,

daß der Ausbruch einen von außen zugänglichen Freiraum (17) im Schaleninneren (18) erzeugt,

daß die elektronischen Bauteile (21), deren Schaltung und gegebenenfalls elektrische Steuerung von einer gehäuseartigen Kapsel (22) umschlossen sind und mit dieser eine vorgefertigte

daß die Elektrokapsel (20) eine Steckeinheit bildet, welche nachträglich in den Freiraum (17) des fertig montierten Schlüsselbehälters (10) einsteckbar (55) und dort festlegbar ist,

daß die Elektrokapsel (20) einen sie vorderendig verlängerten Lappen (56) besitzt,

daß in der Einschublage der Kapsel (20) der Lappen (56) das vor der Oberöffnung (52) des Schlüsselbehälters befindliche Raststück (51) der Oberschale (11) wenigstens bereichsweise überdeckt,

und daß der Lappen (56) eine Ausnehmung (57) aufweist, in welcher der federnde (41) Druckknopf (40) axial einfährt und die Einschublage der Elektrokapsel (20) im Schlüsselbehälter (10) sichert.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die eingesteckte Elektrokapsel (20) auf ihrer im Ausbruch (17) freiliegenden Flächenbereichen Betätigungsstellen (60) zum Wirksamsetzen der in ihrem Inneren befindlichen elektronischen Bauteile (21) besitzt.

3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die eingesteckte Elektrokapsel (20) den Ausbruch (17) im Schlüsselbehälter (10) verschließt

und dass die Steckkombination aus der Elektrokapsel (20) einerseits und dem Schlüsselbehälter (20) andererseits ein Kombinationsgehäuse (50) mit bündig übergehender Umfangsfläche erzeugt.

4.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Ausbruch (17) nicht nur eine nach oben weisende Oberöffnung (52) erzeugt, die durch Wegfall des hinteren Oberschalen-Abschnitts entsteht, sondern sich auch über eine Seitenöffnung (53) erstreckt, die durch einen wenigstens bereichsweisen Wegfall der Seitenwand (14) in der Unterschale (12) und gegebenenfalls in der Oberschale (11) entsteht,

dass die Elektrokapsel (20) durch die Seitenöffnung (53) in den Freiraum (17) des Schlüsselbehälters (10) einschiebbar (55) ist und in ihrer Einschublage auch die Oberöffnung (52) wenigstens bereichsweise verschließt.

5.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 4, wobei der Flachschlüssel (30) zwischen seiner Ruhe- und Gebrauchslage (30.2; 30.1) im Behälter (10) verschwenkbar (29) ist,

wobei der Druckknopf (40) als Schwenklager (33) für den Flachschlüssel (30) dient und seine Federung (41) bestrebt (49) ist, den Flachschlüssel (30) in dessen Gebrauchslage (30.1) herauszuschwenken,

dadurch gekennzeichnet,

dass die Einschubrichtung (55) der Elektrokapsel (50) in den Schlüsselbehälter (10) in einer Parallelebene zur Schwenkbewegung (29) des Flachschlüssels (30) angeordnet ist.

6.) Schlüssel nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass die zum Einschub (55) der Elektrokapsel (20) dienende Seitenöffnung (53) sich an dem bezüglich des Druckknopfs (40) gegenüberliegenden Hinterende (54) des Schlüsselbehälters (10) befindet.

7.) Schlüssel nach einem oder mehreren der Ansprüche 4 bis 6, dadurch gekennzeichnet, dass die Unterschale (12) und die Elektrokapsel (20) Führungsmittel (61, 62) zum gezielten Einstecken und Verschieben (55) der Elektrokapsel (20) besitzen

und dass die Führungsmittel (61, 62) zur Seitenöffnung (53) der Unterschale (12) hin weisen.

8.) Schlüssel nach Anspruch 7, dadurch gekennzeichnet, dass die Führungsmittel (61, 62) in der Unterschale (12) zur Oberöffnung (52) des Schlüsselbehälters (10) hin hinterschnitten sind.

9.) Schlüssel nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass die Führungsmittel aus mindestens einer, vorzugsweise aber zwei Führungsleisten (61) bestehen, die ein schwalbenschwanzförmiges Profil besitzen,

und dass die Elektrokapsel (20) dazu angepasste Führungsnuten (62) besitzt.

10.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die Einstecklage der Elektrokapsel (20) im Schlüsselbehälter (10) durch Anschlagmittel begrenzt und durch Rastmittel gesichert ist.

11.) Schlüssel nach Anspruch 11, dadurch gekennzeichnet, dass die Ausnehmung (57) den Lappen (56) durchsetzt

und dass der Druckknopf (40) in der Einschublage der Elektrokapsel (20) mit seinem Betätigungsende zu Betätigungszwecken aus der Lappenoberseite herausragt.

12.) Schlüssel nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass am Druckknopf (40) und an seiner Aufnahme (44) im Schlüsselbehälter (10) Steuermittel (41, 48, 38, 37) angeordnet sind, die den Druckknopf (40) während der Schwenkbewegung (29) des Flachschlüssels (30) zwischen der Gebrauchs- und Ruhelage (30.1; 30.2) in einer axial eingedrückten Position halten,

und dass der Druckknopf (40) in dieser Eindrückposition aus der Ausnehmung (57) im Lappen (56) ausgefahren ist und die Elektrokapsel (20) freigibt.

13.) Schlüssel nach einem oder mehreren der Ansprüche 11 bis 13, dadurch gekennzeichnet, dass der Lappen (56) im Bereich seiner Ausnehmung (57) eine Membran aufweist, welche in Einschublage der Elektrokapsel (20) den Druckknopf (40) nach oben überdeckt,

und dass diese Membran die manuelle Betätigungsstelle für den Druckknopf (40) bildet.

14.) Schlüssel nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die Membran mit dem Lappen (56) der Elektrokapsel (20) einstückig ausgebildet ist.

15.) Schlüssel nach Anspruch 14 oder 15, dadurch gekennzeichnet, dass die zur Betätigung des Druckknopfs (40) dienende Membran mit weiteren membranartigen Betätigungsstellen (60) im Schlüsselgehäuse (10) bzw. an der im Einsteckfall sichtbar bleibenden Außenfläche der Elektrokapsel (20) kombiniert ist, die zum Wirksamsetzen der elektronischen Bauteile (21) in der Elektrokapsel (20) dienen.

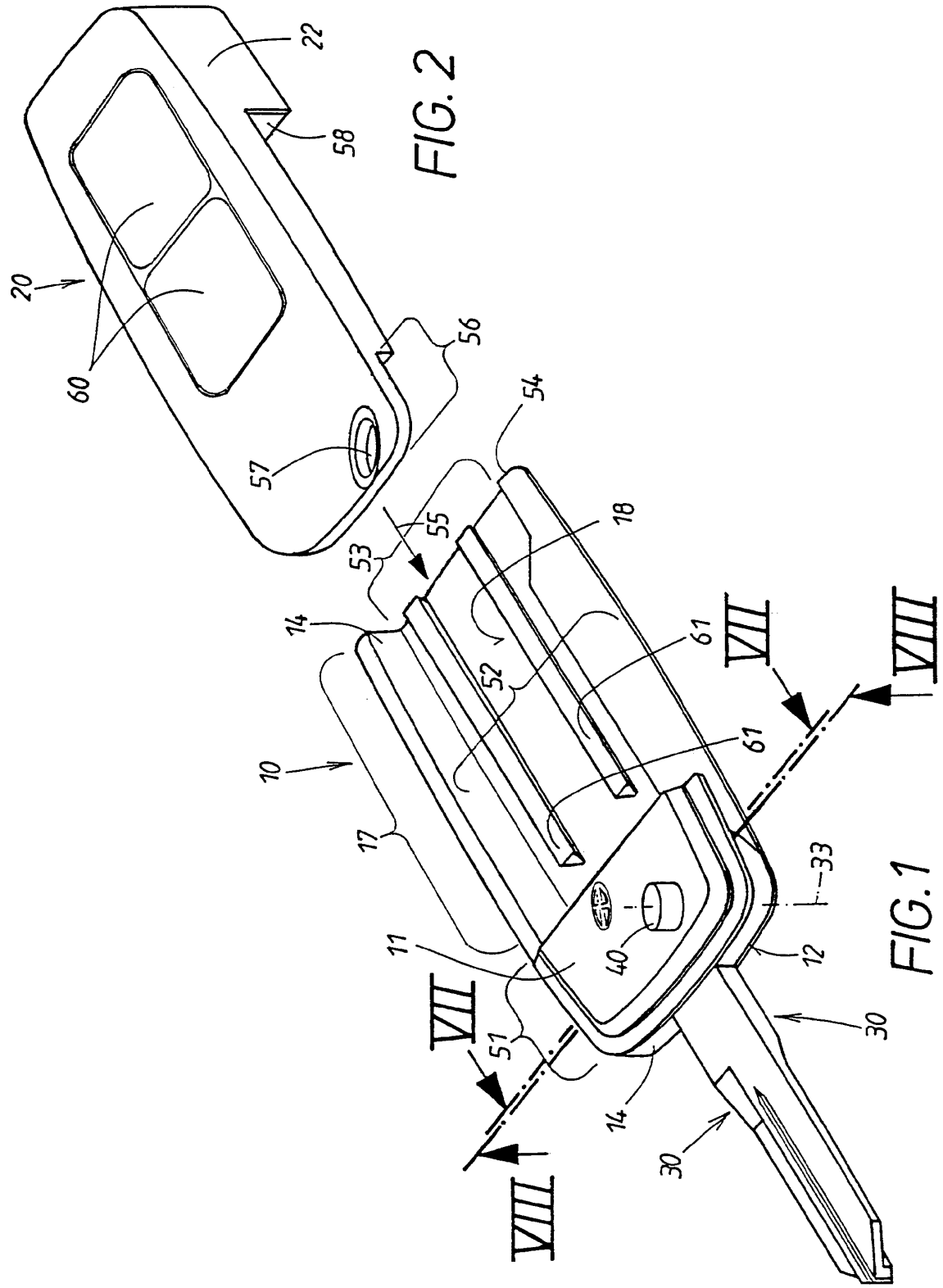


FIG. 2

FIG. 1

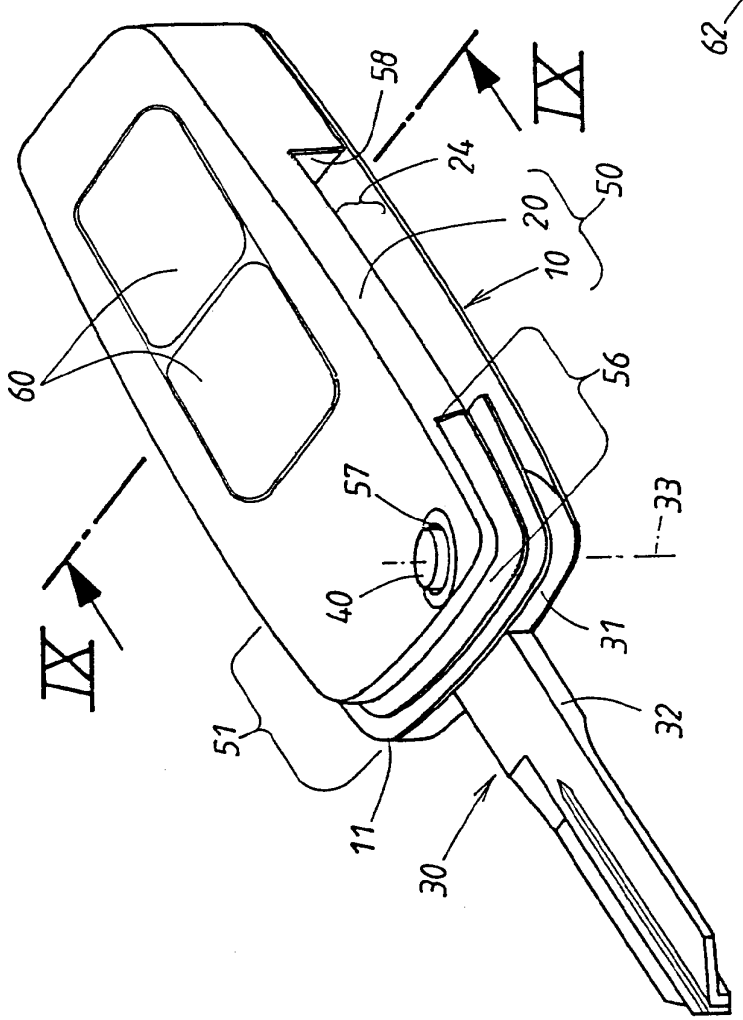

IX
IX
58
24
20
10
50
60
56
57
33
40
31
51
32
11
30

FIG. 3

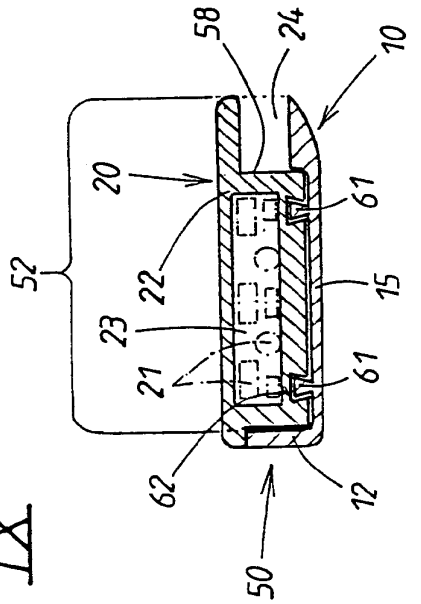

58
24
10
20
61
52
22
15
23
21
61
62
12
50

FIG. 9

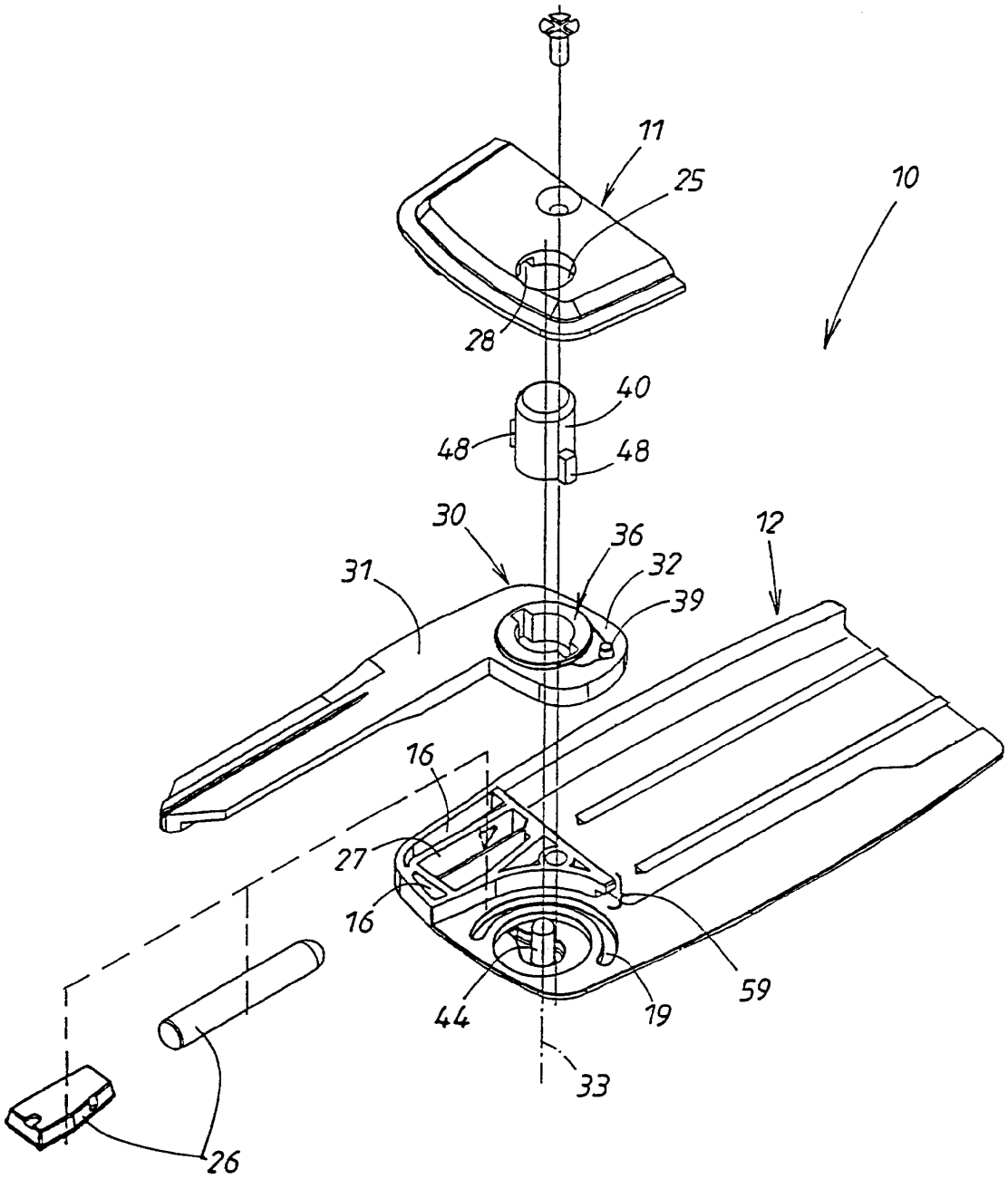


FIG. 4

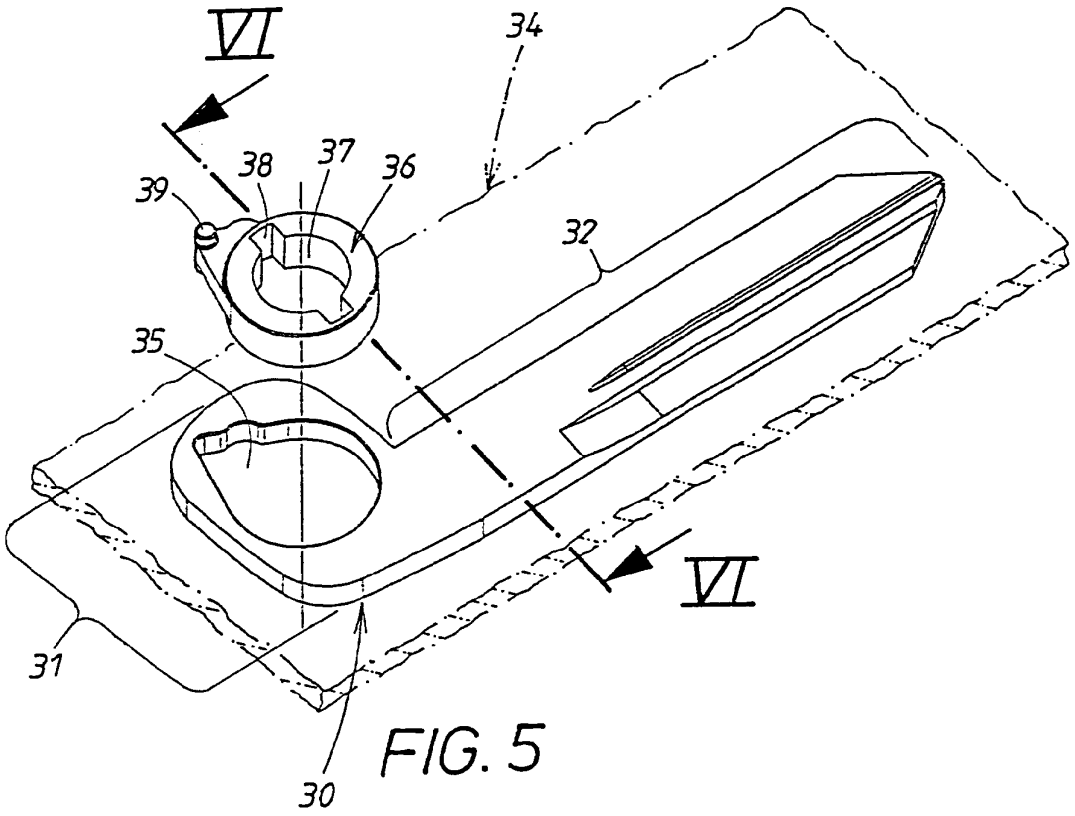


FIG. 5

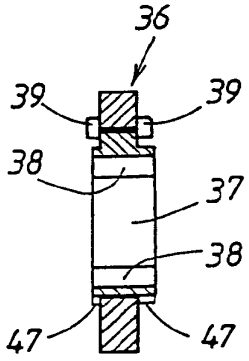


FIG. 6

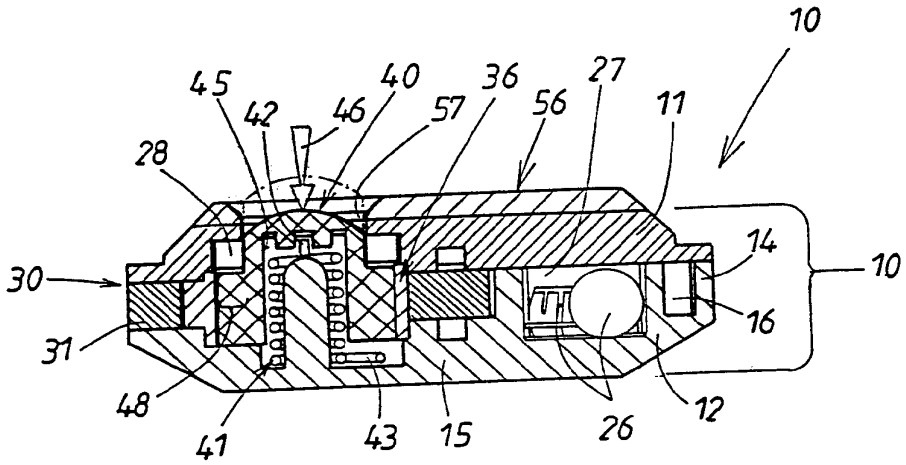

10
45
42
46
40
57
36
56
27
11
28
14
10
30
16
31
48
41
43
15
26
12

FIG. 7

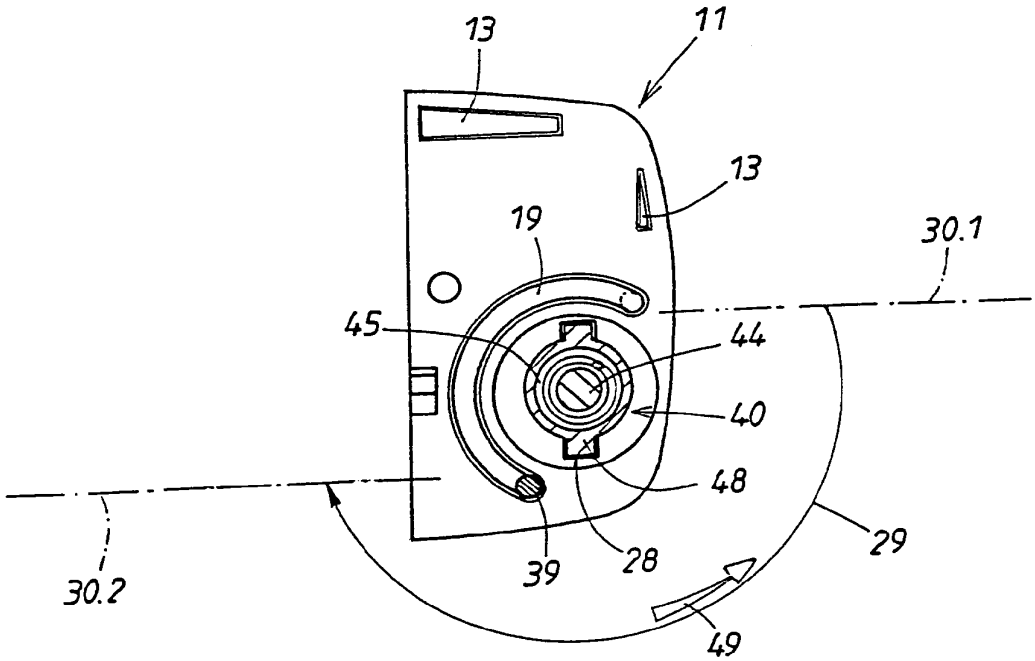

13
11
13
19
30.1
45
44
40
48
29
30.2
39
28
49

FIG. 8

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/EP 00/12431

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00 E05B19/00 E05B19/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B A45C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 39 02 537 A (DAIMLER BENZ AG ;HUELSBECK & FUERST (DE)) 9 August 1990 (1990-08-09) cited in the application the whole document	1
A	EP 0 267 429 A (SIEMENS AG) 18 May 1988 (1988-05-18) cited in the application the whole document	1
A	US 4 726 205 A (ALLERDIST HEINZ ET AL) 23 February 1988 (1988-02-23) column 1, line 31 - line 62 column 2, line 20 - line 38; figure	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 March 2001	26/03/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pieracci, A

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ional Application No
PCT/EP 00/12431

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3902537 A	09-08-1990	NONE	
EP 0267429 A	18-05-1988	DE 3769923 D	13-06-1991
		JP 63110377 A	14-05-1988
		US 4888970 A	26-12-1989
US 4726205 A	23-02-1988	DE 3509579 A	18-09-1986
		DE 3678983 D	06-06-1991
		EP 0195195 A	24-09-1986
		JP 61229079 A	13-10-1986

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Int .tionales Aktenzeichen
PCT/EP 00/12431

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00 E05B19/00 E05B19/04

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B A45C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 39 02 537 A (DAIMLER BENZ AG ;HUELSBECK & FUERST (DE)) 9. August 1990 (1990-08-09) in der Anmeldung erwähnt das ganze Dokument ---	1
A	EP 0 267 429 A (SIEMENS AG) 18. Mai 1988 (1988-05-18) in der Anmeldung erwähnt das ganze Dokument ---	1
A	US 4 726 205 A (ALLERDIST HEINZ ET AL) 23. Februar 1988 (1988-02-23) Spalte 1, Zeile 31 - Zeile 62 Spalte 2, Zeile 20 - Zeile 38; Abbildung -----	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
16. März 2001	26/03/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Pieracci, A

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inte ..ionales Aktenzeichen
PCT/EP 00/12431

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
DE 3902537	A	09-08-1990	KEINE		
EP 0267429	A	18-05-1988	DE	3769923 D	13-06-1991
			JP	63110377 A	14-05-1988
			US	4888970 A	26-12-1989
US 4726205	A	23-02-1988	DE	3509579 A	18-09-1986
			DE	3678983 D	06-06-1991
			EP	0195195 A	24-09-1986
			JP	61229079 A	13-10-1986

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 August 2001 (23.08.2001)

PCT

(10) International Publication Number
WO 01/61692 A1

(51) International Patent Classification[7]: G11B 11/00

(21) International Application Number: PCT/SG00/00029

(22) International Filing Date: 21 February 2000 (21.02.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TREK TECHNOLOGY (SINGAPORE) PTE LTD** [SG/SG]; 30 Loyang Way #07-13/14/15, Loyang Industrial Estate, Singapore 508769 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CHENG, Chong, Seng** [SG/SG]; 129 Loyang Rise, Singapore 507472 (SG).

(74) Agent: **MCCALLUM, Graeme, David**; Lloyd Wise, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).

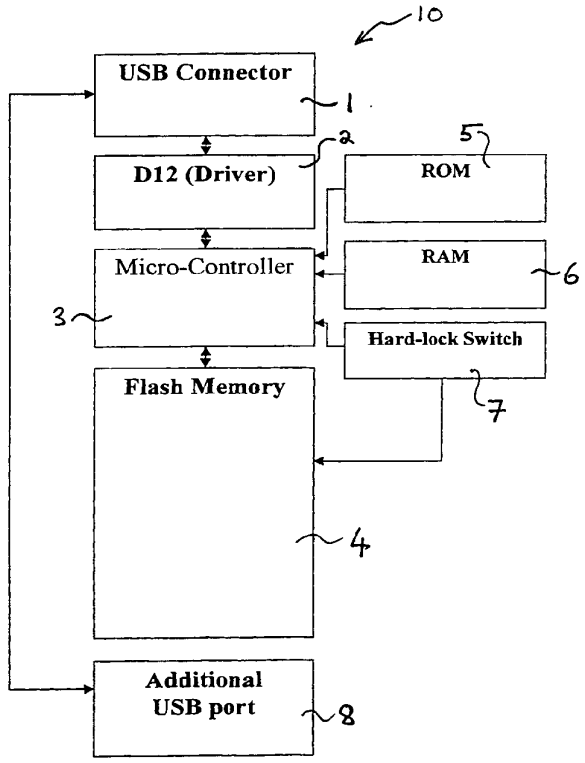
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, 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, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: A PORTABLE DATA STORAGE DEVICE



(57) Abstract: A portable data storage device (10) includes a universal serial bus (USB) coupling device (1) and an interface device (2) is coupled to the USB coupling device (1). The portable data storage device (10) also includes a memory control device (3) and a non-volatile solid-state memory device (4). The memory control device (3) is coupled between the interface device (2) and the memory device (4) to control the flow of data from the memory device (4) to the USB coupling device (1).

WO 01/61692 A1

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.

A Portable Data Storage Device

The invention relates to a portable data storage device, and in particular, a portable data storage device for a computer.

Conventional data storage devices generally fall into two categories. The first category is electronic, solid-state memory devices such as read only memory (ROM) and random access memory (RAM). These memory devices are generally fitted within the computer. They are not intended to be removable or portable so that they may be used on different computers, for example, to permit the transfer of data from one computer to another computer.

The second type of device is surface based data storage devices in which data is stored, typically, on the surface of a disk or tape. Examples of surface storage devices are magnetic disks and CD ROMs. Such data storage devices require a mechanical drive mechanism to be installed in or coupled to the computer to permit the data on the storage device to be read by the computer. In addition, such memory devices are limited by the surface area of the storage device, and the combination of the storage device and the drive mechanism for reading data from the storage device is generally bulky and/or delicate due to the moving parts that are required within the drive mechanism and/or storage device.

In accordance with the present invention, there is provided a portable data storage device comprising a coupling device for coupling to a computer serial

bus, an interface device coupled to the coupling device, a memory control device and a non-volatile solid-state memory device; the memory control device being coupled between the interface device and the memory device to control the flow of data from the memory device to the coupling device.

An advantage of the invention is that by providing a portable data storage device comprising a coupling device with an interface device, memory control device and a non-volatile solid-state memory device, it is possible to provide a portable data storage device which may be coupled to a computer having a serial bus port and which does not include moving parts or require a mechanical drive mechanism to read the data from the data storage device.

Preferably, the non-volatile solid-state memory device may be a read/write memory device, such as a flash memory device.

Preferably, where the memory device is a read/write memory device, the memory control device controls the flow of data to and from the memory device.

Typically, the data storage device further comprises a manually operated switch movable between a first position in which writing of data to the memory device is enabled, and a second position in which writing of data to the memory device is prevented.

Preferably, the memory control device may include a read only memory which stores a program to control the operation of the memory control device. Preferably, the memory control device is a micro-controller.

Typically, the interface device comprises a universal serial bus (USB) driver to convert data between a USB format and a PC format, and the coupling device comprises a USB coupling deivce.

Alternatively, the interface device comprises a driver for IEEE 1394 (Firewire) protocol, and the coupling device comprises a Firewire coupling device.

An example of a data storage device in accordance with the invention will now be described to the accompanying drawings, in which:

Figure 1 is a schematic block diagram of a portable data storage device;

Figure 2 is a flow diagram showing the initial setup of the data storage device by a software supplier;

Figure 3 is a flow diagram showing the initial setup of the data storage device by an end user; and

Figure 4 is a flow diagram showing operation of the data storage device.

Figure 1 shows a data storage device 10 which includes a USB plug 1 which is coupled to a USB interface device 2. The USB interface device 2 is coupled to a micro-controller 3 which is coupled to a flash memory 4. The micro-controller

3 includes a read only memory (ROM) 5 which stores a program to control the operation of the micro-controller 3.

The operations performed by the micro-controller 3 include comparing passwords entered by a user with a corresponding password stored in the flash memory 4 to determine whether the user is authorised to access the contents of the flash memory 4. The program stored in the ROM 5 also controls the data flow to and from the flash memory 4 and can also detect whether the computer to which the memory device 1 is coupled has installed software programs which correspond to passwords stored in the flash memory 4. The micro-controller 3 can automatically retrieve passwords from the installed software to compare with passwords stored in the flash memory to verify that a user of the computer is authorised to access and run the software. In addition, the program stored in the ROM 5 also permits the setting of a password in the flash memory by a software supplier to correspond to the password contained in software supplied to a user. Typically, the password may correspond to the serial number of the software.

The flash memory 4 is typically divided into a number of different sections or zones. Typically, the flash memory is divided into two zones and each zone has a unique password. If the data storage device 10 is supplied with packaged software, the software serial number can be set in one zone to be the password to permit a user to access and use the software. The other zone, which can be used typically for storing a user's data, may have a separate password which is set by the user. Typically, the passwords are stored in a secure location of the

flash memory in an encrypted form. The encryption, decryption, data flow control and USB protocol are all managed by the micro-controller 3.

The micro-controller 3 also includes a random access memory (RAM) 6 which is a temporary storage area to permit functioning of the micro-controller 3. In addition, a manual switch 7 is coupled between the flash memory 4 and the micro-controller 3. The manual switch 7 is movable between a first position in which a user may write data to the flash memory 4 and a second position in which data is prevented from being written to the flash memory 4.

The device 10 also includes a USB socket 8 that is coupled directly to the USB plug 1 and permits other USB devices to be coupled to the USB via the device 10. For example, if a user wishes to increase memory space, a USB plug 1 of a second memory device 10 may be connected to the USB socket 8.

Figure 2 is a flow diagram showing the set up procedure for the device 10 for a software supplier when the software supplier intends to supply the device as an authentication device for the software. Firstly, the plug 1 of the device 10 is plugged into 20 to a USB socket on a computer. After the device 10 has been plugged into the USB socket on the computer, a communication is established 21 between the computer and the device 10. The software supplier has pre-installed installation software on the computer which is run by the operator. From the pre-installed software, the operator selects password set up installation 22, in response to which the pre-installed software requests the operator to enter a password or serial number corresponding to the software

with which the device 10 is to be supplied. The password or serial number is then encrypted 26 and stored 27 in the flash memory 4.

Figure 3 is a flow diagram showing the initial set-up of a password for zone 2 of the flash memory 4 by an end user. The device 10 is typically supplied with driver software that is loaded by the user onto the computer prior to set-up of the device. To set-up the password for zone 2 the user plugs in 20 the device 10 into a USB port on the computer and communication 21 is established between the computer and the device 10. The user then runs the driver software and the driver software enters a password installation set-up mode 23 for zone 2. The user then enters 28 a password that they wish to use to prevent unauthorised access to zone 2 of the flash memory 4. The password entered is then encrypted 29 and stored 30 in the flash memory 4.

After an end user has performed the initial password set up procedure described above and shown in Figure 3, when a user plugs in 20 the device 10 to a USB port on a computer, the computer will establish a communication 21 with the device 10 and firstly, checks 33 an installation status flag stored in the flash memory 4 (see Figure 4). If the status flag is "Y", the device 10 outputs 34 an "OK" flag to the computer. The micro-controller 3 the instructs the computer to issue a request 35 to the user to select the zone they wish to enter. If the status flag is "N", the device does not output an "OK" flag to the computer, and goes straight to step 35. In response to the request 35 for zone selection, the user selects 36 either zone 1 or zone 2.

If zone 1 is selected, the device 10 assumes that the user wishes to install software on the computer which is stored in the flash memory 4 and requests 37 the appropriate password for confirmation that the user is authorised to install the software. The micro-controller 3 receives the password entered by the user, retrieves the zone 1 password stored in the flash memory 4, decrypts the zone 1 password and compares it with the password entered by the user to authenticate 38 whether the user is authorised to install the software. If the passwords do not match, the device 10 prompts the computer to request 37 the user to enter the password again.

If the password entered by the user matches the password stored in the flash memory 4, the micro-controller 3 starts 39 the software installation from the flash memory 4 to the computer. In order to install software, the computer sends 40 a read/write command in USB format to the micro-controller 3 for data, the micro-controller 3 retrieves the requested data from the flash memory 4 and sends 41 the data to the driver 2. The driver 2 converts 42 the data to PC format and outputs the data to the computer through the USB plug 1. The micro-controller 3 then checks 43 whether the software installation is complete. If the operation is not complete, the operation returns to step 40. If the installation of the software is complete, the status flag stored in the flash memory 4 is changed to "Y" and the device 10 may then be removed 45 from the USB socket on the computer.

If a user selects zone 2, the micro-controller 3 sends a command to the computer to request 46 the user to enter the password for zone 2. When the

user enters the password, the computer sends the password to the micro-controller 3. The micro-controller 3 retrieves the password for zone 2 from the flash memory 4, decrypts 47 the password and compares it with the password entered by the user. If the password entered by the user is incorrect, the operation returns to step 46 and the computer requests 46 the user for the password again.

If the password entered by the user is correct, the user has access to zone 2 of the flash memory 4 to read data from the flash memory 4 and to write data to the flash memory 4. However, data can only be written to the flash memory 4 if the manual switch 7 is in the position to permit data to be written to the flash memory 4. In order to read or write data from or to the flash memory 4 a read or write command is sent 48 by the computer in USB format to the micro-controller 3. In response to the read or write command the micro-controller 3 either retrieves 49 data from the flash memory 4 and sends it to the driver 2 for conversion 50 to PC format and then to be output to the computer or receives data from the driver to write it to the flash memory 4.

The micro-controller 3 then determines 51 whether the read or write operation is complete. If the operation is not complete it returns to step 48. If the operation is complete the operation terminates 52.

The device 10 described above is for coupling to a universal serial bus (USB). However, the plug 1, the interface device 2 and socket 8 could be for use with any appropriate computer serial bus. For example, the device 10 could be

modified for use with IEEE 1394 (Firewire) protocol by substituting the USB plug 1, USB interface device 2 and socket 8 with a Firewire protocol compatible plug, interface device and socket respectively.

An advantage of the device 10 described above is that it provides a portable data storage device for a computer which does not require a mechanical operated reading/writing device. In addition, the device 10 has no moving parts. This enables to data storage device 10 to be more compact than conventional portable data storage devices.

CLAIMS

1. A portable data storage device comprising a coupling device for coupling to a computer serial bus, an interface device coupled to the coupling device, a memory control device and a non-volatile solid-state memory device; the memory control device being coupled between the interface device and the memory device to control the flow of data from the memory device to the coupling device.

2. A device according to claim 1, wherein the non-volatile solid-state memory device is a read/write memory device.

3. A device according to claim 2, wherein the read/write memory device is a flash memory device.

4. A device according to claim 2 or claim 3, wherein the memory control device controls the flow of data to and from the memory device.

5. A device according to any of claims 2 to 4, further comprising a manually operated switch movable between a first position in which writing of data to the memory device is enabled, and a second position in which writing of data to the memory device is prevented.

6. A device according to any of the preceding claims, wherein the memory control device comprises a micro-controller.

7. A device according to any of the preceding claims, wherein the coupling device comprises a universal serial bus coupling device and the interface device comprises a USB driver.

8. A device according to any of the preceding claims, wherein the coupling device comprises an IEEE 1394 (Firewire) protocol coupling device and the interface device is a Firewire protocol driver.

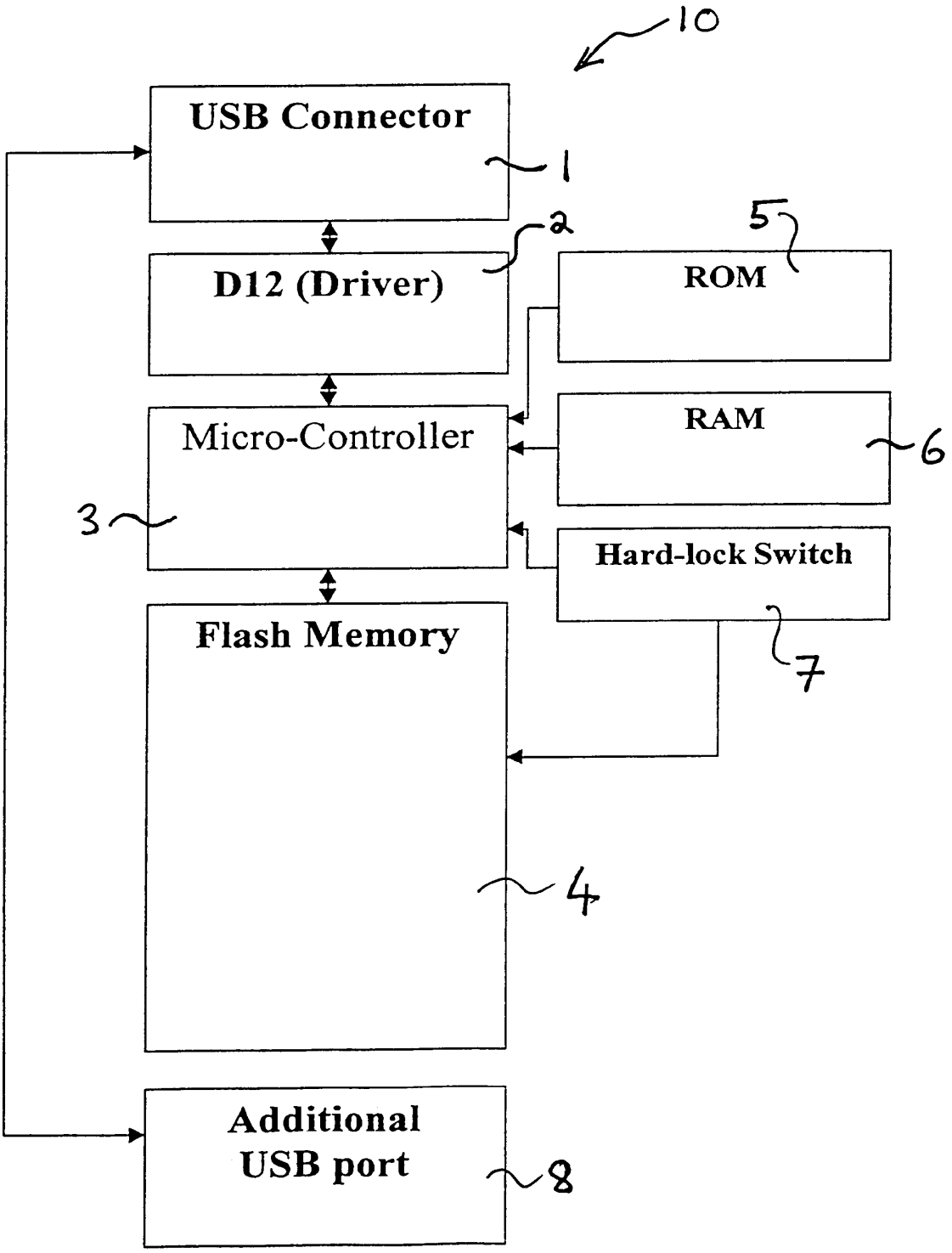

10
USB Connector
1
2
D12 (Driver)
5
ROM
RAM
6
Micro-Controller
3
Hard-lock Switch
7
Flash Memory
4
Additional
USB port
8

Figure 1

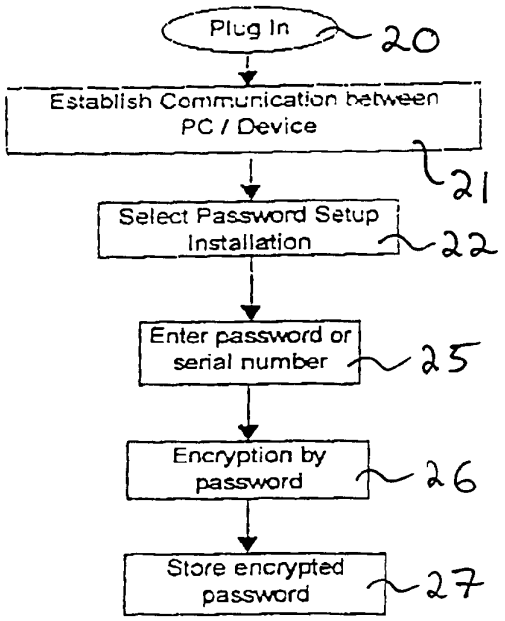


Figure 2

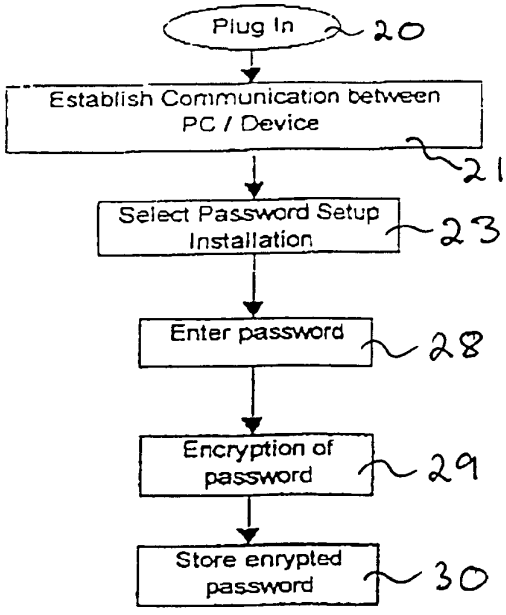


Figure 3

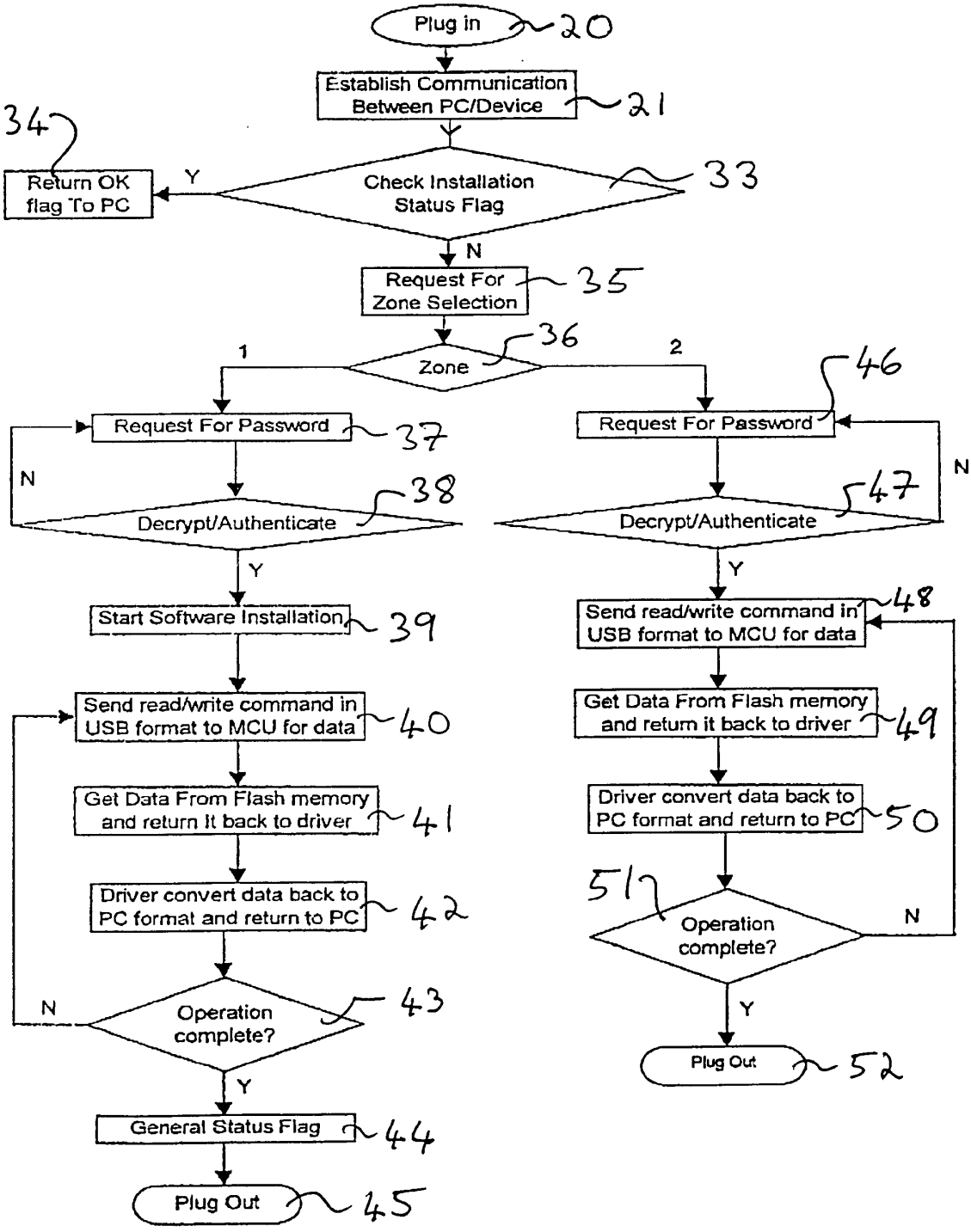

Plug in
20
Establish Communication Between PC/Device
21
34
Return OK flag To PC
Y
Check Installation Status Flag
33
N
Request For Zone Selection
35
Zone
36
1
2
Request For Password
37
N
Decrypt/Authenticate
38
Y
Start Software Installation
39
Send read/write command in USB format to MCU for data
40
Get Data From Flash memory and return it back to driver
41
Driver convert data back to PC format and return to PC
42
N
Operation complete?
43
Y
General Status Flag
44
Plug Out
45
Request For Password
46
N
Decrypt/Authenticate
47
Y
Send read/write command in USB format to MCU for data
48
Get Data From Flash memory and return it back to driver
49
Driver convert data back to PC format and return to PC
50
51
Operation complete?
N
Y
Plug Out
52

Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 00/00029

CLASSIFICATION OF SUBJECT MATTER

IPC[7]: G11B 11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: G11B 11/00, 02,05

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

G06F 3/00, 12/00, 12/06

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6016530 A (AUCLAIR et al.) 18 January 2000 (18.01.00)	1
P,A	US 6058441 A (SHU) 2 May 2000 (02.05.00)	1
A	US 5760986 A (MOREHOUSE et al.) 2 June 1998 (02.06.98)	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed

„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 March 2001 (24.03.2001)	12 April 2001 (12.04.2001)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Authorized officer GRÖSSING Telephone No. 1/53424/386

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG 00/00029

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
US	A	5760986	0 :-06-1998	EP	A1	614564	14-09-1994
				EP	A4	614564	19-07-1995
				US	A	5379171	03-01-1995
				WO	A1	9306594	01-04-1993
				US	A	5835303	10-11-1998
				US	A	5579189	26-11-1996
				US	A	5592349	07-01-1997
				US	A	5694267	02-12-1997
				US	A	5867340	02-02-1999
US	A	6016530	18-01-2000	US	A	5778418	07-07-1998
US	A	6058441	02-05-2000			none	

Electronic Acknowledgement Receipt

EFS ID:	2039867
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	02-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	12:59:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO200065180.pdf	540410 8cf965fb08eae4bb420664bb0fb5e2909e8c35c0	no	14
Warnings:					

Information:					
2	Foreign Reference	WO200075755.pdf	1004753 5b39ddf70484e3cbf3a0367ed17619bb3af656d8	no	40
Warnings:					
Information:					
3	Foreign Reference	WO200114179.pdf	2071078 1b545b9e4532416fb7bd7e1da53b6b2ee7600cdc	no	56
Warnings:					
Information:					
4	Foreign Reference	WO200138673.pdf	1396174 fa98b9df354ad9e4f260d80223ab1d9763bc0759	no	38
Warnings:					
Information:					
5	Foreign Reference	WO200139102.pdf	784012 a3d93872302d95a7e3bf65451476ca42a633bdaf	no	14
Warnings:					
Information:					
6	Foreign Reference	WO200148339.pdf	1049894 bd6d4926d22f7fe5f10238a686ef426b31a515fc	no	27
Warnings:					
Information:					
7	Foreign Reference	WO200148342.pdf	1098879 63641981dd430b53847b680894dc6cd83c4a2d42	no	30
Warnings:					
Information:					
8	Foreign Reference	WO200161692.pdf	531955 41769f9721b22c85b15dac2ca8bde315e48f4990	no	18
Warnings:					
Information:					
		Total Files Size (in bytes):	8477155		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. November 2001 (22.11.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/88693 A2

(51) Internationale Patentklassifikation[7]: G06F 7/72

(21) Internationales Aktenzeichen: PCT/EP01/05532

(22) Internationales Anmeldedatum:
15. Mai 2001 (15.05.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
100 24 325.8 17. Mai 2000 (17.05.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **SEYSEN, Martin** [DE/DE]; Schleissheimer Strasse 339, 80809 München (DE).

(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, 80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, 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.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

WO 01/88693 A2

(54) Title: CRYPTOGRAPHIC METHOD AND CRYPTOGRAPHIC DEVICE

(54) Bezeichnung: KRYPTOGRAPHISCHES VERFAHREN UND KRYPTOGRAPHISCHE VORRICHTUNG

(57) Abstract: The invention relates to a cryptographic method comprising at least one arithmetic step which contains a modular exponentiation E, according to the equation $E=x^d \pmod{p.q}$, comprising a first prime factor p, a second prime factor q, an exponent d and a number x. According to said method, the modular exponentiation E is calculated according to the Chinese Remainder Theorem.

(57) Zusammenfassung: Die Erfindung betrifft ein kryptographisches Verfahren mit mindestens einem eine modulare Exponentiation E gemäss $E=x^d \pmod{p \cdot q}$ enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Zahl x, wobei die modulare Exponentiation E gemäss dem Chinesischen Restwertsatz berechnet wird.

Kryptographisches Verfahren und kryptographische Vorrichtung

Kryptographische Verfahren in Gestalt von Verschlüsselungs- und Signaturverfahren erfreuen sich insbesondere durch die steigende Bedeutung des elektronischen Geschäftsverkehres einer stetig wachsenden Verbreitung. Sie werden in der Regel mittels elektronischer Vorrichtungen implementiert, die beispielsweise einen programmierbaren universellen Microkontroller oder auch eine spezialisierte elektronische Schaltung etwa in Gestalt eines ASIC beinhalten können. Eine besonders interessante Form kryptographischer Vorrichtungen ist die Chipkarte, da sich in ihr bei zweckdienlicher technischer Ausgestaltung geheime Schlüsseldaten gegen unbefugten Zugriff schützen lassen. Ein ständiges Bemühen gilt dabei sowohl der Verbesserung der Ausführungsgeschwindigkeit der kryptographischen Verfahren als auch deren Sicherung gegen alle denkbaren Arten von Angriffen. Die Erfindung eignet sich insbesondere für den Einsatz im Zusammenhang mit Chipkarten, ist aber in keiner Weise darauf beschränkt. Sie ist vielmehr im Zusammenhang mit allen Arten von kryptographischen Vorrichtungen implementierbar.

Bei einer Reihe bekannter kryptographischer Verfahren ist es erforderlich, eine modulare Exponentiation gemäß der Gleichung

$$E = x^d \pmod N = x^d \pmod{p \cdot q} \qquad (1)$$

durchzuführen, wobei p und q Primzahlen sind. Ein besonders bedeutendes kryptographisches Verfahren, welches einen modularen Exponentiationsschritt beinhaltet, ist das beispielsweise aus Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone, "Handbook of Applied Cryptography", Boca Raton: CRC Press, 1997, Seiten 285 bis 291, bekannte RSA-Verfahren. Die Verwendung der modularen Exponentiation ist jedoch nicht auf das RSA-Verfahren beschränkt, sondern umfaßt beispielsweise auch aus Menezes et al., a.a.O., Seiten 438 bis 442, bekannte Rabin-Signaturen und das aus Mene-

zes et al., a.a.O., Seite 408 bis 410, bekannte Fiat-Shamir'sche Identifikationsschema.

Die Sicherheit von kryptographischen Verfahren, die die modulare Exponentiation einbeziehen, ist regelmäßig abhängig von der Schwierigkeit, die Zahl N aus Gleichung (1) in ihre Primfaktoren p und q zerlegen zu können. Dieses Problem ist nur für hinreichend große Werte N von ausreichender Komplexität, so daß einerseits N möglichst groß gewählt werden sollte. Der Rechenaufwand zur Berechnung von Werten mittels modularer Exponentiation gemäß Gleichung (1) steigt andererseits monoton mit der Größenordnung von N, so daß es unter dem Gesichtspunkt der praktischen Anwendbarkeit wünschenswert wäre, trotz großer Werte von N den Rechenzeitaufwand auf akzeptable Werte beschränken zu können.

Es ist bekannt, durch Anwendung des sog. "Chinesischen Restwertsatzes" die Rechengeschwindigkeit um einen Faktor 4 erhöhen zu können, wodurch beispielsweise bei gleicher Rechenzeit größere Werte N zugelassen werden können. Statt unmittelbar die Gleichung (1) auszuwerten, wird eine Umformung vorgenommen gemäß

$$E = x^d \pmod{p \cdot q} = aE_1 + bE_2 \pmod{N} \qquad (2)$$

mit

$$E_1 = x^d \pmod{p} \qquad (3)$$

$$E_2 = x^d \pmod{q} \qquad (4)$$

Eine Folge der Anwendung des Chinesischen Restwertsatzes besteht darin, daß die modulare Exponentiation nicht mehr modulo N, also modulo derjenigen Zahl, die ihre eigene Primfaktorzerlegung noch in sich verbirgt, sondern nacheinander in einem ersten Teilschritt modulo p und in einem zweiten Teilschritt modulo q erfolgt, d.h. die Kenntnis der geheimzuhaltenden

Primfaktorzerlegung $n = p \cdot q$ wird bei dieser Rechenvorschrift vorausgesetzt und führt zu einer Aufteilung des Gesamtrechenprozesses in einen ersten Rechenschritt (3), in den der erste Primfaktor wesentlich eingeht, und einen zweiten Rechenschritt (4), in den der zweite Primfaktor wesentlich eingeht. Der Vorteil hierbei liegt darin, daß der Exponent d in Gleichung (1) modulo $\phi(p \cdot q)$ definiert sein muß, wohingegen die Exponenten in Gleichung (2) lediglich modulo $\phi(p)$ bzw. $\phi(q)$ definiert sein müssen, wobei mit ϕ die Euler'sche Funktion notiert ist.

Interessanterweise ist nun in der letzten Zeit ein Angriffsschema auf solche kryptographischen Verfahren, die die modulare Exponentiation nutzen, bekannt geworden, bei dem durch einen geeigneten artifiziellen Eingriff in den ansonsten störungsfreien Rechenablauf aus dem fehlerhaften Ergebnis einer gestörten modularen Exponentiation die Information über die Primfaktorzerlegung von N zurückgewonnen werden kann, sofern die konkrete Implementation von dem Chinesischen Restwertsatz gemäß den Gleichungen (2) bis (4) Gebrauch macht. Dieser als "Bellcore-Angriff" bekannte Versuch ist beispielsweise in Dan Boneh, Richard A. DeMillo und Richard J. Lipton: "On the importance of checking Cryptographic Protocols for Faults", Advances in Cryptology -EUROCRYPT, 97, Lecture Notes in Computer Science 1233, Berlin: Springer, 1997 beschrieben. Eine Verschlüsselungseinrichtung wird durch physikalische Eingriffe wie beispielsweise Übertaktung, zu hohe Betriebsspannung oder Bestrahlung manipuliert, so daß mit einer gewissen, nicht zu großen Wahrscheinlichkeit Rechenfehler bei der Ausführung der modularen Exponentiation nach dem Chinesischen Restwertsatz auftreten. Wenn ein Rechenfehler nur bei einem der beiden Terme in Gleichung (2) auftritt, können die beiden Primfaktoren p und q aus dem fehlerbehafteten Exponentiationsergebnis rekonstruiert werden.

Die aus dieser Verletzlichkeit der mittels des Chinesischen Restwertsatzes implementierten modularen Exponentiation zu ziehende Konsequenz besteht darin, das Ergebnis des Rechenvorganges zuerst auf seine Korrektheit zu prüfen, bevor es weiterverarbeitet, insbesondere aber bevor es in irgend einer Form, etwa in Gestalt einer Signatur, ausgegeben wird.

Ein triviales Gegenmittel gegen den "Bellcore-Angriff" besteht darin, diese Korrektheitsprüfung dadurch zu bewerkstelligen, indem der Rechenvorgang mindestens einmal wiederholt wird. Bei zufälligen Rechenfehlern kann davon ausgegangen werden, daß das Ergebnis des ersten Rechenganges von demjenigen der Kontrollrechengänge abweicht. Der wesentliche Nachteil dieses Ansatzes besteht darin, daß sich die Rechenzeit bereits bei einer Kontrollrechnung verdoppelt.

Aus der Druckschrift WO-A1-98/52319 ist insbesondere ein Verfahren zum Schutz von eine modulare Exponentiation nach dem Chinesischen Restwertsatz ausführenden Rechenoperationen gegen den "Bellcore-Angriff" bekannt. Dabei wird eine geheime ganz Zahl j beispielsweise im Bereich $[0, 2^k-1]$ mit $16 \leq k \leq 32$ ausgewählt. Sodann werden folgende Ausdrücke berechnet:

$$v_1 = x \pmod{j \cdot q} \tag{5}$$

$$v_2 = x \pmod{j \cdot q} \tag{6}$$

$$d_1 = d \pmod{\phi(j \cdot p)} \tag{7}$$

$$d_2 = d \pmod{\phi(j \cdot q)} \tag{8}$$

$$w_1 = v_1^{d1} \pmod{j \cdot p} \tag{9}$$

$$w_2 = v_2^{d2} \pmod{j \cdot q} \tag{10}$$

Sodann wird geprüft, ob gilt:

$$w_1 = w_2 \pmod j \tag{11}$$

Kann der Ausdrucke (11) verifiziert werden, so werden bei dem bekannten Verfahren folgende Ausdrücke berechnet:

$$y_1 = w_1 \pmod p \tag{12}$$

$$y_2 = w_2 \pmod q \tag{13}$$

woraus dann mittels des Chinesischen Restwertsatzes der Wert für

$$E = x^d \pmod N \tag{14}$$

ermittelt werden kann.

Dieses bekannte Verfahren weist gegenüber einfachen Kontrollrechengängen den Vorteil auf, daß der zusätzliche Rechenzeitaufwand wesentlich geringer ist.

Bei diesem Verfahren müssen beide Primzahlen p und q mit demselben Faktor d multipliziert werden. In der Druckschrift WO-A1-98/52319 ist ein zweites Verfahren beschrieben, welches es erlaubt, die Primzahlen p und q mit verschiedenen Faktoren r und s zu multiplizieren. Hierbei sind jedoch für die Kontrollrechnung zwei weitere Exponentiationen möglich.

Aufgabe der Erfindung ist es, ein kryptographisches Verfahren bzw. eine kryptographische Vorrichtung anzugeben, bei dem bzw. bei der unter Beibehaltung oder Erhöhung der Sicherheit Rechenoperationen oder Rechenzeit eingespart werden kann.

Diese Aufgabe wird erfindungsgemäß gelöst durch ein kryptographisches Verfahren mit den in Anspruch 1 oder 2 angegebenen Merkmalen als auch durch eine kryptographische Vorrichtung mit den in Anspruch 13 oder 14 angegebenen Merkmalen.

Den abhängigen Ansprüchen 3 bis 12 sowie 15 bis 24 sind vorteilhafte Weiterbildungen entnehmbar.

Wie weiter unten erwähnt wird, ist es auf bestimmten Rechenwerken vorteilhaft, wenn ein Modulus bei der modularen Exponentiation viele führende binäre Einsen besitzt, so daß verschiedene Faktoren r und s hier einen gewissen Vorteil bedeuten. Ferner gibt es für die modulare Exponentiation optimierte Rechenwerke, wobei aber allein der Datentransfer von der Zentraleinheit in das optimierte Rechenwerk für die Exponentiation einen beträchtlichen Verwaltungsaufwand verursacht. Die vorliegende Erfindung spart gegenüber dem oben beschriebenen Verfahren bei verschiedenen Faktoren r und s eine Exponentiation ein.

Erfindungsgemäß werden zwei ganze Zahlen r und s beispielsweise im Bereich $[0, 2^k\text{-}1]$ mit $16 \leq k \leq 32$ ausgewählt, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, wobei kgV(r,s) das kleinste gemeinsame Vielfache von r und s angibt, und $\phi()$ die Euler'sche Funktion darstellt. Sodann werden folgende Ausdrükke berechnet:

$$x_1 = x \pmod{p \cdot r} \quad (15)$$

$$x_2 = x \pmod{q \cdot s} \quad (16)$$

$$d\_1 = d \pmod{\phi(p \cdot r)} \quad (15)$$

$$d\_2 = d \pmod{\phi(q \cdot s)} \quad (16)$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r} \quad (15)$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s} \quad (16)$$

Jetzt gilt $z_1 = x^d \pmod{p \cdot r}$ und $z_2 = x^d \pmod{q \cdot s}$. Nach dem Chinesischen Restwertsatz läßt sich aus z_1 und z_2 leicht eine Zahl z berechnen mit

$$z = z_1 \pmod{p \cdot r} \; ; \; z = z_2 \pmod{q \cdot s} \; ; \; z = x^d \pmod{p \cdot q \cdot kgV(r,s)} \quad (17)$$

Die Zahlen r und s müssen erfindungsgemäß so gewählt werden, daß d teilerfremd ist zu $\phi(kgV(r,s))$. Unter diesen Umständen läßt sich mit Hilfe des erweiterten Euklid'schen Algorithmus leicht eine natürliche Zahl e finden mit

$$e \cdot d = 1 \pmod{\phi(kgV(r,s))} \quad (18)$$

Mit Hilfe von Z und e wird die Zahl C wie folgt berechnet:

$$C = z^e \pmod{kgV(r,s)} \quad (19)$$

Nach dem Satz von Euler gilt:

$$C = x^{d \cdot e} = x \pmod{kgV(r,s)} \quad (20)$$

Durch Vergleich der beiden Werte C und x modulo kgV(r,s) läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn $C \neq x \pmod{kgV(r,s)}$ festgestellt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

Bei RSA-Verfahren (ebenso wie beim Rabin'schen Signaturverfahren) ist zur Erzeugung einer digitalen Signatur oder zur Entschlüsselung eine modulare Exponentiation durchzuführen, wobei der Modulus p·q und Exponent d nur vom privaten Schlüssel abhängen. Infolgedessen können die Zahlen d, e, r und s einmal beim Einbringen des privaten Schlüssel berechnet und zur Wiederverwendung abgespeichert werden.

In einer Variante der Erfindung werden ebenfalls zwei ganze Zahlen r und s beispielsweise im Bereich $[0, 2^k\text{-}1]$ mit $16 \leq k \leq 32$ ausgewählt. Auf einem binären Rechenwerk wird empfohlen, daß die Zahlen r und s beide ungerade sind. Außerdem werden zwei feste, nicht von x abhängige Zahlen b_1 und b_2 im Intervall [1,...,r-1] bzw. [1,...,s-1] und teilerfremd zu r bzw. s gewählt. Falls r und s nicht teilerfremd sind, müssen b_1 und b_2 die zusätzliche Bedin-

gung $b_1 = b_2 \pmod{ggT(r,s)}$ erfüllen, wobei ggT(r,s) den größten gemeinsamen Teiler von r und s bezeichnet.

Nach dem Chinesischen Restsatz wird zunächst eine Zahl x_1 berechnet mit

$$x_1 = x \pmod{p}, \quad x_1 = b_1 \pmod{r} \tag{21}$$

Ebenso wird eine Zahl x_2 berechnet mit

$$x_2 = x \pmod{q}, \quad x_2 = b_2 \pmod{s} \tag{22}$$

Sodann werden folgende Ausdrücke berechnet:

$$d\_1 = d \pmod{\phi(p)} \tag{23}$$

$$d\_2 = d \pmod{\phi(q)} \tag{24}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r} \tag{25}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s} \tag{26}$$

$$C_1 = b_1^{d\_1} \pmod{\cdot r} \tag{27}$$

$$C_2 = b_2^{d\_2} \pmod{\cdot s} \tag{28}$$

Zur Einsparung von Rechenzeit können die Exponenten d_1 und d_2 in (27) bzw. (28) vor der Durchführung der Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden.

Aus (23) und (25) folgt

$$z_1 = x^d \pmod{p} \tag{29}$$

Aus (24) und (26) folgt

$$z_2 = x^d \pmod{q}. \tag{30}$$

Nach dem Chinesischen Restwertsatz läßt sich aus z_1 und z_2 leicht eine Zahl z berechnen mit

$$z = z_1 \pmod{p \cdot r}\ ;\ z = z_2 \pmod{q \cdot s}\ ; \tag{31}$$

Selbst wenn r und s nicht teilerfremd sind, existiert eine solche Zahl z wegen $z_1 = C_1 = b_1^{d\_1} = b_2^{d\_2} = C_2 = z_2 \pmod{ggT(r,s)}$. Da p und q teilerfremd sind, folgt aus (29), (30) und (31):

$$z = x^d \pmod{p \cdot q}. \tag{32}$$

so daß sich die gesuchte Zahl z leicht aus den oben berechneten Werten ermitteln läßt.

Aus (21), (25) und (27) folgt

$$z_1 = C_1 \pmod{r} \tag{33}$$

Aus (22), (26) und (28) folgt

$$z_2 = C_2 \pmod{s} \ . \tag{34}$$

Durch Prüfung der Bedingungen (33) und (34) läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn eine der Bedingungen (33) oder (34) verletzt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

Im Gegensatz zu dem Verfahren in Patentanspruch 8 der Druckschrift WO-A1-98/52319 sind die Zahlen b_1 und b_2 in der hier vorgestellten Variante des Verfahrens nicht von der Basis x abhängig. Typischerweise wird bei der Anwendung des RSA-Verfahrens oder des Rabin'schen Signaturverfahrens ein privater Schlüssel einmal in ein kryptographisches Gerät, z. B: in eine Chipkarte eingebracht, und anschließend mehrmals verwendet. Hierbei ist bei der in diesen Verfahren angewendeten modularen Exponentiation der Exponent d sowie der Modulus p·q jeweils ein fester Bestandteil des privaten Schlüssels. Infolgedessen müssen die Werte C_1 und C_2 nur einmal beim Einbringen des Schlüssels in das kryptographische Gerät berechnet werden, und können dann anschließend in dem Gerät abgespeichert werden. Das

Abspeichern dieser Werte spart ggü. dem in der Druckschrift WO-A1-98/52319 vorgestellten Verfahren zwei modulare Exponentiationen.

Eine kryptographische Vorrichtung, beispielsweise eine Chipkarte, mit einer Zusatzhardware für die Beschleunigung der modularen Arithmetik enthält bei üblichen Ausführungsformen schnelle Addier- und/oder Multiplizierereinheiten, während die bei der modularen Reduktion erforderliche Division durch eine lange Zahl nach üblichen Standardverfahren durchgeführt werden muß, wie sie beispielsweise aus Donald Knuth: "The Art of Computer Programming", Volume 2: Seminumerical Algorithms, 2. Ed., Addison-Wesley, 1981, bekannt sind. Eines von mehreren bekannten Verfahren zur Vereinfachung der Divisionsoperation besteht darin, den Modulus p vor der Exponentiation mit einer Zahl r zu multiplizieren, so daß die Binärdarstellung des Produktes $p \cdot r$ möglichst viele Einsen enthält; siehe beispielsweise Menezes et al. a.a.O., Seiten 598 bis 599. Die Division durch eine Zahl mit möglichst vielen führenden Einsen ist erheblich einfacher als die Division durch eine allgemeine Zahl.

Der Multiplikator r wird erfindungsgemäß so gewählt, daß d teilerfremd zu $\phi(r)$ ist. Bei der o.g. Variante der Erfindung ist diese Teilerfremdheit nicht erforderlich. Für jeden Modulus p gibt es einen von der jeweiligen technischen Implementierung der Division abhängigen optimalen Multiplikator r_{opt}. Falls der gewählte Wert von r geringfügig kleiner als das Optimum ist, enthält das Produkt $p \cdot r$ immer noch genügend viele führende Einsen, um die Division einfach gestalten zu können. Mit hoher Wahrscheinlichkeit ist die Zahl d teilerfremd zu mindestens einem der Werte $\phi(r_{opt}-i)$, wobei $i = 1, ..., k$, wobei k eine von der Implementation abhängige kleine Zahl ist.

Wenn dies nicht der Fall ist, ersetze man r durch $2^i \cdot r$, wobei 2^i eine von der Implementierung abhängige geeignete Zweierpotenz ist.

Dieselben Substitutionen sind entsprechend auch auf den zweiten Primfaktor q anwendbar. Da die Multiplikatoren r (für p) und s (für q) unabhängig voneinander gewählt werden können, ist für den Multiplikator s ebenfalls eine entsprechende Wahl möglich.

Patentansprüche

1. Kryptographisches Verfahren,

a) mit mindestens einem eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s gewählt werden mit der Bedingung , daß d teilerfremd ist zu $\phi(kgV(r,s))$ und wobei die folgenden Rechenschritte durchgeführt werden:

$$x_1 = x \pmod{p \cdot r}$$

$$x_2 = x \pmod{q \cdot s}$$

$$d\_1 = d \pmod{\phi(p \cdot r)}$$

$$d\_2 = d \pmod{\phi(q \cdot s)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s},$$

und wobei $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

c) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

d) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

e) die vorher berechnete Zahl z und damit das Ergebnis E in einem Prüfschritt auf Rechenfehler geprüft wird,

f) der Prüfschritt folgende Rechenoperationen beinhaltet:

f1) Berechnen der kleinstmöglichen natürlichen Zahl e mit der Eigenschaft $e \cdot d = 1 \pmod{\phi(kgV(r,s))}$ mit Hilfe des erweiterten Euklids'schen Algorithmus

f2) Berechnen des Wertes $C = z^e \pmod{kgV(r,s)}$

f3) Vergleich der Werte x und C modulo kgV(r,s), wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $x \neq C \pmod{kgV(r,s)}$.

2. Kryptographisches Verfahren,

a) mit mindestens einer eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s , sowie zwei Zahlen b_1 und b_2 im Intervall [1,...,r-1] bzw. [1,...,s-1] und teilerfremd zu r bzw. s gewählt werden, und wobei b_1 und b_2 die Bedingung $b_1 = b_2 \pmod{ggT(r,s)}$ erfüllen, wobei ggT(r,s) den größten gemeinsamen Teiler von r und s bezeichnet,

c) mit Hilfe dir beiden Zahlen b_1 und b_2 nach dem Chinesischen Restwertsatz Werte x_1 und x_2 berechnet werden, die die folgenden Bedingungen erfüllen:

$$x_1 = x \pmod{p} , \quad x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q} , \quad x_2 = b_2 \pmod{s}$$

und anschließend folgende Rechenschritte durchgeführt werden:

$$d\_1 = d \pmod{\phi(p)}$$

$$d\_2 = d \pmod{\phi(q)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s}$$

und $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

d) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

e) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

f) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

g) der Prüfschritt folgende Rechenoperationen beinhaltet:

g1) Berechnen der Zahlen

$$C_1 = b_1^{d\_1} \pmod{r}$$

$$C_2 = b_2^{d\_2} \pmod{s}$$

wobei d_1 und d_2 vor der Durchführung der modularen Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden

g2) Vergleich der Werte z_1 und C_1 modulo r sowie z_2 und C_2 modulo s, wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $C_1 \neq z_1 \bmod r$ oder $C_2 \neq z_2 \bmod s$ gilt.

3. Kryptographisches Verfahren nach Anspruch 2, **dadurch gekennzeichnet,** daß die Zahlen r und s ungerade sind.

4. Kryptographisches Verfahren nach Anspruch 1 bis 3, **dadurch gekennzeichnet,** daß die Zahlen r und s im Bereich $[0, 2^k-1]$ mit $16 \leq k \leq 32$ ausgewählt werden.

5. Kryptographisches Verfahren nach Anspruch 1 bis 4, **dadurch gekennzeichnet,** daß mindestens eine der Zahlen r und s so gewählt wird, daß die

Binärdarstellung des Produktes p·r beziehungsweise q·s möglichst viele führende Einsen enthält.

6. Kryptographisches Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet,** daß beide Zahlen r und s so gewählt werden, daß die Binärdarstellung des Produktes p·r und des Produktes q·s möglichst viele führende Einsen enthalten.

7. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

8. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt für jede der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $l = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

9. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt mindestens eine der Zahlen r_{opt} und s_{opt} zunächst ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird,

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls ein solcher Wert für $i = 0, 1,..., k$ existiert, und

c) in einem dritten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $i = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

10. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das RSA-Verfahren beinhaltet.

11. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.

12. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

13. Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x ausführt, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s gewählt werden mit der Bedingung , daß d teilerfremd ist zu $\phi(kgV(r,s))$ und wobei die folgenden Rechenschritte durchgeführt werden:

$$x_1 = x \pmod{p \cdot r}$$

$$x_2 = x \pmod{q \cdot s}$$

$$d\_1 = d \pmod{\phi(p \cdot r)}$$

$$d\_2 = d \pmod{\phi(q \cdot s)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s},$$

und $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

c) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

d) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

e) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

f) der Prüfschritt folgende Rechenoperationen beinhaltet:

f1) Berechnen der kleinstmöglichen natürlichen Zahl e mit der Eigenschaft $e \cdot d = 1 \pmod{\phi(kgV(r,s))}$ mit Hilfe des erweiterten Euklid'schen Algorithmus

f2) Berechnen des Wertes $C = z^e \pmod{kgV(r,s)}$

f3) Vergleich der Werte x und C modulo kgV(r,s), wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $x \neq C \pmod{kgV(r,s)}$.

14. . Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x ausführt, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s , sowie zwei Zahlen b_1 und b_2 im Intervall [1,...,r-1] bzw. [1,...,s-1] und teilerfremd zu r bzw. s gewählt werden, und wobei b_1 und b_2 die Bedingung $b_1 = b_2 \pmod{ggT(r,s)}$ erfüllen, wobei ggT(r,s) den größten gemeinsamen Teiler von r und s bezeichnet,

c) mit Hilfe dir beiden Zahlen b_1 und b_2 nach dem Chinesischen Restwertsatz Werte x_1 und x_2 berechnet werden, die die folgenden Bedingungen erfüllen:

$$x_1 = x \pmod{p}, \quad x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q}, \quad x_2 = b_2 \pmod{s}$$

und anschließend folgende Rechenschritte durchgeführt werden:

$$d\_1 = d \pmod{\phi(p)}$$

$$d\_2 = d \pmod{\phi(q)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s}$$

und wobei $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

d) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

e) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

f) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

g) der Prüfschritt folgende Rechenoperationen beinhaltet:

g1) Berechnen der Zahlen

$$C_1 = b_1^{d\_1} \pmod{r}$$

$$C_2 = b_2^{d\_2} \pmod{s}$$

wobei d_1 und d_2 vor der Durchführung der modularen Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden,

g2) Vergleich der Werte z_1 und C_1 modulo r sowie z_2 und C_2 modulo s, wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $C_1 \neq z_1 \bmod r$ oder $C_2 \neq z_2 \bmod s$ gilt.

15. Kryptographische Vorrichtung nach Anspruch 14, **dadurch gekennzeichnet,** daß die Zahlen r und s ungerade sind.

16. Kryptographische Vorrichtung nach Anspruch 13 bis 15, **dadurch gekennzeichnet,** daß die Zahlen r und s im Bereich $[0, 2^k\text{-}1]$ mit $16 \leq k \leq 32$ ausgewählt werden.

17. Kryptographische Vorrichtung nach Anspruch 13 bis 16, **dadurch gekennzeichnet,** daß mindestens eine der Zahlen r und s so gewählt wird, daß die Binärdarstellung des Produktes $p \cdot r$ beziehungsweise $q \cdot s$ möglichst viele führende Einsen enthält.

18. Kryptographische Vorrichtung nach einem der Ansprüche 13 bis 17, **dadurch gekennzeichnet,** daß beide Zahlen r und s so gewählt werden, daß die Binärdarstellung des Produktes p·r und des Produktes q·s möglichst viele führende Einsen enthalten.

19. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

20. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt für jede der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $l = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

21. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt mindestens eine der Zahlen r_{opt} und s_{opt} zunächst ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird,

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls ein solcher Wert für $i = 0, 1,..., k$ existiert, und

c) in einem dritten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $i = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

22. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das RSA-Verfahren beinhaltet.

23. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.

24. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2001 (20.12.2001)

PCT

(10) International Publication Number
WO 01/96990 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP01/06816

(22) International Filing Date: 15 June 2001 (15.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/594,456 15 June 2000 (15.06.2000) US

(71) Applicant: **RAINBOW TECHNOLOGIES, B.V.** [NL/NL]; Oliphanteweg 10, NL-1397 Le Rotterdam (NL).

(72) Inventors: **ABBOTT, Shawn, D.**; 305 Pinnacle Ridge Place, RR12, Calgary, Alberta T3E 6W3 (CA). **ANDERSON, Allan, D.**; 11158 Bertha Place, Cerritos, CA 90703 (US). **GODDING, Patrick, N.**; 22665 Shady Grove Circle, Lake Forest, CA 92630 (US). **PUNT, Maarten, G.**; 24942 Paseo Arboleda, Lake Forest, CA 92630 (US). **SOTOODEH, Mehdi**; 17 Paloma Drive, Mission Viejo, CA 92692 (US).

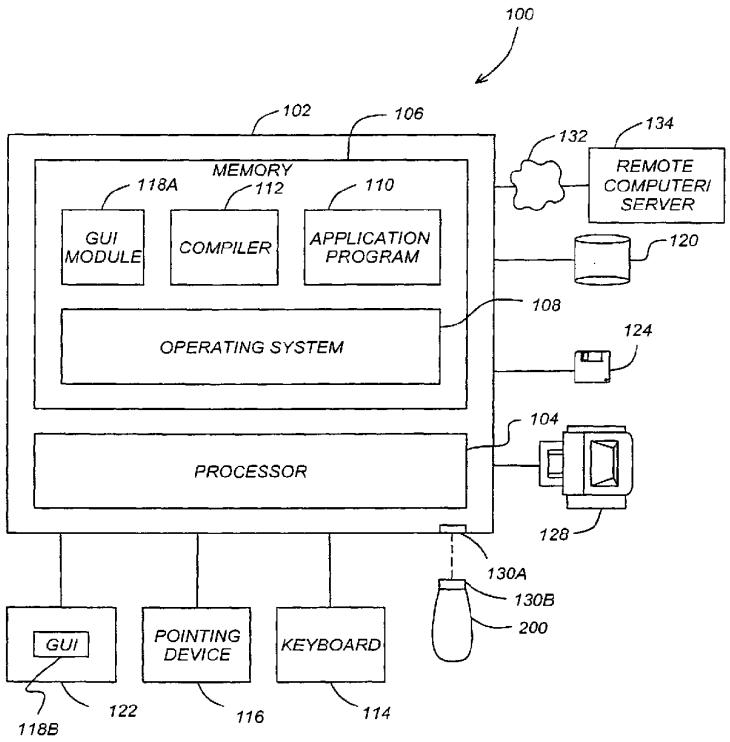
(74) Agents: **SMITH, Samuel, Leonard** et al.; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, UZ, VN, YU, ZA, ZW.

(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

[Continued on next page]

(54) Title: USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR



(57) Abstract: A compact, self-contained, personal key is disclosed. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface of communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

WO 01/96990 A2

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
without international search report and to be republished upon receipt of that report

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.

USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. Patent Application No. 09/449,159, filed November 24, 1999, by Shawn D. Abbott, Bahram Afghani, Mehdi Sotoodeh, Norman L. Denton III, and Calvin W. Long, and entitled "USB-Compliant Personal Key with Integral Input and Output Devices," which is a continuation-in-part of U.S. Patent Application No. 09/281,017, filed March 30, 1999 by Shawn D. Abbott, Bahram Afghani, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt, and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key," which claims benefit of U.S. Provisional Patent Application No. 60/116,006, filed January 15, 1999 by Shawn D. Abbott, Barham Afghani, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt, and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key," all of which applications are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computer peripherals, and in particular to an inexpensive USB-compliant personal key that is compatible with existing smartcard processors, drivers, and instruction sets.

2. Description of the Related Art

In the last decade, the use of personal computers in both the home and in the office have become widespread. These computers provide a high level of functionality to many people at a moderate price, substantially surpassing the performance of the large mainframe computers of only a few decades ago. The trend is further evidenced by the increasing popularity of laptop and notebook computers, which provide high-performance computing power on a mobile basis.

The widespread availability of personal computers has had a profound impact on interpersonal communications as well. Only a decade ago, telephones or fax machines offered virtually the only media for rapid business communications. Today, a growing number of businesses and individuals communicate via electronic mail (e-mail). Personal computers have also been instrumental in the emergence of the Internet and its growing use as a medium of commerce.

While certainly beneficial, the growing use of computers in personal communications, commerce, and business has also given rise to a number of unique challenges. These challenges include the prevention of unauthorized use of software, ensuring the security of e-mail and other electronic communications, as well as Internet commerce.

Smartcards represent a longstanding attempt to deal with at least some of the foregoing challenges. Substantial resources have been made in the design and development of smartcards, smartcard readers, and the associated reader/smartcard drivers which allow computer applications to interface with the smartcard to perform security and data storage functions. Even so, smartcards have not enjoyed widespread popularity. Smartcard readers are relatively expensive, and not widely available. Further, the lack of uniform smartcard/smartcard reader physical interface standards have resulted in smartcard/smartcard reader physical interface compatibility problems, many of which remain unresolved.

USB-compliant personal keys, such as that which is disclosed in co-pending and commonly assigned U.S. Patent Application Nos. 09/449,159 and 09/281,017, described above, offer the benefit of smartcard functionality in a universally accepted USB form factor. The Universal Serial Bus (USB) is a connectivity standard developed by computer and telecommunication industry members for interfacing computers and peripherals. USB-compliant devices allow the user to install and hot-swap devices without long installation procedures and reboots, and features a 127 device bus capacity, dual-speed data transfer, and can provide limited power to devices attached on the bus. Because the USB connectivity standard is rapidly

becoming available on most personal computers, it offers a standard, widely available physical interface, the unavailability of which has prevented smartcards from achieving widespread acceptance.

While smartcards have not enjoyed widespread popularity in the United States, they are widely accepted in Europe. Hence, many software applications and drivers have been developed for existing smartcard-based devices and their readers. Unfortunately, smartcard interface protocols such as those described in ISO 7816 are incompatible with the USB protocols used in the above-described devices. This incompatibility has led to two unfortunate consequences. First, to comply with USB interface protocol requirements, current USB-compliant personal keys utilize special purpose processors, instead of the low cost, limited capability processors currently available for smartcards. This increases the cost of the USB-compliant personal key, making widespread acceptance more difficult. Also, because each USB-compatible personal key may use a different processor (and different instruction sets), users may require different device drivers for different personal keys. This too represents another barrier to widespread acceptance of the personal key.

From the foregoing, it is apparent that there is a need for a USB-compliant personal key that is usable with legacy personal identification devices, such as processors having smartcard processors and/or those complying with the ISO 7816. There is also a need for a USB-compliant personal key that makes maximum use of existing smartcard protocols, software and devices wherever possible, and which retain at least a limited compatibility with existing devices designed to interface with smartcards. The present invention satisfies that need.

SUMMARY OF THE INVENTION

The present invention satisfies all of these needs with a personal key in a form factor that is compliant with a commonly available I/O interface such as the Universal Serial Bus (USB) and at the same time, usable with existing smartcard software applications. The personal key comprises a USB-compliant interface releaseably

coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

In one embodiment, the method comprises the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The present invention is well suited for controlling access to network services, or anywhere a password, cookie, digital certificate, or smartcard might otherwise be used, including:

- Remote access servers, including Internet protocol security (IPSec), point to point tunneling protocol (PPTP), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), remote access dial-in user service (RADIUS), terminal access controller access control system (TACACS);
- Providing Extranet and subscription-based web access control, including hypertext transport protocol (HTTP), secure sockets layer (SSL);

- Supporting secure online banking, benefits administration, account management;
- Supporting secure workflow and supply chain integration (form signing);
- Preventing laptop computer theft (requiring personal key for laptop operation);
- Workstation logon authorization;
- Preventing the modification or copying of software;
- Encrypting files;
- Supporting secure e-mail, for example, with secure multipurpose Internet mail extensions (S/MIME), and open pretty good privacy (OpenPGP)
- Administering network equipment administration; and
- Electronic wallets, with, for example, secure electronic transaction (SET, MilliCent, eWallet)

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an exemplary hardware environment for practicing the present invention;

FIG. 2 is a block diagram of a personal key communicatively coupled to a host computer;

FIG. 3 is a block diagram of a personal key with a smartcard processor communicatively coupled to a host computer; and

FIGs. 4A-4D are flow charts presenting exemplary method steps that can be used to practice the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which is shown, by way of illustration, several

embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

FIG. 1 illustrates an exemplary computer system 100 that could be used to implement the present invention. The host computer 102 comprises a processor 104 and a memory, such as random access memory (RAM) 106. The host computer 102 is operatively coupled to a display 122, which presents images such as windows to the user on a graphical user interface 118B. The host computer 102 may be coupled to other devices, such as a keyboard 114, a mouse device 116, a printer 128, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the host computer 102.

Generally, the host computer 102 operates under control of an operating system 108 stored in the memory 106, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module 118A. Although the GUI module 118A is depicted as a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system 108, the computer program 110, or implemented with special purpose memory and processors. The host computer 102 also implements a compiler 112 which allows an application program 110 written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor 104 readable code. After completion, the application 110 accesses and manipulates data stored in the memory 106 of the host computer 102 using the relationships and logic that are generated using the compiler 112. The host computer 102 also comprises an input/output (I/O) port for a personal token 200 (hereinafter alternatively referred to also as a personal key 200). In one embodiment, the I/O port is a USB-compliant interface comprising a host computer USB-compliant interface 130A and a personal token USB-compliant interface 130B (hereinafter referred to collectively as the USB-compliant interface 130.

In one embodiment, instructions implementing the operating system 108, the computer program 110, and the compiler 112 are tangibly embodied in a computer-readable medium, e.g., data storage device 120, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive 124, hard drive, CD-ROM drive, tape drive, etc. Further, the operating system 108 and the computer program 110 are comprised of instructions which, when read and executed by the computer 102, causes the computer 102 to perform the steps necessary to implement and/or use the present invention. Computer program 110 and/or operating instructions may also be tangibly embodied in memory 106 and/or data communications devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

The host computer 102 may be communicatively coupled to a remote computer or server 134 via communication medium 132 such as a dial-up network, a wide area network (WAN), local area network (LAN), virtual private network (VPN) or the Internet. Program instructions for computer operation, including additional or alternative application programs can be loaded from the remote computer/server 134. In one embodiment, the computer 102 implements an Internet browser, allowing the user to access the world wide web (WWW) and other internet resources.

Those skilled in the art will recognize that many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the present invention.

FIG. 2 is a block diagram illustrating the components of one embodiment of a personal key 200. The personal key 200 communicates with and obtains power from the host computer 102 through a USB-compliant communication path in the USB-compliant interface 130 which includes the input/output port 130A of the host

computer 102 and a matching input/output (I/O) port 130B on the personal key 200. The processor 212 is communicatively coupled to a memory 214, which stores data and instructions to implement the above-described features of the invention. In one embodiment, the memory 214 is a non-volatile random-access memory that can retain factory-supplied data as well as customer-supplied application related data. The processor 212 may also include some internal memory for performing some of these functions.

The processor 212 is optionally communicatively coupled to an input device 218 via an input device communication path 224 and to an output device 222 via an output device communication path 224, both of which are distinct from the USB-compliant interface 130. These separate communication paths 220 and 224 allow the user to view information about processor 212 operations and provide input related to processor 212 operations without allowing a process or other entity with visibility to the USB-compliant interface 130 to eavesdrop or intercede. This permits secure communications between the key processor 212 and the user. In one embodiment of the invention set forth more fully below, the user communicates directly with the processor 212 by physical manipulation of mechanical switches or devices actuatable from the external side of the key (for example, by pressure-sensitive devices such as buttons and mechanical switches). In another embodiment of the invention set forth more fully below, the input device includes a wheel with tactile detents indicating the selection of characters.

The input device and output devices 218, 222 may cooperatively interact with one another to enhance the functionality of the personal key 200. For example, the output device 222 may provide information prompting the user to enter information into the input device 218. For example, the output device 222 may comprise a visual display such as an alphanumeric LED or LCD display (which can display Arabic numbers and or letters) and/or an aural device. The user may be prompted to enter information by a beeping of the aural device, by a flashing pattern of the LED, or by both. The output device 222 may also optionally be used to confirm entry of

information by the input device 218. For example, an aural output device may beep when the user enters information into the input device 218 or when the user input is invalid. The input device 218 may take one of many forms, including different combinations of input devices.

Although the input device communication path 220 and the output device communication path 224 are illustrated in FIG. 2 as separate paths, the present invention can be implemented by combining the paths 220 and 224 while still retaining a communication path distinct from the USB-compliant interface 130. For example, the input device 218 and output device 222 may be packaged in a single device and communications with the processor 212 multiplexed over a single communication path.

FIG. 3 is a block diagram of the personal key 200 and host computer 102 as applied to the present invention. Unlike the personal key 200 illustrated in FIG. 2, the personal key 300 illustrated in FIG. 3 comprises a smartcard processor 320. The smartcard processor 300 is a processor which complies with well-known smartcard I/O protocols and smartcard command sets and functions, such as those described by the International Standards Organization (ISO) standard 7816 Part III (defining electronic properties and transmission characteristics), which is hereby incorporated by reference herein.

Physically, the smartcard compliant I/O interface 324 includes a serial I/O line, a reset (RST) line, a clock (CLK) line, a programming voltage (VPP), a power supply voltage (VCC) and a ground. This I/O interface 324 is further described in the publication "Introduction to Smartcards" by Dr. David B. Everett, which was published in 1999 by the Smart Card News Ltd., and is incorporated by reference herein.

As was the case with the personal key 200 and host computer 102 illustrated in FIG. 1, the present invention allows the use of a personal key 300 communicating with the host computer 102 via a USB-compliant interface 130. However, the substitution of the smartcard processor 320 for the ordinary processor 212 depicted in

FIG. 2 has several advantages. First, smartcard processors 212 are relatively inexpensive and readily available. Second, a large number of application programs 110 have been developed for the use of smartcards, including the personal computer/smartcard (PC/SC) interface developed by the MICROSOFT CORPORATION. By providing a smartcard processor (which complies with the smartcard I/O protocols and supports smartcard command sets), this software can be used with a personal key 300 in a USB-compliant form factor.

The use of the smartcard processor 320 in the personal key 300 is enabled by use of an interface processor 314 communicatively coupled to the smartcard processor 320 via a smartcard-compatible (S/C 7816) interface 324. The interface processor 314 comprises a smartcard reader emulator module (SREM) 316 and a translation module 318. The SREM 316 implements functions that emulate those of a smartcard reader, thus projecting the image of a smartcard reader to the smartcard processor 320. The SREM 316 provides all instructions and commands to the smartcard processor 320 and receives messages and responses from the smartcard processor 320 according to the S/C protocol.

The host computer 102 comprises a virtual smartcard reader module (VSRM) 302. The VSRM comprises a communication module 312, an answer-to-reset module 308, and a smartcard insertion/removal reporting module 306. The communication module 312 packages messages intended for the personal key 300 for transmission via the USB-compliant interface. In one embodiment, messages and commands that are sent to the personal key 300 packaged as:

USB command = USB header + USB cdata (wherein USB cdata is the smartcard compliant command)

and messages and responses from the personal key 300 are packaged as:

USB response = USB header + USB rdata (wherein USB rdata is the smartcard compliant response)

These packaged messages are unpacked by the translation module 318 in the personal key 300. Similarly, messages transmitted by the smartcard processor 320 to the host computer 102 are packaged by the translation module 318 and unpackaged by the communication module 312 before being provided to the operating system 108, the application program interface 260, and the application 110 using the personal key 300 to perform operations.

Just as the SREM 316 emulates the presence of a smartcard reader for the smartcard processor 320, the VSRM 302 emulates the presence of a smartcard reader to the OS 108 in the host computer 102. These functions are accomplished in the bootup module 311, the insert/remove module 306, the answer-to-reset module 308, and the PTS module 310.

As a part of a normal bootup sequence, the host computer's 102 operating system performs a startup sequence to determine which hardware elements are available for use. In prior art smartcard systems, the smartcard reader remains coupled to the host computer 102, whether a smartcard is inserted into the reader or not. Hence, the smartcard reader can respond to startup sequence queries, and the smartcard reader is recognized by the operating system 108 for further operations. However, in the present invention, there is no smartcard reader to answer to the bootup query, and the operating system would ordinarily be unable to operate with a smartcard thereafter. To solve this problem, the present invention comprises a bootup module 311, which responds to messages from the operating system 108 in the same way as a smartcard reader would if it were coupled to the host computer 102.

Similarly, the insert/remove module 306 provides an indication to the operating system 108 that the personal key 300 has been inserted or removed from the

USB-compliant interface 130. This is accomplished by querying the host computer USB-compliant interface port 130A.

When a software application calls 110, via API 260 and the operating system 108 invokes a command that calls for a smartcard related function, the smartcard reader passes a reset command to the smartcard. The smartcard returns an answer-to-reset message which indicates, among other things, the protocol and I/O interface supported by the attached smartcard.

The reset signal is used to start up the program contained in a memory 322 communicatively coupled to or resident within the smartcard processor 320. The ISO standard defines three reset modes, internal reset, active low reset, and synchronous high active reset. Most smartcard processors 320 operate using the active low reset mode. In this mode, the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The synchronous mode of operation is more commonly met with smartcards used for telephonic applications.

The sequence of operations for activating the smartcard processor 320 is defined in order to minimize the possibility of damaging the smartcard processor 320. Of particular importance is avoiding corruption of the non-volatile memory 322 of the smartcard. Most smartcard processors 320 operate using an active low reset mode in which the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The sequence performed by the smartcard processor includes the steps of setting the RST line low, applying VCC to the proper supply voltage, setting the I/O in the receive mode, setting VPP in the idle mode, applying the clock, and taking the RST line high (active low reset).

In prior art smartcard systems, after the reset signal is applied by the smartcard reader, the smartcard processor 320 responds with an answer-to-reset message. For the active low reset mode, the smartcard processor 320 should respond between 400 and 40,000 clock cycles after the rising edge of the reset signal. The answer-to-reset

signal is at most 33 characters, and includes 5 fields including an initial character (TS), a format character (TO), interface characters (TAi, TBi, TCi, and TDi), historical characters (T1, T2, ... , TK), and a check character (TCK). Among other things, the answer-to-reset signal provides an indication of the smartcard protocol(s) which are supported smartcard processor. Typical smartcard protocols include the T=0 protocol (asynchronous half duplex byte transmission) and T=1 (asynchronous half duplex block transmission).

In the embodiment of the present invention shown in FIG. 3, the reset signal is provided by the VSRM 302, packaged by the communication module 312, and sent via the USB-compliant interface 130B to the personal key 300. The message is unwrapped by the translation module 318. Then, the smartcard reader emulation module activates the RST signal path in the smartcard interface 324, thus providing the RST command to the smartcard processor 320. The smartcard processor 320 responds with an answer-to-reset message, sends the message via the serial I/O line of the smartcard interface 324 to the interface processor 314. The message is then packaged by the translation module 318 and transmitted to the host computer 102 via the USB-compliant interface 326. The message is then unpackaged by the communication module 312 and provided to the operating system 108 and ultimately, the application 110 that requested the use of the smartcard.

In another embodiment of the present invention, the personal key 300 does not comprise a smartcard processor 320, but rather a special purpose processor which does not respond to messages and commands in the smartcard I/O protocol (such as that which is illustrated in FIG. 1). The present invention can still be used with existing smartcard applications 110, however, because the VSRM 302 and the interface processor 314 can be used to simulate the presence of a smartcard processor 320. When the smartcard software application 110 desires use of the personal key 300, the VSRM accepts the reset command from the PC/SC modules in the operating system 108, translates the reset message into a functionally equivalent message for the special purpose processor in the personal key 300, and transmits the message to the

personal key 300. After the personal key 300 is activated, it sends a message indicating as such to the host computer 102. The VSRM 302, and translates this message to a response that is compatible with the smartcard application 110, namely, an ATR message. Alternatively, the smartcard command to special purpose processor command translation can occur in the emulation processor 314 in the personal key 300.

Returning to the embodiment disclosed in FIG. 3, after the smartcard processor has issued the ATR message, a protocol type selection (PTS) message may be sent to the smartcard processor 320. The PTS message from the OS 108 is received by the PTS module 310 in the VSRM 302, packaged for transmission via the USB-compliant interface 130 to the personal key 300, where it is unpackaged and provided to the smartcard processor 320. The smartcard provides a response consistent with the ISO standards to the emulation module 316. The response is packaged, and transmitted over the USB-compliant interface 130 to the host computer 102, where it is unpackaged by the communication module 312 and provided to the operating system.

FIGs. 4A-4D are flow charts presenting exemplary method steps used to practice one embodiment of the present invention. When the host computer 102 is booted up, the virtual smartcard reader 302 accepts 402 a bootup query from the host computer's operating system 108. Although a smartcard reader is not communicatively coupled to the host computer 130 the virtual smartcard reader 302 emulates the existence of a smartcard reader and provides an indication that a smartcard reader is available to the OS 108. Consequently, when the bootup procedures are completed, a smartcard reader will be registered as an available device to smartcard applications 110.

When the host computer is booted up, a personal key 300 may or may not be communicatively coupled to the USB-compliant interface 130. When a personal key 300 is not attached, the VSRM 302 provides 404 the same indication to the operating system 108 as would be supplied by a smartcard reader without an inserted smartcard. This is accomplished by receiving 406 an indication that the personal key has been

communicatively coupled to the USB-compliant interface, and providing an indication to the host computer operating system. Since the VSRM is emulating the functions of a smartcard, the indication is provided 408 to the host computer operating system (or equivalently, the personal computer/smartcard (PC/SC) interface modules therein) is that of an insert event.

If desired and the smartcard processor 320 supports multiple protocols, a protocol type selection (PTS) command may be issued by the operating system 108. The VSRM 302 receives 410 the PTS command, packages the command for transmission to the personal key 300 via the USB-compliant interface 130. The wrapped PTS command is then transmitted over the USB-compliant interface 130 and received by the personal key 300. The PTS command is unwrapped by the translate module 318 in the interface processor 314 and provided to the smartcard processor 320 via the smartcard-compliant interface 324. The smartcard processor computes the appropriate response, sends the response to the interface processor 314, where the response is packaged by the translate module 318 for transmission to the host computer 102 via the USB-compliant interface 130. The communication module 312 unpackages the response, and the PTS module 310 formats the response, if necessary, to be consistent with a PTS response received from a smartcard reader. The formatted response is then provided 412 to the OS 108.

FIG. 4B is a flow chart describing exemplary method steps used to provide commands and/or data from the OS 108 to the smartcard processor 320 and from the smartcard processor 320 to the OS 108. A message, which may comprise a smartcard reader command belonging to a smartcard reader command set is accepted 414 from a host computer operating system 108 in the virtual smartcard reader module (VSRM) 302. The message is packaged 416 for transmission via the USB-compliant interface 130 according to a first message transfer protocol.

The packaged message is then transmitted 418 to the communicatively coupled personal key 300 via the USB-compliant interface 130. The packaged message is received 420 and unpackaged 422 in the personal key 300. If the

smartcard reader command requires additional processing before being forwarded to the smartcard processor 320, the smartcard reader command is translated 424 into a smartcard command within the personal key 300 before being provided 426 to the smartcard processor 320.

The smartcard processor 320 then performs the indicated operation, and a response is accepted 428 from the smartcard processor 320. If the smartcard response requires further processing by a smartcard reader, the smartcard response is translated 430 into a smartcard reader response. The smartcard reader response is then packaged 432 and transmitted 434 to the host computer 102 via the USB-compliant interface 130. The host computer 102 receives 436 and unpackages 438 the message and provides 440 the response to the smartcard software application 110 that issued the command.

Next, when the personal key 300 is removed, the VSRM 302 reports 444 an indication to the OS 108 that the "virtual smartcard" (the personal key 300) has been removed. The provided indication is the same as that which would be provided by a smartcard reader when a smartcard is removed. The indication can be obtained, for example by receiving 442 an indication from a USB driver or other device indicating the removal of a USB device.

In summary, Tables I and II provides an summary of the communication protocol for an OS 108 command from the host computer 102 to the smartcard processor 320 in the personal key (Table I), and for a smartcard processor 320 response to the operating system 108.

Step	Description
1	Smartcard reader command issued from OS 108 is passed to VSRM 302
2	VSRM 302 adds a USB header, and creates a USB command
3	VSRM's 302 communication module 312 sends the USB command to the personal key 300
4	The translation module 318 strips off the USB header and recovers the smartcard command
5	The smartcard command is sent to the smartcard processor 320
6	The smartcard processor 320 executes the function requested by the smartcard command

Table I

Step	Description
1	Smartcard processor 320 generates a smartcard response
2	The smartcard response is sent from the smartcard processor 320 to the translation module 318
3	The translation module 318 adds a USB header to create a USB response
4	The USB response is transmitted to the VSRM 302
5	The communication module 312 strips off the USB header and recovers the smartcard response
6	The smartcard response is transmitted to the OS 108

Table II

Tables III and IV provides a summary of the communication protocol for a request from an application program 110 to the smartcard processor 320 and for a request from an application program 110 to the smartcard processor 320.

Step	Description
1	Smartcard processor 320 command from the application program 110 is sent to the OS 108 via an API 260
2	The smartcard processor 320 command is sent from the OS 108 to the VSRM 302
3	The VSRM 302 adds a USB header to the smartcard processor 320 command to create a USB-compatible command
4	The VSRM's comm module 312 sends the USB-compliant command to the personal key 300
5	Translation module 318 strips off the USB header and recovers the smartcard processor command
6	The smartcard processor command is transmitted to the smartcard processor 320
7	The smartcard processor 320 performs the function indicated by the smartcard processor command

Table III

Step	Description
1	The smartcard processor 320 generates a response to the smartcard processor command
2	The response is provided to the translation module 318
3	The translation module adds a USB header to create a USB-compatible smartcard processor response
4	The USB-compatible smartcard processor response is sent to the VSRM 302
5	The communication module 312 strips off the USB header to recover the smartcard processor response
6	The smartcard processor response is provided to the application 110 via the OS 108 and the API 260

Table IV

Conclusion

This concludes the description of the preferred embodiments of the present invention. In summary, the present invention describes a personal key comprising a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant

messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages. In another embodiment, the invention is described by a method comprising the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

WHAT IS CLAIMED IS:

1. A compact personal token (300), comprising:

a USB-compliant interface (130B) releaseably coupleable to a host processing device (102) operating under command of an operating system (108);

a smartcard processor (320) having a smartcard processor-compliant interface (324) for communicating according to a smartcard input and output protocol;

an input device (218) communicatively coupled to the smartcard processor for providing secure input to the processor;

an interface processor (314), communicatively coupled to the USB-compliant interface (130B) and to smartcard processor-compliant interface (324) the interface processor (314) implementing a translation module (318) for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

2. The apparatus of claim 1, wherein the interface processor (314) emulates a smartcard reader to the smartcard processor (320).

3. The apparatus of claim 1, wherein:

the host processing device (102) comprises a virtual smartcard reader in communication with the operating system, the virtual smartcard reader for emulating a smartcard reader communicatively coupled to the host processing device (102) and including a communication module (312) for packaging messages for transmission to the personal token (300) via the USB compliant interface (130) according to a first protocol and for unpackaging messages received from the personal token (300) via the USB-compliant interface according to the first protocol; and

the interface processor translation module (318) unpackages messages from the host processing device (102) according to the first protocol and packages messages destined for the host processing device (102) according to the first protocol.

4. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a bootup module (311) for responding to an operating system bootup procedure with an indication that a smartcard reader is communicatively coupled to the host processor.

5. The apparatus of claim 3, wherein the virtual smartcard reader further comprises an answer-to-reset (ATR) module (308) for providing an ATR message to the operating system (108) in response to a reset message.

6. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a reporting module for receiving and reporting the insertion of the personal token in a USB-compliant port communicatively coupled to the host processor (102) and the removal of the personal token as a removal of a smartcard from a smartcard reader.

7. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a protocol selection module for receiving a protocol type selection (PTS) command from the operating system and providing a PTS response message to the operating system (108).

8. A method of communicating between a smartcard processor (320) in a personal key (300) communicatively coupled to a host computer (102) via a USB-compliant interface (130), comprising the steps of:

accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system (108) in a virtual smartcard reader;

packaging the message for transmission via a USB-compliant interface (130) according to a first message transfer protocol;

transmitting the packaged message to a personal key (300) communicatively coupled to the USB-compliant interface (130);

receiving the packaged message in the personal key (300);

unpackaging the message in the personal key (300) to recover the smartcard reader command;

translating the smartcard reader command into a smartcard command within the personal key (300); and

providing the smartcard command to the smartcard processor (320);

accepting a user input to the smartcard processor (320) via an input device (218) communicatively coupled to the smartcard processor (320) via an input communication device communication path distinct from the USB-compliant interface (130);

accepting a smartcard response from the smartcard processor (320);

translating the smartcard response into a smartcard reader response;

packaging the smartcard reader response for transmission to the host processor (102) via the USB-compliant interface (130);

transmitting the packaged message from the personal key (300) to the host processor (102);

receiving the packaged message in the host computer (102);

unpackaging the smartcard reader response; and

providing the smartcard reader response to the host processor operating system (108).

9. The method of claim 8, further comprising the steps of:

accepting a startup query from the host computer operating system (108) in the virtual smartcard reader; and

providing an indication that a smartcard reader is communicatively coupled to the host computer to the host computer operating system (108).

10. The method of claim 9, further comprising the steps of:

receiving an indication that the personal key (300) has been communicatively coupled to the USB-compliant interface (130);

reporting the indication that the personal key (300) is communicatively coupled to the USB-compliant interface (130) to the host processor operating system (108) as the insertion of a smartcard;

receiving an indication that the personal key (300) has been communicatively decoupled from the USB-compliant interface (130); and

reporting the indication that the personal key has been communicatively decoupled from the USB-compliant interface (130) to the host processor operating system (108) as the removal of the smartcard.

11. The method of claim 8, further comprising the steps of:

receiving a protocol type selection (PTS) command from the host computer operating system (108); and

providing a PTS response message to the operating system (108).

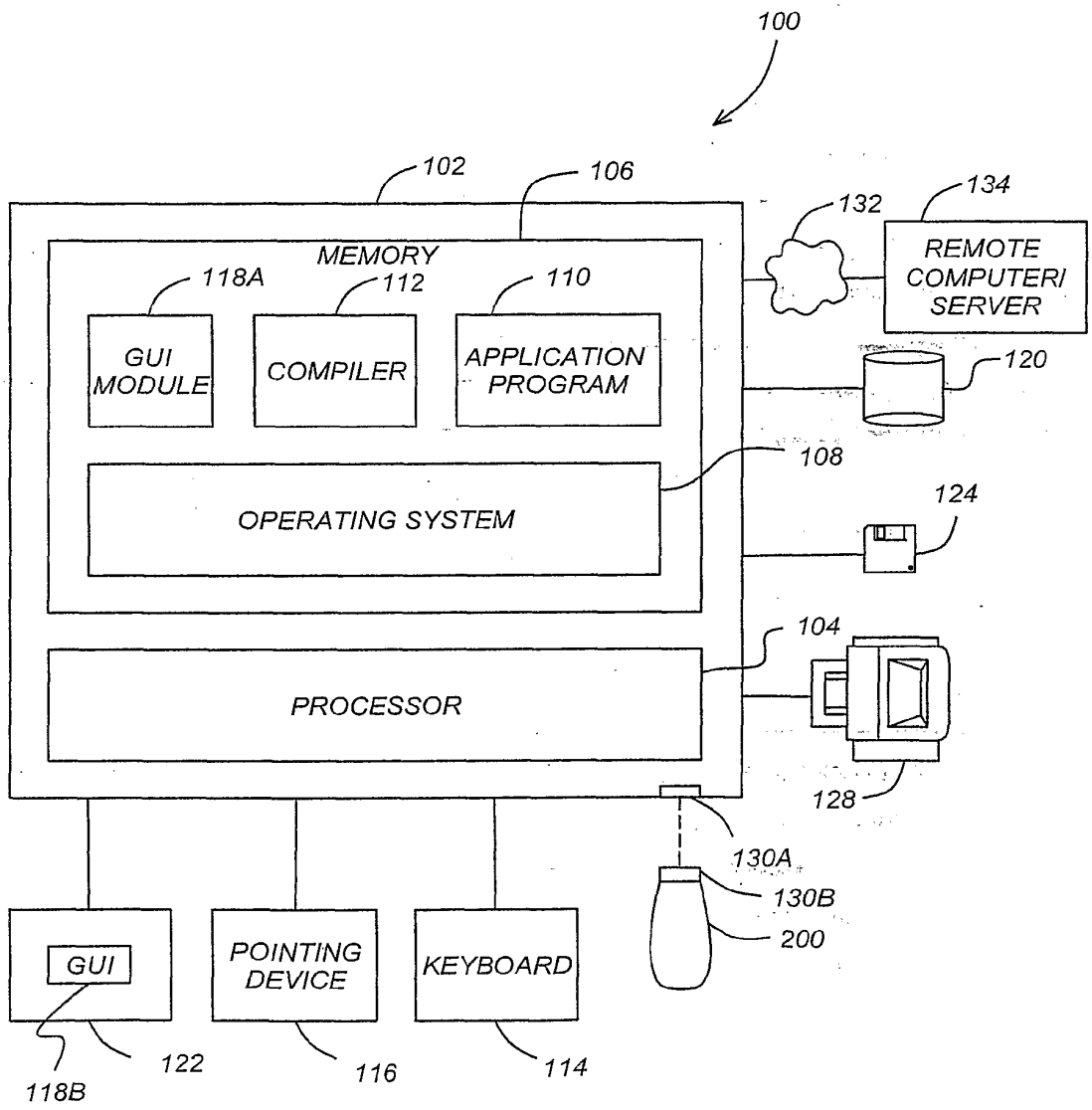

100
102
106
132
134
REMOTE COMPUTER/ SERVER
MEMORY
118A
112
110
GUI MODULE
COMPILER
APPLICATION PROGRAM
120
108
OPERATING SYSTEM
124
104
PROCESSOR
128
130A
130B
200
GUI
POINTING DEVICE
KEYBOARD
122
116
114
118B

FIG. 1

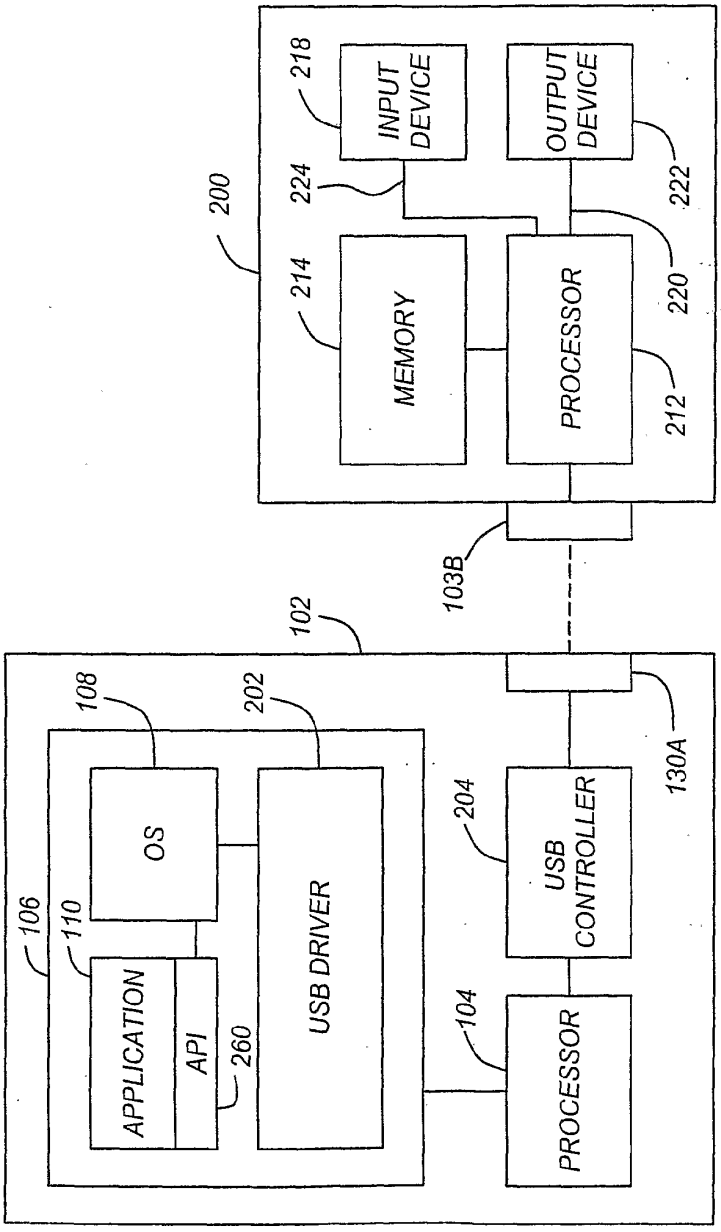
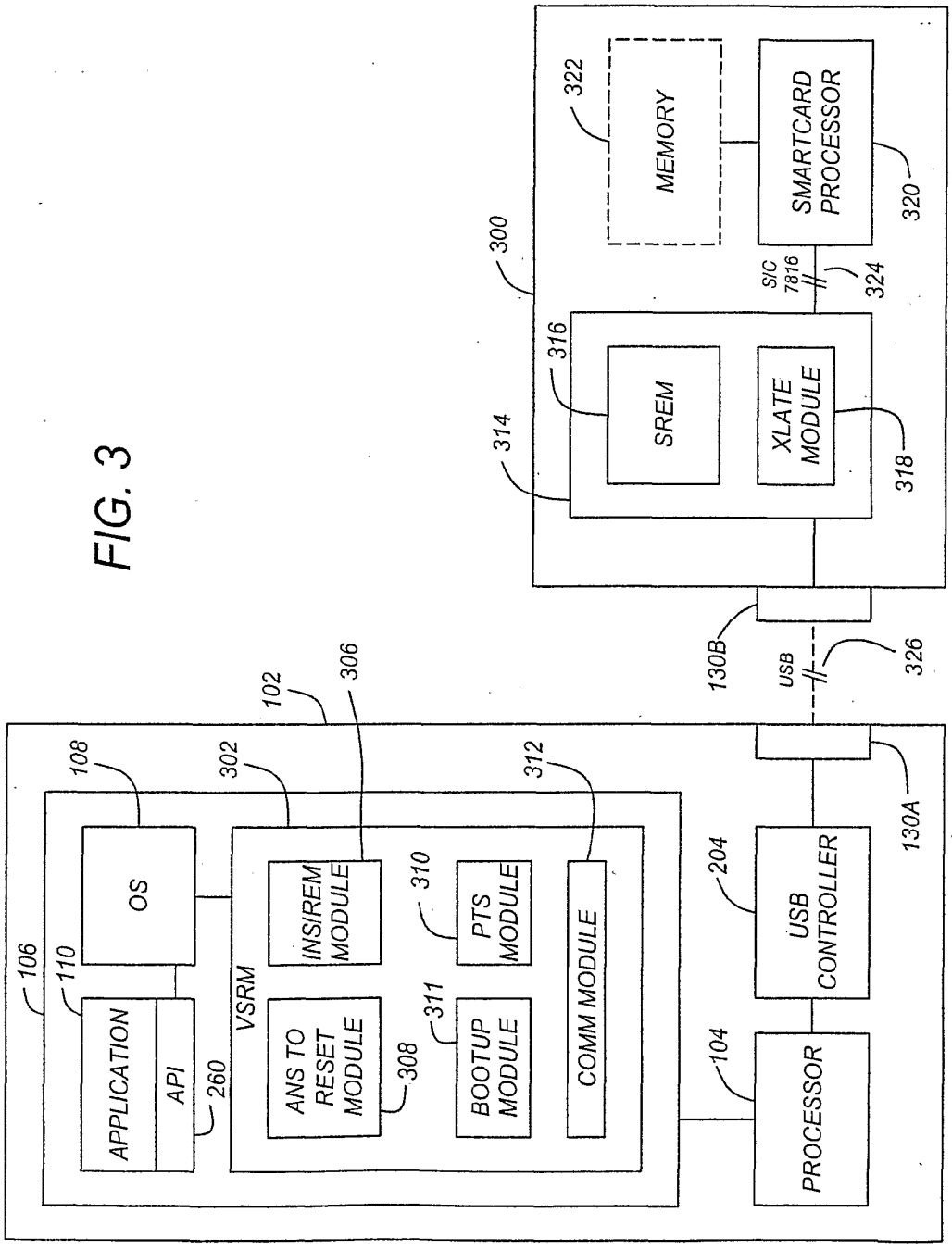

200
218
INPUT DEVICE
OUTPUT DEVICE
224
222
214
MEMORY
PROCESSOR
220
212
103B
102
108
202
OS
USB DRIVER
130A
204
USB CONTROLLER
106
110
APPLICATION
API
260
104
PROCESSOR

FIG. 2

FIG. 3


106
110
APPLICATION
API
260
108
OS
VSRM
302
ANS TO RESET MODULE
308
INS/REM MODULE
306
102
311
BOOTUP MODULE
310
PTS MODULE
312
COMM MODULE
104
PROCESSOR
204
USB CONTROLLER
130A
USB
326
130B
300
314
316
SREM
XLATE MODULE
318
S/C 7816
324
322
MEMORY
SMARTCARD PROCESSOR
320

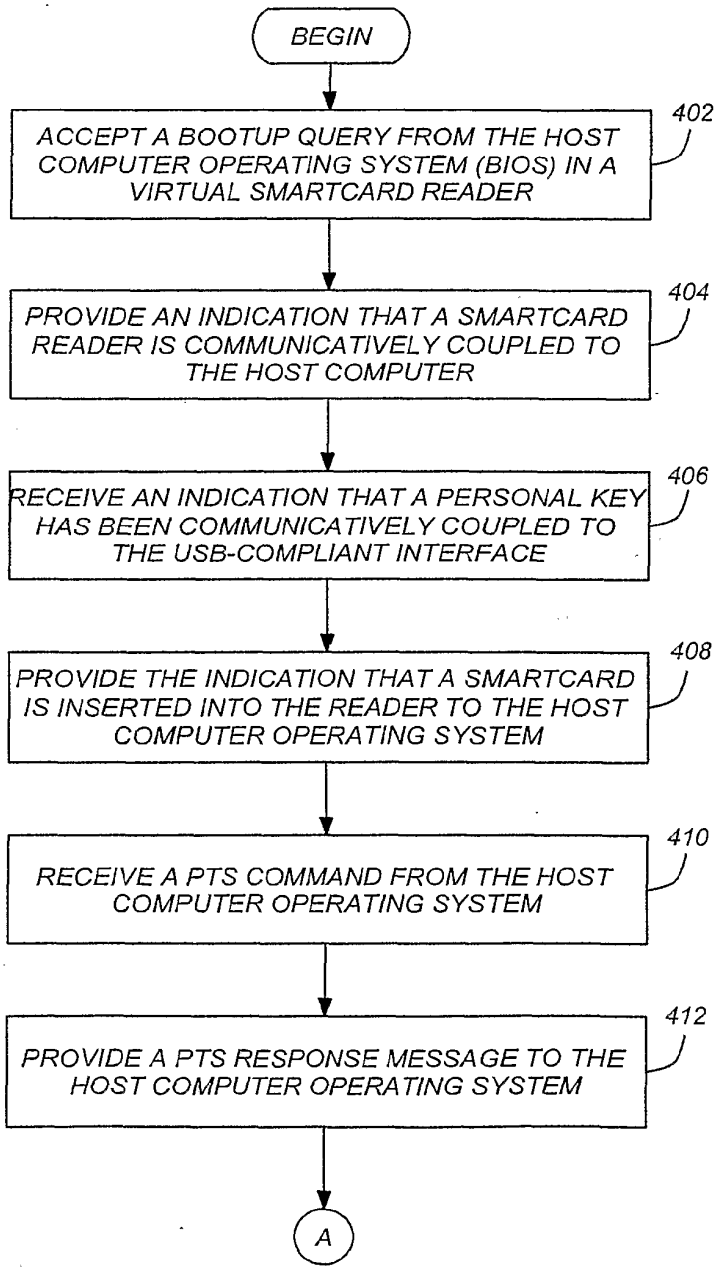

BEGIN
ACCEPT A BOOTUP QUERY FROM THE HOST COMPUTER OPERATING SYSTEM (BIOS) IN A VIRTUAL SMARTCARD READER
402
PROVIDE AN INDICATION THAT A SMARTCARD READER IS COMMUNICATIVELY COUPLED TO THE HOST COMPUTER
404
RECEIVE AN INDICATION THAT A PERSONAL KEY HAS BEEN COMMUNICATIVELY COUPLED TO THE USB-COMPLIANT INTERFACE
406
PROVIDE THE INDICATION THAT A SMARTCARD IS INSERTED INTO THE READER TO THE HOST COMPUTER OPERATING SYSTEM
408
RECEIVE A PTS COMMAND FROM THE HOST COMPUTER OPERATING SYSTEM
410
PROVIDE A PTS RESPONSE MESSAGE TO THE HOST COMPUTER OPERATING SYSTEM
412
A

FIG. 4A

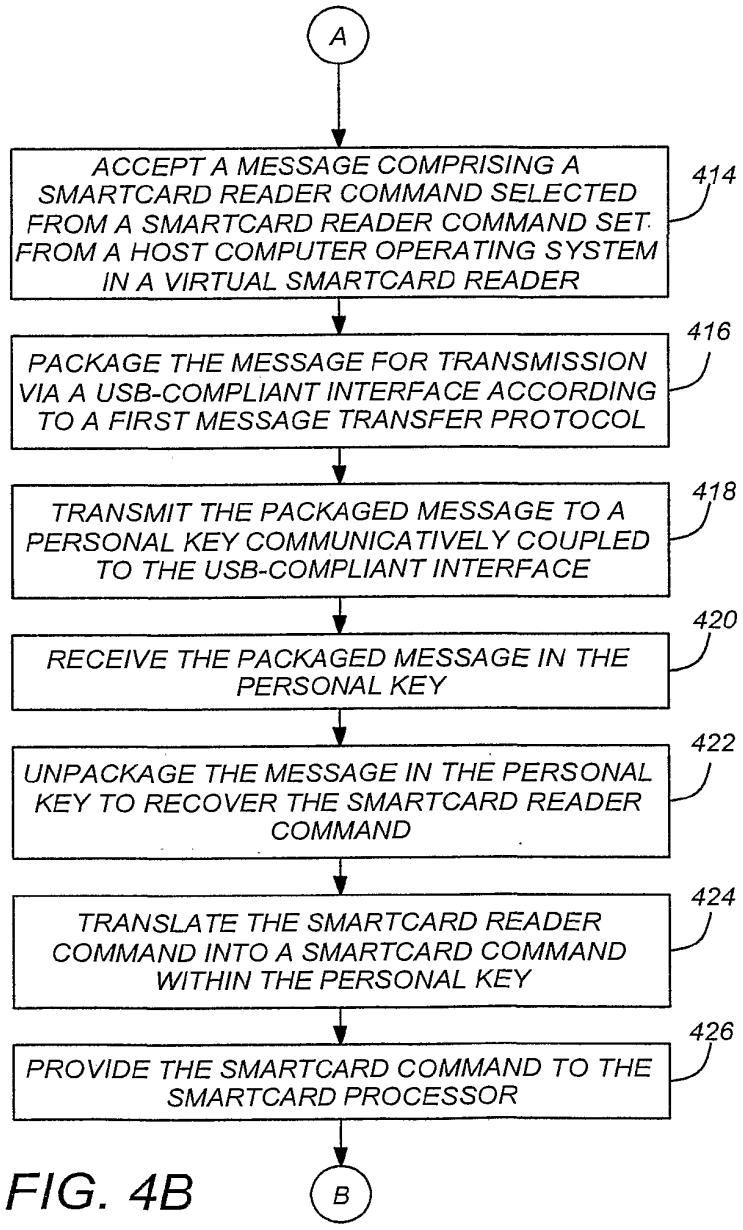

A
ACCEPT A MESSAGE COMPRISING A SMARTCARD READER COMMAND SELECTED FROM A SMARTCARD READER COMMAND SET FROM A HOST COMPUTER OPERATING SYSTEM IN A VIRTUAL SMARTCARD READER
414
PACKAGE THE MESSAGE FOR TRANSMISSION VIA A USB-COMPLIANT INTERFACE ACCORDING TO A FIRST MESSAGE TRANSFER PROTOCOL
416
TRANSMIT THE PACKAGED MESSAGE TO A PERSONAL KEY COMMUNICATIVELY COUPLED TO THE USB-COMPLIANT INTERFACE
418
RECEIVE THE PACKAGED MESSAGE IN THE PERSONAL KEY
420
UNPACKAGE THE MESSAGE IN THE PERSONAL KEY TO RECOVER THE SMARTCARD READER COMMAND
422
TRANSLATE THE SMARTCARD READER COMMAND INTO A SMARTCARD COMMAND WITHIN THE PERSONAL KEY
424
PROVIDE THE SMARTCARD COMMAND TO THE SMARTCARD PROCESSOR
426
B

FIG. 4B

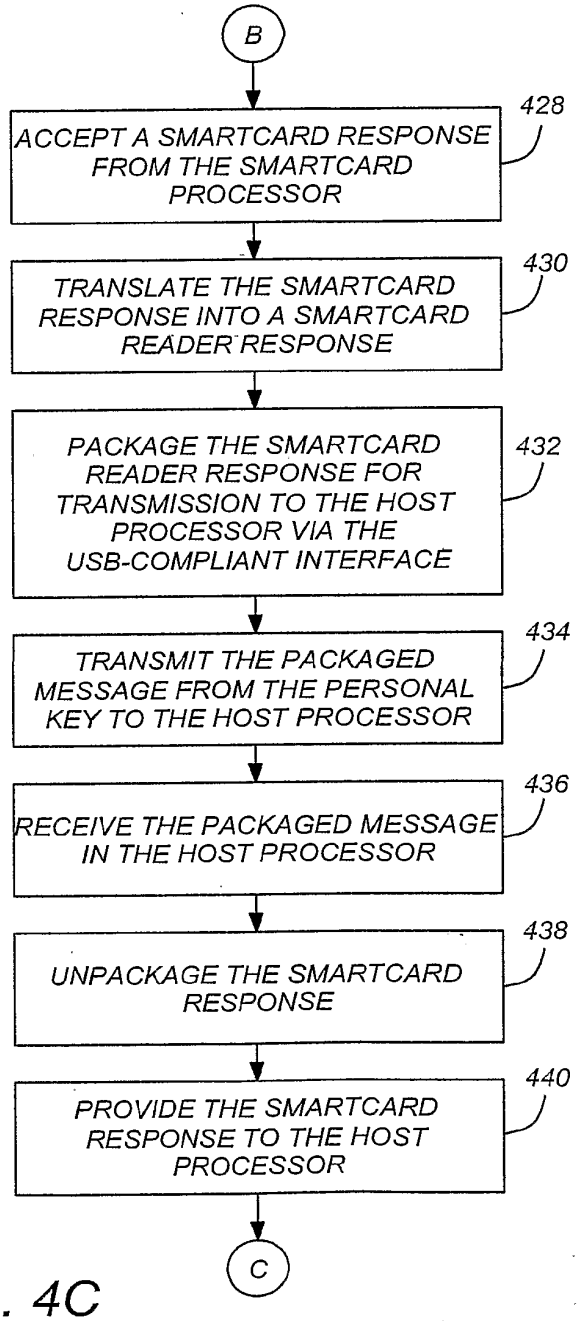

B
ACCEPT A SMARTCARD RESPONSE FROM THE SMARTCARD PROCESSOR
428
TRANSLATE THE SMARTCARD RESPONSE INTO A SMARTCARD READER RESPONSE
430
PACKAGE THE SMARTCARD READER RESPONSE FOR TRANSMISSION TO THE HOST PROCESSOR VIA THE USB-COMPLIANT INTERFACE
432
TRANSMIT THE PACKAGED MESSAGE FROM THE PERSONAL KEY TO THE HOST PROCESSOR
434
RECEIVE THE PACKAGED MESSAGE IN THE HOST PROCESSOR
436
UNPACKAGE THE SMARTCARD RESPONSE
438
PROVIDE THE SMARTCARD RESPONSE TO THE HOST PROCESSOR
440
C

FIG. 4C

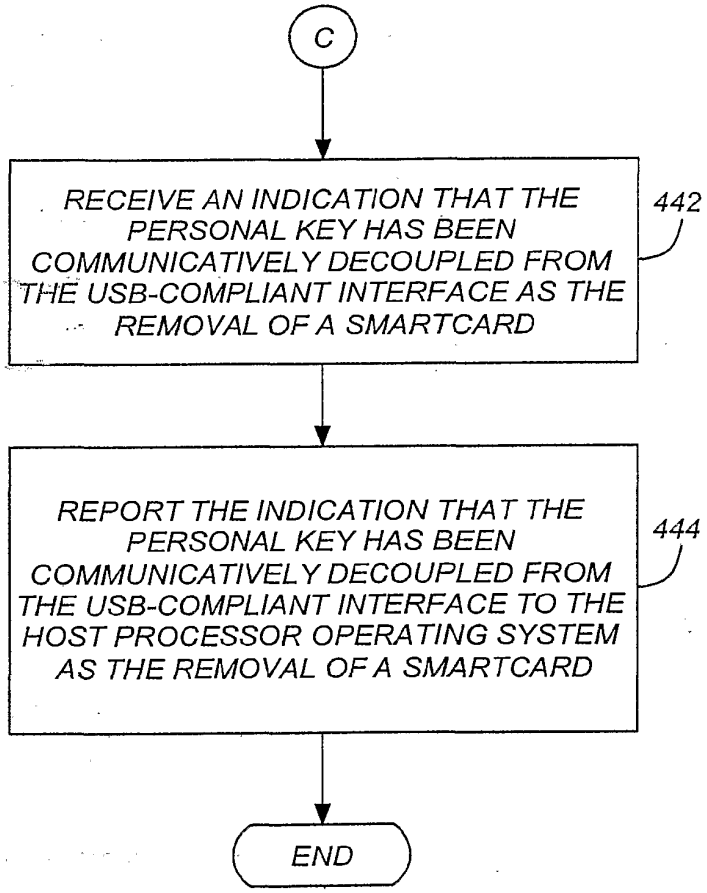

C
RECEIVE AN INDICATION THAT THE PERSONAL KEY HAS BEEN COMMUNICATIVELY DECOUPLED FROM THE USB-COMPLIANT INTERFACE AS THE REMOVAL OF A SMARTCARD
442
REPORT THE INDICATION THAT THE PERSONAL KEY HAS BEEN COMMUNICATIVELY DECOUPLED FROM THE USB-COMPLIANT INTERFACE TO THE HOST PROCESSOR OPERATING SYSTEM AS THE REMOVAL OF A SMARTCARD
444
END

FIG. 4D

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/014887 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP02/08069

(22) International Filing Date: 18 July 2002 (18.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/924,502 9 August 2001 (09.08.2001) US

(71) Applicant: ACTIVCARD IRELAND, LIMITED [IE/IE]; -, 30 Herbert Street, Dublin 2 (IE).

(72) Inventor: HILLHOUSE, Robert, D.; -, Unit 4B, 120 Holland Avenue, Ottawa, Ontario K1Y0X6 (CA).

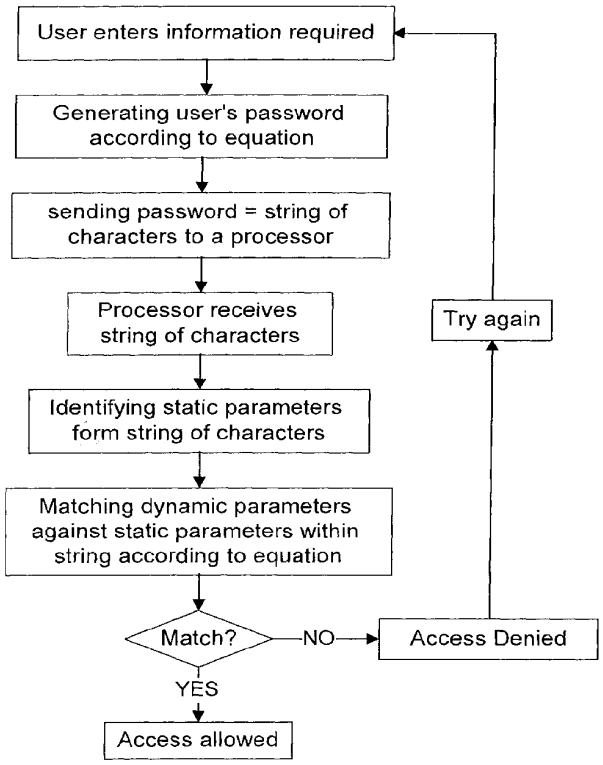
(74) Agent: CABINET JP COLAS; -, 37 avenue Franklin D. Roosevelt, F-75008 Paris (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR SUPPORTING DYNAMIC PASSWORD



(57) Abstract: A method of generating dynamic password is disclosed. A method of generating a dynamic password comprising the steps of providing a plurality of variable parameters, each parameter from the plurality of variable parameters being variable upon predetermined criteria; providing a plurality of predetermined static parameters; and processing at least some of the plurality of variable parameters and of the predetermined static parameters according to a dynamic password generating equation manipulating at least some of the plurality of variable parameters and of the predetermined static parameters resulting in an ordered sequence of dynamic and static parameters.

WO 03/014887 A2

Published:
— *without international search report and to be republished upon receipt of that report*

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.

Method for Supporting Dynamic Password

[001] The present invention relates to a method of generating passwords and more particularly to a method of generating a password that changes as a function of various parameters making the password dynamic.

Background of the Invention

[002] Security is fast becoming an important issue. Is has always been an issue for everybody to protect his belongings. It is also well known that with the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

[003] Preset codes are often forgotten, as users have no reliable method of remembering them. Writing down the codes and storing them in close proximity to an access control device (i.e., the combination lock) results in a secure access control system with a very insecure code. Alternatively, the nuisance of trying several code variations renders the access control system more of a problem than a solution.

[004] It is well known that a user determines a meaningful password, in the form of, for example, the name of their dog, the birth date of their child or an election year of the favorite candidate. This type of password is easily compromised with investigation. Conversely, a computer can randomly associates a password with a user, but this type of password is meaningless to the user and as such difficult to memorize. Consequently, the former method, which is simple, is insecure and the latter method, which is more secure, is difficult to use and often leads to a user writing their password next to their computer, thereby making the system insecure.

[005] The multiplicity of protected system encountered in the daily life of an individual renders the use of password particularly inconvenient, because a user has to remember a password for each accessible system. For example, the user must remember passwords for accessing network, database, E-mail, bank machine, personal

voice mails at home and at work, etc. The plurality of the systems wherein a password is needed favors a single simple password for all systems. In addition, a skilled person may find a predetermined password given sufficient time, rendering the system insecure. In more sophisticated theft situations, "Trojan horse" type viruses can be used to capture a user ID number and password that have been entered at a keyboard or across a network connection. That is, the user thinks he is logging on as usual, but the dialogue box in which the data is entered is really a look-alike window that is capturing his keystrokes.

[006] To secure access to a network, a further system was developed that relies on a user's personal information. A user requesting access to the network is prompted to answer a series of questions regarding his private life displayed on a computer screen. Such questions might be related to a relative's date of birth, a bone that was broken during childhood, a year of his first car accident, insurance company, address in January 1994, name of his first girlfriend, etc. The computer checks the validity of the answers before allowing access to the user. A computer is programmed with pertinent questions to ask a user and answers associated therewith, and when the system is initialised, the user enters the answers a first time, they are stored in a memory of the system, and are associated with the user identity. The time taken to answer all the questions prior to gaining access to the system is burdensome. It is evident that a major inconvenient with such a system is that a skilled person can find enough information of a personal nature relating to a user for answering properly the questions, and as such render the security ineffectual.

Object of the Invention

[007] To overcome such disadvantages, it is an object of this invention to provide a method for rendering a computer system access more secure.

[008] It is another object of this invention to provide a method for generating dynamic password.

[009] It is a further object of this invention to provide a method for generating a dynamic password dependent on various dynamic parameters.

Summary of the Invention

[0010] In accordance with a preferred embodiment of the present invention, there is provided a method of password verification comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter;

providing at least a variable parameter as a known password;

determining from data available to an individual and from the known password a static string;

providing the determined static string as a password for verification;

verifying the static string to determine that it is an accurate transformation of the at least a variable parameter according to the provided process and when the determination is that the transformation is accurate, providing an indication that the password is verified.

[0011] In accordance with another preferred embodiment of the present invention, there is provided a method of changing dynamic passwords comprising the steps of:

providing a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a variable parameter variable upon predetermined criteria;

receiving the provided string of characters; and,

storing data based on the known password, the data sufficient for verifying provided passwords to determine their accuracy.

[0012] Advantageously, the invention provides a method of verifying a dynamic password comprising the steps of:

receiving a password comprising a string of characters wherein the characters are sequenced according to a predetermined sequence of variable parameters and static parameters;

identifying static parameters within the string of characters;

determining dynamic parameter values related to the dynamic parameters in accordance with the predetermined sequence ;

comparing static parameters received within the string of characters with previously stored static parameters and the received dynamic parameter within the determined dynamic parameters to determine a first comparison result;

wherein upon both the first comparison result being indicative of a match, the dynamic password is validated.

Further advantageously, the invention provides a method of generating a dynamic password comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter; and,

providing at least a variable parameter as a password, the provided variable parameter provided by an individual via a data entry device.

Brief description of the drawings

[0013] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0014] Fig. 1 is a computer screen display of a password dialog box;

[0015] Fig. 1a is an example of a filled password dialog box on a computer screen display;

[0016] Fig. 2 is a flow diagram of a method of evaluating a dynamic password generated according to the present invention;

[0017] Fig. 3 is an illustration of a computer screen displaying some possible images incorporated in the password;

Detailed Description of the Invention

[0018] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each

employee. However, it is necessary to limit access of a company's network to the company's employees. As such, Fig. 1 is an example of a screen display prompting an employee to enter a login identity and an associated password to allow the employee to access the network. An example of a filled dialog box is shown in Fig. 1a. Classically, the login identity is the user's first name, illustrated here, as "Smith" and an exemplary password is "Fido", their dog's name. For security purpose, each character of the password is replaced with a star on the display so that nobody can read it. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified their password during a previous session. An ill-intentioned person can easily find out this type of static password and freely enter a company's network system.

[0019] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to enter a new password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. However, due to the multiplicity of the systems and the recurrence of the demand, employees often use the same password to which a number is just added. For example, the "Fido" password becomes after a change request "Fido1". During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent person may rapidly find out the password of a user and access a company's network..

[0020] As mentioned, the fact that the password remains unchanged during a long period of time between two modifications renders the system insecure. It will be advantageous to provide a security system based upon a dynamic password, i.e. a password comprising at least one parameter that changes in an uncontrollable way.

[0021] A most probable parameter that is uncontrollably variable is a parameter related to time. It is therefore advantageous to introduce a parameter related to the time in a dynamic password generation process because the time can be used in many ways such as hour of the day, day of the week/month, age, etc. By introducing at least a time parameter into a dynamic password generating equation, a password is automatically and deterministically different nearly every time it is used. The password mostly comprises some static or passive parameters such as the name of the user and perhaps

also isolated letters that may complicate the determination of the password. An example of such a dynamic password generating equation is shown below:

[0022] $hour + "Smith2" + $mday + 23 + "I" + ($hour + 16)/2

[0023] Where the uncontrollably variable parameters are:

hour that represents the hour of the day, and mday that represents the day of the month.

[0024] Where the static parameters are:

Smith2 that represents the user's name and can be easily remembered by the user and I is an isolated letter.

[0025] The dollar sign indicates a variable parameter, and the quote sign is indicative of static parameters. Alternatively, the distinction between static and variable parameters is made another way or using other characters.

[0026] Assuming that a user wants to access the company's network at 8:22 am on May 25, and has the account Smith, she determines from the variable password equation her password at the present time. Here it is:

8Smith248I12

[0027] and enters it into the system which verifies it. Anyone trapping the password and storing it for later use will be sadly disappointed because the password will expire one hour later while Smith easily determines the correct password an hour later without needing to change the password on the system.

[0028] Of course, the predetermined equation shown here is just for illustrative purpose. In the present example, only two different variable parameters are in the equation, there is no limitation as to the number of these parameters or as to the number of static parameters. However, it is most probably difficult to introduce too many parameters in a single equation, either variable or passive, because the user has to remember them and their combination, and as such has to memorize at least the order in which the various parameters have to be entered. Advantageously, the parameters variable and passive are not difficult to memorize because they are certainly available and easily accessible by the user such as the hour of the day, the date or a name, a word of the day, etc.

[0029] Referring now to Fig. 2, a flow diagram of a method of validating a dynamic password is illustrated. The user needs to know the equation for generating the dynamic password. In the present example the equation is:

$$\$hour + \text{“Smith2”} + \$mday + 23 + \text{“I”} + (\$hour + 16)/2,$$

the user provides the hour of the day – “8” -, the characters “Smith2” followed by the value 48 being the day of the month plus 23, the letter “I” and 12 being (8+16)/2. The processor receives the string of characters for verifying the validity of the dynamic password. The processor generates a same password to verify that the user's password and then compares the characters within the string relative to the generated string according to the equation.

[0030] Eventually, a problem might rise when a password is entered at a time close to a change of the hour, for example. For example, assuming a variable parameter corresponds to the hour a user is entering a password, if the user's watch indicates 7:58 am, which is a time close to changing from 7 to 8, and the computer's watch has already turned over 8, the user might be rejected because the user password indicates a character 7 where the computer waits a 8. Even in these situations, it is easy for a user to either wait a few minutes or to realize that the system hour may be 7 or 8. Of course, synchronizing computers to the network password server clock will obviate this problem so long as users verify the time on their computers and not with their watches or desk clocks. Eventually, during a short period of time of a few minutes overlapping a change of hour as in the previous example, the network server accepts a password wherein the character indicative of the hour is incorrect within predetermined limits. In the previous example, the computer accepts password comprising the character 7 instead of 8 for indicating the hour. Similarly, if the user's watch indicates 8:02 am, and the computer's watch indicates 7:58 am, the computer accepts password comprising the character 8 instead of 7 for indicating the hour.

[0031] What may introduce a difficulty for a user are the numbers to memorize and eventually the operations to perform to complete the password. There are no prerequisites to incorporate operations in an equation for generating a dynamic password. Similarly, there is no prerequisite not to incorporate operations while

elaborating or programming the dynamic password generating equation for securing a network access.

[0032] In a further embodiment, the generation of a dynamic password relies again on a predetermined equation wherein an image is introduced as a parameter along with the variable and the static parameters. Referring to Fig. 3, a computer screen is displaying a plurality of images including various shapes, animals, trees, and different symbols. An image of a series as the one illustrated in Fig. 3 is part of a dynamic password generating equation. An example of such a dynamic password generating equation is shown below:

$hour + "Smith2" + $image

Where the variable parameter is: hour that represents the time of the day.

Where the static parameter is: Smith2 - the user's name.

Where the image parameter is: image

[0033] Where the dollar sign indicates a variable parameter, the quote sign is indicative of a static parameter.

[0034] Assuming that the user wants to access her company's network at 8:22 am. An image is presented in the dialogue box asking for her password. For example, a tree may be displayed. In that instance, the user enters a password according to the above-predetermined dynamic password generating equation. The password will thus be in the form of:

8Smith2tree

[0035] Advantageously, an interpretation of the image is as valid as the image itself. For example, if the imaged tree is a pine, the password might reflect this particularity and incorporate the tree species. Moreover, English is not the exclusive language that can be used to describe a tree. Indeed, computers of large companies, especially international companies, are preferably programmed to accept passwords generated in any of a number of possible languages. Alternatively, only the user's mother tongue is accepted for a given password entry. Consequently, incorporating an image in the equation allows multiple other possibilities for the resulting password.

[0036] Back to the previous example and the possibilities allowed with a single image of a tree, here are 3 of the possible passwords:

8Smith2tree

8Smith2pine

8Smith2arbre

[0037] All the images are interpreted to a certain extent. For example, if an image of a bulb is selected, the possible words illustrating a bulb, not withstanding a foreign language, might be lamp, idea, light, lightbulb, bulb, eureka, etc. Of course the flexibility in image identification is a parameter that is set during system implementation or alternatively as an option to be set by a system administrator.

[0038] Thus, generating a dynamic password incorporating an image in the equation along with the variable and the static parameters also makes the system less secure when variability of many parameters is supported. That said, since the image is not immediately discernible to an unauthorized individual and its location within the password is unknown, it is believed that overall security will increase when the system is used by unconcerned individuals – individuals who are not specially trained in computer security.

[0039] In the example shown here, only one variable, one static, and one image parameter form part of the predetermined equation for generating the password but of course, there is no limitation as to the number of these parameters. The limit that may be taken into consideration is the good will of the user as to his capacity to memorize parameters to enter when prompt to do so. Additionally, there is no prerequisite to incorporate operations in the equation for generating a dynamic password. Similarly, there is no prerequisite not to incorporate operations while elaborating or programming the dynamic password generating equation for securing a network access.

[0040] Even though a dynamic password offers enormous advantages over static passwords, it is beneficial to have the possibility to change the password from time to time to decrease drastically the possibility to compromise security of the system. A way to achieve such beneficial possibility is to assign a code to the different parameters that compose a dynamic password. A code might be of various forms as for example an

Arabic number, or a Roman numeral, or a letter, etc. The codes are assigned, for example, according to a predetermined setting or more probably are randomly assigned.

[0041] Referring to a previous example wherein the dynamic password generating equation was in the form of:

$hour + "name2" + $image

[0042] A first possibility is to determine as many codes as parameters in the equation. So in the present example, three codes are assigned:

Possibility 1	Possibility 2	Possibility 3
code 1 → hour	code 1 → name	code 1 → image
code 2 → name	code 2 → image	code 2 → hour
code 3 → image	code 3 → hour	code 3 → name
Possibility 4	Possibility 5	Possibility 6
code 1 → hour	code 1 → name	code 1 → image
code 2 → image	code 2 → hour	code 2 → name
code 3 → name	code 3 → image	code 3 → hour

[0043] An advantage in coupling codes to parameters is that the codes can be ordered arbitrarily by the server, allowing for a multiplicity of representations of a same password. Thus, intercepting the password equation is of limited value. Also, often codes are easier to enter than textual representations of parameters. Effectively, by changing the code assignment, the password though unchanged, appears differently to a Trojan Horse application and is therefore more difficult to decode. Also, it is unclear what each code entry refers to. Here, there exist 6 possibilities of reassigning the three codes to the three parameters, which leads to six different possible password entries resulting in the three identical parameters in the same sequence as in the Possibility 1.

[0044] To drastically increase the password's possibilities wherein the same dynamic and static parameters are initially required, the number of codes can exceed the number of parameters. For example, if 10 codes are available and 5 parameters are required for generating a dynamic password, the number of possibilities is increased according to the combination of 5 codes chosen from 10 to obtain an arrangement of the

parameters identical to the arrangement required in the equation. Consequently, the number of possibilities is increased by about 252. Of course, these numbers are cited for exemplary purpose only, the number of codes available is not limited to any of the mentioned numbers.

[0045] Static parameters as used in the specification denote parameters that do not change. These can include string values and defined answers to questions that do not change. For example, "iQw4" is a string. Another static parameter is a user's name, employee number, address, etc. Which are determined and unchanging parameters. Of course, the static parameters can also be identified within passwords by encoded value in order to make interception of the password during password changes more difficult.

[0046] When a system has access to a significant amount of data, it is also possible to relate the password to data known to the system. Some example variable parameters include: days to a new moon, days until a product release, days since year end, months since hiring, years since hiring, employee age in years, months since last vacation week, number of people on vacation within a person's group, amount on last paycheck, taxes deducted on last paycheck, amount in employee savings plan, and so forth. Also, posted data is useful such as today's lunch menu items, word of the day, and so forth.

[0047] In order to verify a password when provided, there are several possible methods. According to a preferred embodiment, the static portions of the password are hashed either separately or in a concatenated or other joined form. The hashed value is stored. When a password is received, it is separated into static and dynamic values. The dynamic values are regenerated to verify the dynamic values. The static values are hashed and the hash values are compared. As such, the resulting static portions are not stored on the server and cannot be detected by a snooping device. The dynamic parameters are stored in an encoded fashion that is typically other than human intelligible. For example, if 256 variable parameters are known, the variable parameters are stored as 8 bit values.

[0048] Alternatively, the dynamic values are verified without regenerating same. For example, if the variable parameter is day of month + 23, then the verification process merely subtracts 23 from the provided value and compares the result to the

present day of the month. Of course, other methods of password verification are possible.

[0049] Advantageously, the dual composition of these passwords, i.e. dynamic and static values renders the dynamic passwords usable with various existing system without requiring any other support. Typically, a password is used for activating encryption keys for encrypting data. Advantageously, the static values of a dynamic password are used as keys like typical passwords. However, the presence of dynamic values in combination with the static values in a dynamic password increases the security of the system. That said, even if static values are potentially accessible to an unauthorized individual, their location within the password is unknown. Therefore, accessibility to encryption data is possible thanks to the static values and moreover, the accessibility is protected by the dynamic values.

[0050] Numerous other embodiments might be envisioned without departing from the scope and the spirit of the present invention. For example, the description of the invention implicitly inferred that the dynamic password generating equation was identical for all the employees of a company. The difference between the dynamic passwords of two employees login in at the same time being the static parameters. However, each employee can have a specific dynamic password generating equation. The multiplicity of equations, i.e. as many equations as employees, might be advantageous if an employee leaves the company. In such a case, the equation is deleted and nobody else in the company is affected, otherwise, the whole system must adapt to the departure for keeping the system as secure as possible.

Claims

What is claimed is:

1. A method of password verification comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter;

providing at least a variable parameter as a known password;

determining from data available to an individual and from the known password a static string;

providing the determined static string as a password for verification; and,

verifying the static string to determine that it is an accurate transformation of the at least a variable parameter according to the provided process and when the determination is that the transformation is accurate, providing an indication that the password is verified.

2. A method according to claim 1, characterized in that the step of verifying the static string includes the steps of:

performing the process for transforming at least a variable parameter on the known password to determine a second static string;

comparing the provided static string with the second static string to determine a comparison result and,

when the comparison result is indicative of a match, providing an indication that the password is verified.

3. A method according to claim 1, characterized in that the at least a variable parameter includes an uncontrollably variable parameter.

4. A method according to claim 2, characterized in that the at least a variable parameter includes at least a static parameter.

5. A method according to claim 1, characterized in that the process includes steps of determining from present time data, a current value for a variable parameter relating to time.

6. A method according to claim 1, characterized in that the process includes steps of providing data to a user for interpretation by the user and then comparing the user's interpretation to a predetermined known interpretation.

7. A method according to claim 6, characterized in that the provided data is an image and the interpretation is a string indicative of the image.

8. A method according to claim 1, characterized in that the known password is provided by a user.

9. A method according to claim 8, characterized in that the known password is entered as a string of characters and wherein at least a character is indicative of one of a variable parameter and a static parameter.

10. A method according to claim 9, characterized in that the string of characters is parsable to form the known password, the parsing distinguishing variable parameters from static parameters within the known password.

11. A method of changing dynamic passwords comprising the steps of:

providing a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a variable parameter variable upon predetermined criteria;

receiving the provided string of characters; and,

storing data based on the known password, the data sufficient for verifying provided passwords to determine their accuracy.

12. A method of changing dynamic passwords according to claim 11, comprising the step of:

with a processor parsing the provided string of characters to distinguish static data from the at least a variable parameter.

13. A method of changing dynamic passwords according to claim 11, characterized in that the parameters are selected from a plurality of available parameters and characterized in that the plurality of available parameters are provided to a user for selecting thereform.

14. A method of changing dynamic passwords according to claim 13, characterized in that the plurality of available parameters are each represented by an identifier and characterized in that the identifier for a given parameter in one instant is different from the identifier for a same parameter in another instant.

15. A method of changing dynamic passwords according to claim 11, characterized in that the step of storing data based on the known password comprises the steps of:

extracting static data from the known password;

hashing the extracted static data to determine at least a static hash value;

storing the at least a static hash value; and,

extracting dynamic data from the known password and storing indications of the dynamic data.

16. A method of verifying a dynamic password comprising the steps of:

receiving a password comprising a string of characters wherein the characters are sequenced according to a predetermined sequence of variable parameters and static parameters;

identifying static parameters within the string of characters;

determining dynamic parameter values related to the dynamic parameters in accordance with the predetermined sequence ;

comparing static parameters received within the string of characters with previously stored static parameters and the received dynamic parameter within the determined dynamic parameters to determine a first comparison result;

wherein upon both the first comparison result being indicative of a match, the dynamic password is validated.

17. A method of generating a dynamic password comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter; and,

providing at least a variable parameter as a password, the provided variable parameter provided by an individual via a data entry device.

18. A method of generating dynamic passwords according to claim 17, characterized in that the plurality of variable parameters comprises uncontrollably varying parameters.

19. A method of generating dynamic passwords according to claim 18, characterized in that the predetermined criteria for varying the variable parameters is characteristic of a time frame.

Fig. 1

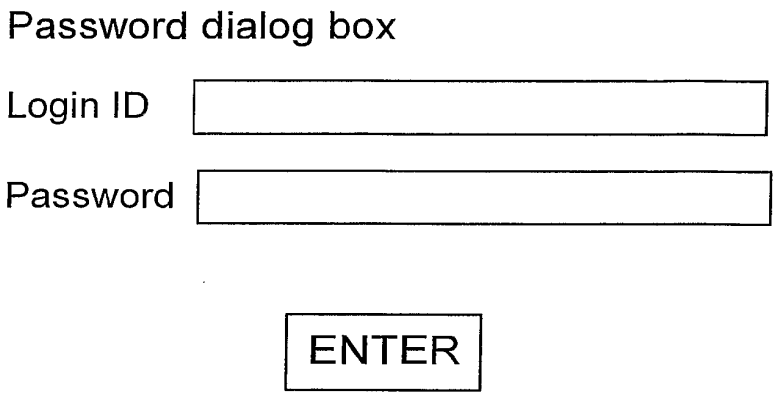
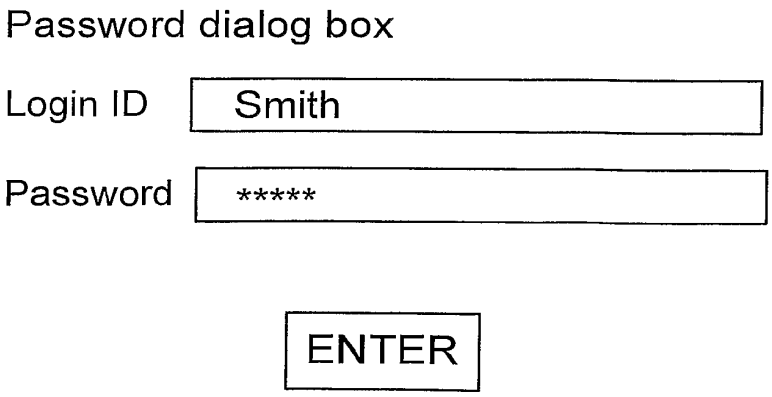

Password dialog box
Login ID
Password
ENTER

Fig. 1a


Password dialog box
Login ID
Smith
Password
*****
ENTER

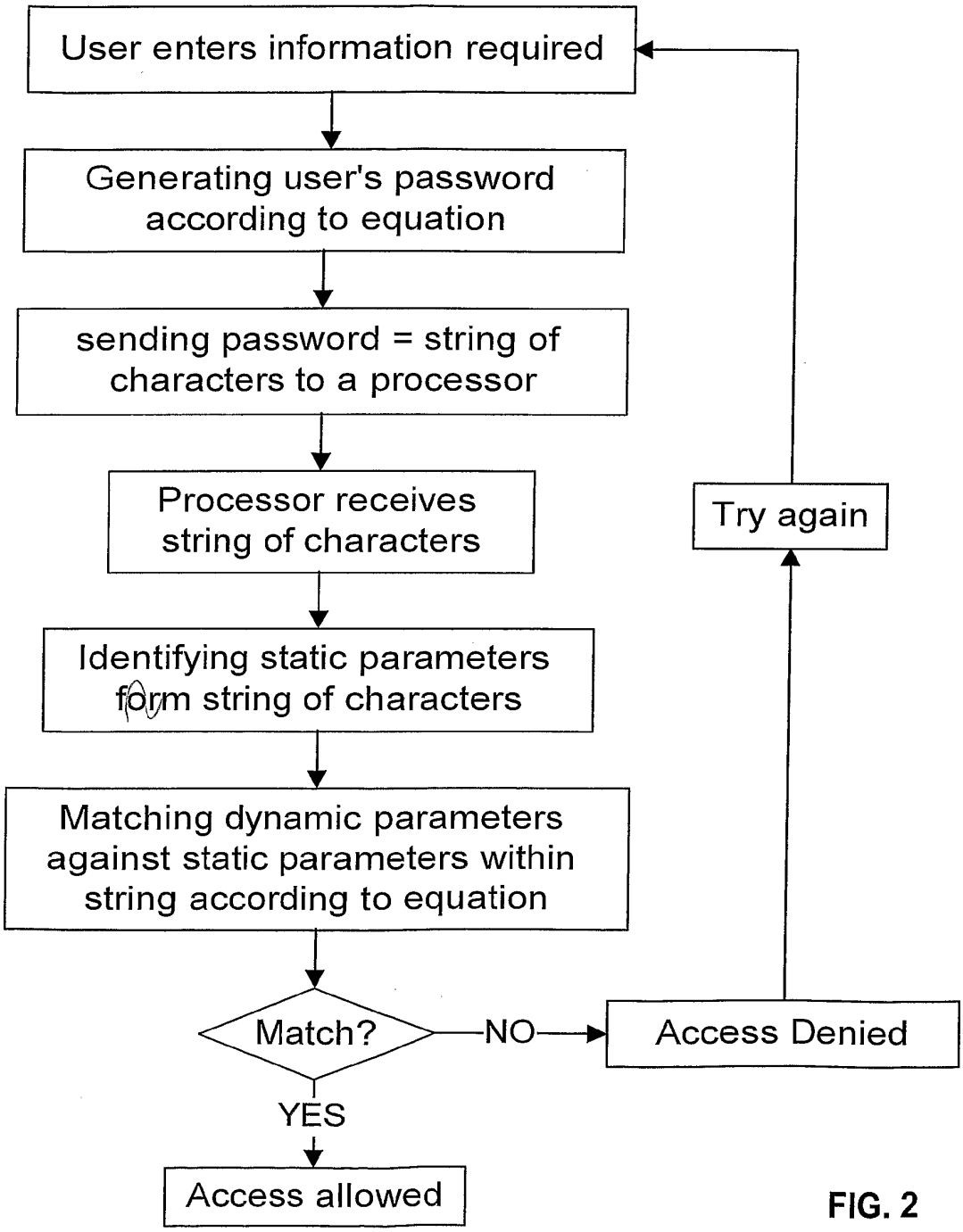

User enters information required
Generating user's password according to equation
sending password = string of characters to a processor
Processor receives string of characters
Identifying static parameters form string of characters
Matching dynamic parameters against static parameters within string according to equation
Match?
NO
Access Denied
Try again
YES
Access allowed

FIG. 2

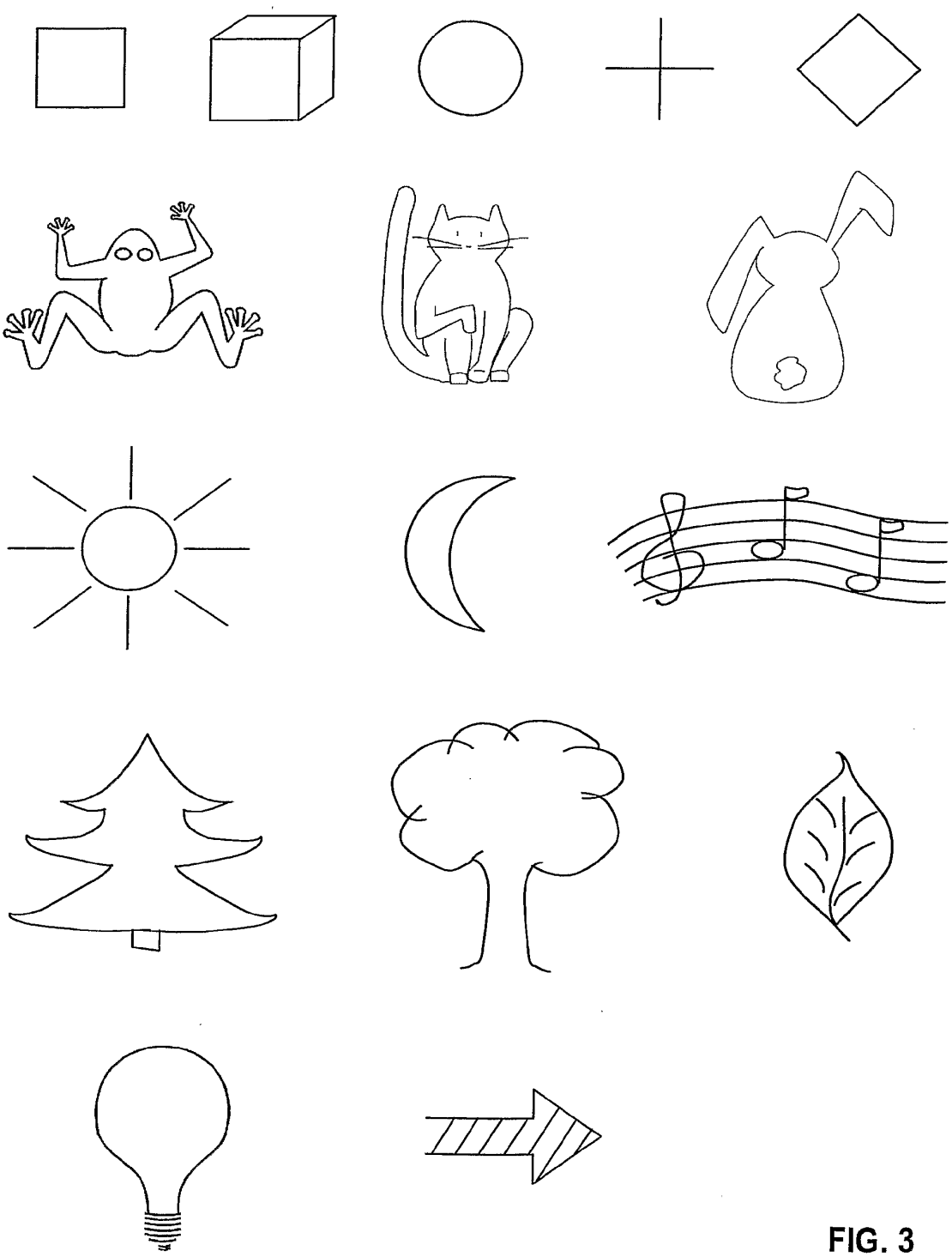


FIG. 3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2003 (24.04.2003)

PCT

(10) International Publication Number
WO 03/034189 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP02/11445

(22) International Filing Date: 11 October 2002 (11.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/977,202 16 October 2001 (16.10.2001) US

(71) Applicant: ACTIVCARD IRELAND, LIMITED [IE/IE]; 30 Herbert Street, 2 DUBLIN (IE).

(72) Inventor: CHARBONNEAU, Marc; 23, Terrace Sauve, Casselman, OTTAWA, Ontario KOA 1MO (CA).

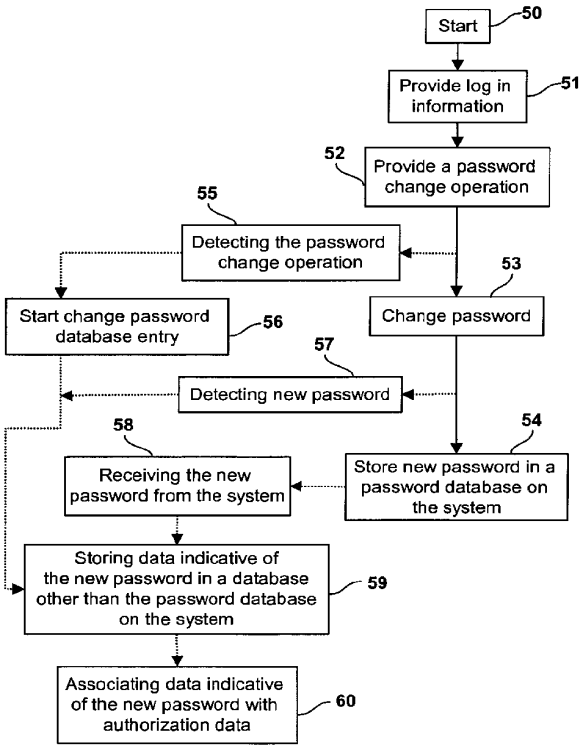
(74) Agent: CABINET JP COLAS; 37, avenue Franklin D. Roosevelt, F-75008 PARIS (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR SUPPORTING SINGLE SIGN ON



(57) Abstract: A method of securely supporting password change is disclosed. The method comprises the steps of: detecting an occurrence of a password change operation (55) in execution on a system and receiving a new password by the system; detecting the new password when provided (57); storing data indicative (59) of the new password in a database other than the password database of the system for later retrieval, the data indicative of the new password for provision to the system.

WO 03/034189 A2

Published:
— *without international search report and to be republished upon receipt of that report*

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.

Method for Supporting Single Sign On

[001] The present invention relates to a method for changing password data, and more particularly, to a method for securely supporting password change for a central database of passwords independent of some processes with which the password is associated.

Background of the invention

[002] Security is fast becoming an important issue. It is well known that with the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

[003] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each employee. However, it is necessary to limit access of a company's network to the company's employees. As such, prior to access the company's network, a password window prompted the company's employees to enter a login identity and an associated password. Usually, a user specifies passwords. Most users, being unsophisticated users of security systems, classically choose as the login identity their first name, and their dog's name as a password for example. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified his password during a previous session. As such, many password systems are easily accessed through a simple trial and error process.

[004] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to change their

password, or are required to run a specific routine to change their password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent person may rapidly find out the password of a user and access a company's network.

[005] Optionally, a password is stored in a password database and user authorisation information such as biometric information, a digital key, a smart card, or a global password is required to retrieve the password. When the password is retrieved, it is provided to the password window. It is known to those skilled in the art that a biometric identification system accepts unique biometric information from a user and identifies the user by matching the information against information belonging to registered users of the system. Fingerprint sensing and matching is a reliable technique for personal identification and/or verification.

[006] The combination of a password and biometric information such as a fingerprint for example is beneficial because it increases the security and limits accessibility to a system. However, an association between a biometric information sample and a password also raises a problem when the password is changed. If an individual changes his password manually using, for example, a change password command of a password protected system, a next time he wants to access the system and provides his fingerprint, his old password is retrieved and provided to the password prompt. The old password is not current and therefore a message indicating that the password is incorrect is provided for the user. Thus, the user has to manually type in the new password. Eventually, the user can run a password change routine wherein the old password is provided along with the fingerprint, the new password typed in and the biometric sample assigned from then to the new password.

Object of the Invention

[007] To overcome such an inconvenience, it is an object of this invention to provide a method for automatically assigning a new password.

[008] It is another object of the present invention to provide a method of detecting a password change operation in a system and prompt for a new password.

[009] It is another object of the present invention to provide a method of detecting a password change command and authorizing a password change operation.

Summary of the invention

[0010] In accordance with the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting at least one of the operations in execution on a system comprising: detecting a password change operation, and detecting a new password storage operation; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0011] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for a new password, the prompt independent of the password change operation; receiving the new password; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored..

[0012] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for authentication information, the prompt independent of the password change operation; receiving the authentication information; when the authentication information is indicative of a known user, providing a password associated with the user to the system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new

password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0013] In accordance with another preferred embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored; wherein the system has a known user authorized thereon, and wherein the step of performing an operation to change the password comprises the step of automatically generating a new password.

Brief description of the drawings

[0014] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0015] **Fig. 1** is a flow diagram of a prior art method of associating a password to a fingerprint upon a match of a fingerprint with an associated template;

[0016] **Fig. 2** is an example of a prior art password window dialog display;

[0017] **Fig. 2a** is an example of a filled password window dialog box on a computer screen display;

[0018] **Fig. 3** is a flow diagram of a prior art method of changing password;

[0019] **Fig. 4** is a flow diagram of a prior art method of retrieving the password for provision to the system;

[0020] **Fig. 5** is a flow diagram of a method of securely supporting password change in accordance with a preferred embodiment of the present invention;

[0021] **Fig. 6** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention;

[0022] **Fig. 7** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention; and,

[0023] **Fig. 8** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention wherein a choice is given to the user.

Detailed description of the invention

[0024] In the prior art, many security systems involving imaging fingerprints to allow access for example to a building, to a specific area within a building, to a computer, are described. The security systems wherein biometric information is used for identifying and authorizing access to an individual mostly rely on a prior art method as shown in Fig.1. Following a starting step 10, after a biometric information sample, in a form of a fingerprint for example, has been provided to a system at step 11, in order to generate a fingerprint, a fingertip is imaged to generate an image thereof, which is called a fingerprint or a fingerprint image. The fingerprint is then characterized at step 12. During the process of identification, the characterized fingerprint is compared to stored templates associated with fingerprints of the person at step 13 – for a one-to-one identification system - or of any person registered for access the system – in a one-to-many identification system. Upon a positive result of the comparison, when there is a match between the provided fingerprint and a stored template associated with a fingerprint at step 14, the system provides at step 15 a password associated with the stored template to, for example, a legacy password based system and the user is identified and authorized at step 16.

[0025] Referring to Fig. 2, an example of a screen display prompting an employee to enter a login identity in 21 and an associated password in 22 to allow the employee to access the network. An example of the display of Figure 1 filled in is shown in Fig. 2a. Classically, the login identity is the user's name, illustrated here, as "Smith" in 23. For security purpose, each character of the password is replaced with a star on the display so that nobody can read it as shown in 24. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has changed his password during a previous session.

[0026] Optionally, to make the system more difficult to break, the network system is organized in such a way that, regularly, all the employees are prompted to enter a new password in order to change the passwords at regular intervals. Often, the system allows the users to combine a non-predetermined number of letters, either small or capital, and digits in their passwords. Referring to Fig. 3, a prior art method of changing passwords is shown. After a starting step 30, in order to access a system at step 32, the password change window prompts a user to provide an identity and the old password associated with the provided identity at step 31. Once authorized, the user is able to provide the system with a new password at step 33. Typically, the user is prompted to type in a new password two times as shown at step 34. The new password is stored in a password database of an application or operating system related to the password change operation on the system and now replaces the old password at step 35 before an ending session at 36.

[0027] Referring now to Fig. 4, a flow diagram of a method of retrieving the password for provision to the system is shown. For accessing a system after a starting step 40, a user provides authorization data at step 41, in the form of biometric information sample or information stored on a smart card. The authorization data is verified and is used to retrieve data indicative of the user password at step 42. Upon provision of the authorization data, the password is retrieved from a database other than the password database of the system or application at step 43 and provided to the system or application so that the user can gain access thereto.

[0028] The authorization data permits identifying a user based on, for example, biometric information provided therefrom. This provides an indication that the correct person was actually present when the request for changing a password was provided. A major advantage of using biometric information for retrieving a password is that the password does not have to be memorized. Typically, the user provides biometric information from a biometric source. The biometric information is characterized, processed and compared against templates stored in the system. Upon a match of the features extracted from the templates and the characterized biometric information corresponding to the biometric source provided by the user, an authorization signal is either provided or denied.

[0029] Referring now to Fig. 5, a method for securely supporting password change in accordance with a preferred embodiment is shown. To facilitate the comprehension of the figure, lines are plain for showing a classic password change routine flow, whereas dashed lines show changes in process flow for securely supporting password change. Each individual also has access from its workstation to a password change command. It is understandable that when a user has any doubt concerning the confidentiality of his password, he can change it independently of a network administrator. The user accesses the system at step 50 and provides a command 51 for a password change operation to be performed on the system at step 52. Usually, the user is prompted to type in a new password twice as disclosed with reference to Fig. 3 at step 53, and then the new password is stored in a password database on the system at step 54. Inconveniently, the password is changed independently of the authorization data or log in information when the system supports user authorization and password retrieval as disclosed with reference to Fig. 4. Therefore, the next time the user tries to access the system, his password information will not match with the new password – it has not been updated, and access will be denied.

[0030] According to the present invention, when a change password operation in execution on the system occurs, it is detected at step 55. That said, any password change command options in the form for example of the word "password" or the abbreviation "pwd" typed in are recognized. Of course, though it is preferred that all possible password change operations are detected, the present invention is advantageous if even a single change password operation is detected. The new password is changed at step 53 and the new password is stored in the password database on the system at step 54. Approximately simultaneously, the new password is detected by another process at step 57 that uses the detected data to change the password in another database at step 59. For example, the data indicative of the new password is automatically associated with the authorization data within a system at step 60 such as that of Fig. 4. Therefore, for future accesses to the system, the user just provides his authorization data in a form of a fingerprint for example, the system retrieves the data indicative of the new password associated with the authorization data and the user is authorized to access the system.

[0031] Alternatively, the storage of the new password in a password database on the system is detected and data indicative of the new password are also detected for storing in a database other than the password database on the system as shown at step 58.

[0032] Interestingly, the user is not aware of the detection procedure and of the automatic assignment of the authorization data to the data indicative of the new password. Therefore, the user types in a new password twice for storing the new password in a password database on the system, data indicative of the new password is saved in a database other than the password database on the system at step 59 and the password is changed on the system, and the user does not have to retype this new password for further access. However, because of the transparency of such a system, the user does not know whether his new password has effectively been changed or not.

[0033] Referring now to Fig. 6, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention is shown. When a password change operation is provided at step 61, the password change operation is detected at step 61 and a secure password change process prompts the user for a new password at step 63 to allow the change password operation to proceed at step 64. The new password is provided to the process at step 65 to allow changing of the password, which is stored in an independent database at step 66. The data indicative of the new password is automatically associated with the authorization data in replacement of the data indicative of the old password. From the independent database, the new password is provided to a password database on the system at step 67 to change the password there. The prompt for a new password by the secure password change process instead of by the process associated with the system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

[0034] Advantageously, the above process is implemented with no apparent change to the users of the system. In other words, a user is completely unaffected by the method of Fig. 6, since it is transparent to the user and does not affect any existing change password processes.

[0035] Referring now to Fig. 7, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention is shown. When a password change operation is provided at step 70, the password change operation is detected at step 71 and a secure user authorization process prompts the user for an authorization data at step 72. Once authorized at step 73, the system allows the change password operation to proceed at step 74. The new password is provided to allow changing of the password, which is stored in an independent database at step 75. The data indicative of the new password is automatically associated with the user identity in replacement of the data indicative of the old password. From the independent database, the new password is provided to a password database on the system at step 76 to change the password there. The prompt for user authorization data by the secure authorization process instead of by the process associated with the system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

[0036] The above process is highly advantageous. It provides a single password change process and as such a single ergonomic interface for changing passwords. Therefore, design and implementation of the secure change password process replaces all legacy change password processes allowing for better information for the users and a more modern and ergonomic process.

[0037] Further advantageously, the above process allows for changing of passwords of several systems/files/applications simultaneously. Thus, a single change password operation is used where before several or several hundred processes would have been required. This is most applicable when changing a password used to protect a single file such as a Microsoft ® Word® file or the like.

[0038] Of course, it is evident to those of skill in the art that a password entered in accordance with the above described process is optionally long and complex since there is no need to remember the password. Because of the automatic password retrieval, a user never needs to know their password so an arbitrary string of characters such as "efkjhgbshgdxfbkj#$$JHYT$kjsfd*(&REW^kvhgfd)(*^*&^%C^Tvc hbjhf86%(%(ffgf nm.b.nm.,mn.vb2609" is usable as a password allowing for greatly increased security.

[0039] Another advantage to the present method is that it allows tracking of old passwords to provide for access to older system restorations or old files that were saved using earlier passwords.

[0040] Of course, the process also supports different passwords for different systems, files and applications without substantial user inconvenience. This is achieved by storing each password in association with data indicative of the user identity or authorization and the system, file, or application with which the password is to be used. Of course, more complex associations are also possible when desired.

[0041] Referring now to Fig. 8, a flow diagram of a method of securely supporting password change for use with the method of Figure 7 wherein a choice is given to the user is shown. During the password change operation of step 80 and after user authorization at step 82 due to the detection of the password change operation at step 81, the user is given the opportunity to either enter a password or to have the process automatically generate a new password at step 83. Therefore, in the case of a computer-generated password, the user does not have to invent and remember the new password because it is automatically assigned to his authorization data and automatically retrieved for access to the system. Consequently, choosing a computer-generated password means that the new password is never typed in which decreases the possibilities of a Trojan Horse application from detecting same.

[0042] Advantageously, when a password is automatically generated, it is unknown to the user. This makes the password impossible to ascertain except by breaching security of password database. For example, when automatic password generation is used, an encryption key may form each password allowing for security relating to access and for encryption of file data to prevent mining of file data.

[0043] Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What is claimed is:

1. A method of securely supporting password change comprising the steps of:

detecting at least one of the operations in execution on a system comprising:

(i) detecting a password change operation (55; 62; 71; 81),

(ii) and detecting a new password storage operation (57);

performing an operation to change the password of a user to a new password in the system (53, 64, 74);

storing the new password in a password database on the system (54; 67; 76); and,

storing data indicative (59, 66; 75) of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored.

2. A method of securely supporting password change according to claim 1 wherein the step of detecting a password change operation (55; 62; 71; 81) in execution on a system comprises the step of detecting a new password prompt.

3. A method of securely supporting password change according to claim 1 comprising the steps of:

prompting a user to provide authorization data (72); and,

associating the authorization data with the password.

4. A method of securely supporting password change according to claim 1, wherein the step of detecting the new password comprises the step of detecting the new password at least two separate times.

5. A method of securely supporting password change according to claim1 wherein the operation detected is a password change operation and further comprising the steps of:

displaying to a user a prompt for a new password (63), the prompt independent of the password change operation;

receiving the new password (65);

6. A method of securely supporting password change according to claim 5 wherein the step of detecting the change password operation in execution on a system comprises the step of detecting password change command options.

7. A method of securely supporting password change according to claim 1 wherein the operation detected is a password change operation and further comprising the steps of:

displaying to a user a prompt for authentication information (72), the prompt independent of the password change operation;

receiving the authentication information (73);

when the authentication information is indicative of a known user, performing said operation to change the password (74) of the known user to a new password in the system; and;

8. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for biometric information.

9. A method of securely supporting password change according to claim 8 comprising the step of:

providing biometric information;

processing the provided biometric information to provide biometric data;

comparing the biometric data with a stored template; and

in dependence upon a comparison result retrieving a user password from a database.

10. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for information stored on a smart card.

11. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of providing the new password to the system.

12. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of prompting the user to select between provision of the new password and automatic generation of the new password (83).

13. A method of securely supporting password change according to any of claims 7 and 12, characterized in that the step of performing an operation to change the password comprises the step of automatically generating the new password.

14. A method of securely supporting password change according to claim 13 wherein data secured with the new password is encrypted using an encryption key.

15. A method of securely supporting password change according to claim 7 comprising the step of performing another operation to change another password of the known user to the new password.

16. A method of securely supporting password change according to claim 7 comprising the step of determining all passwords identical to the password being changed and automatically performing at least another operation to change each identical password of the known user to the new password.

17. A method of securely supporting password change according to claim 1
wherein the operation detected is a password change operation;
wherein the system has a known user authorized thereon; and,
wherein the step of performing an operation to change the password comprises the step of automatically generating a new password .

18. A method of securely supporting password change according to any of claims 13 and 17, characterized in that the automatically generated new password is unknown to the user.

19. A method of securely supporting password change according to any of claims 13 and 18, characterized in that the automatically generated new password is an encryption key.

20. A method of securely supporting password change according to any of claims 13 and 19, characterized in that the data secured with the new password is encrypted using an encryption key.

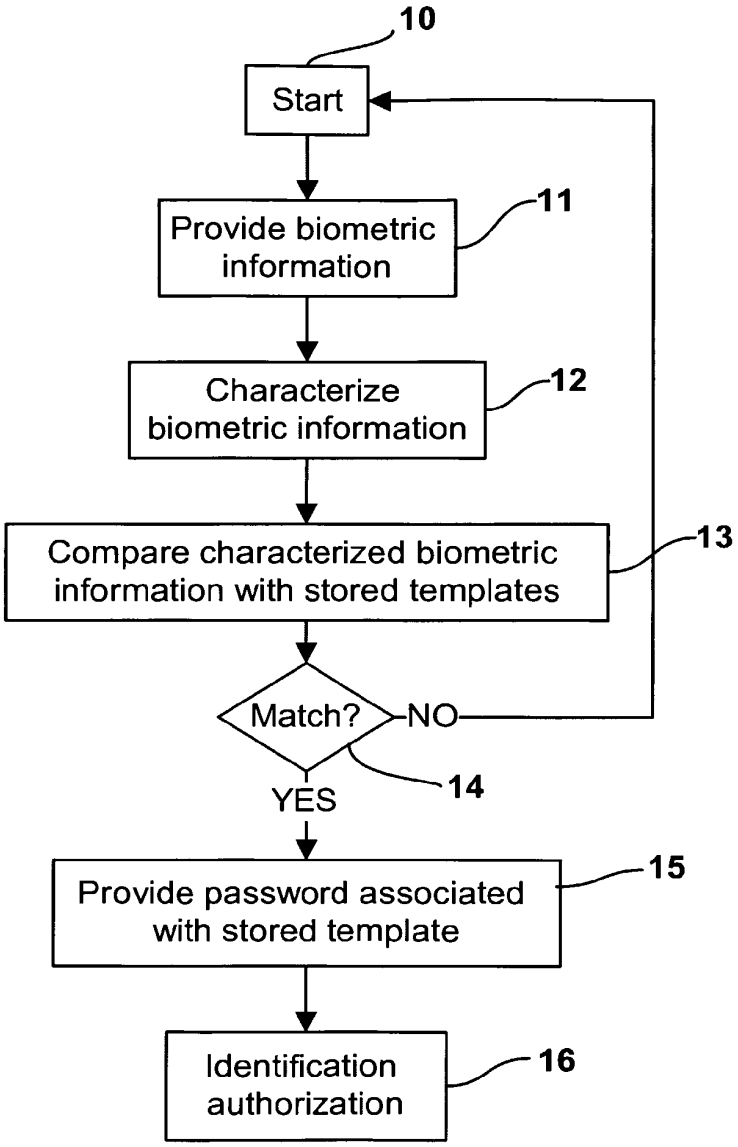


Fig. 1
(PRIOR ART)

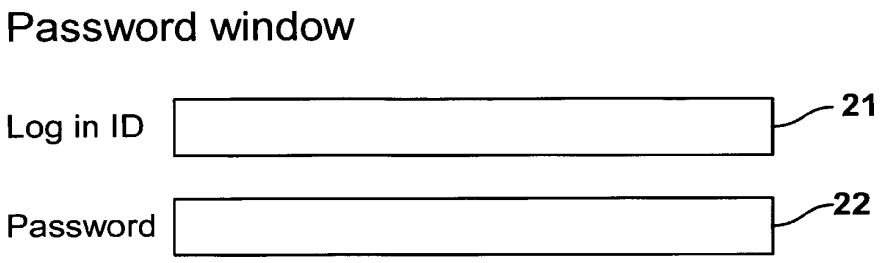


Fig. 2
(PRIOR ART)

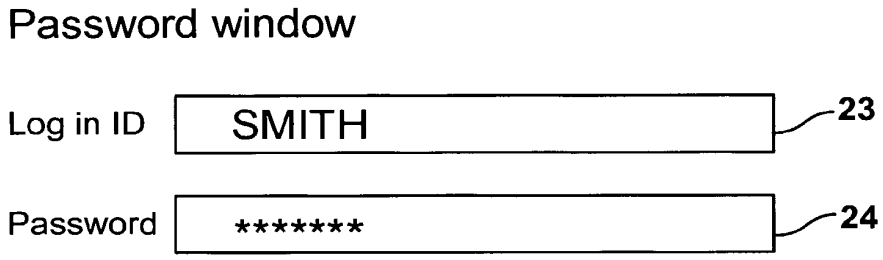


Fig. 2a
(PRIOR ART)

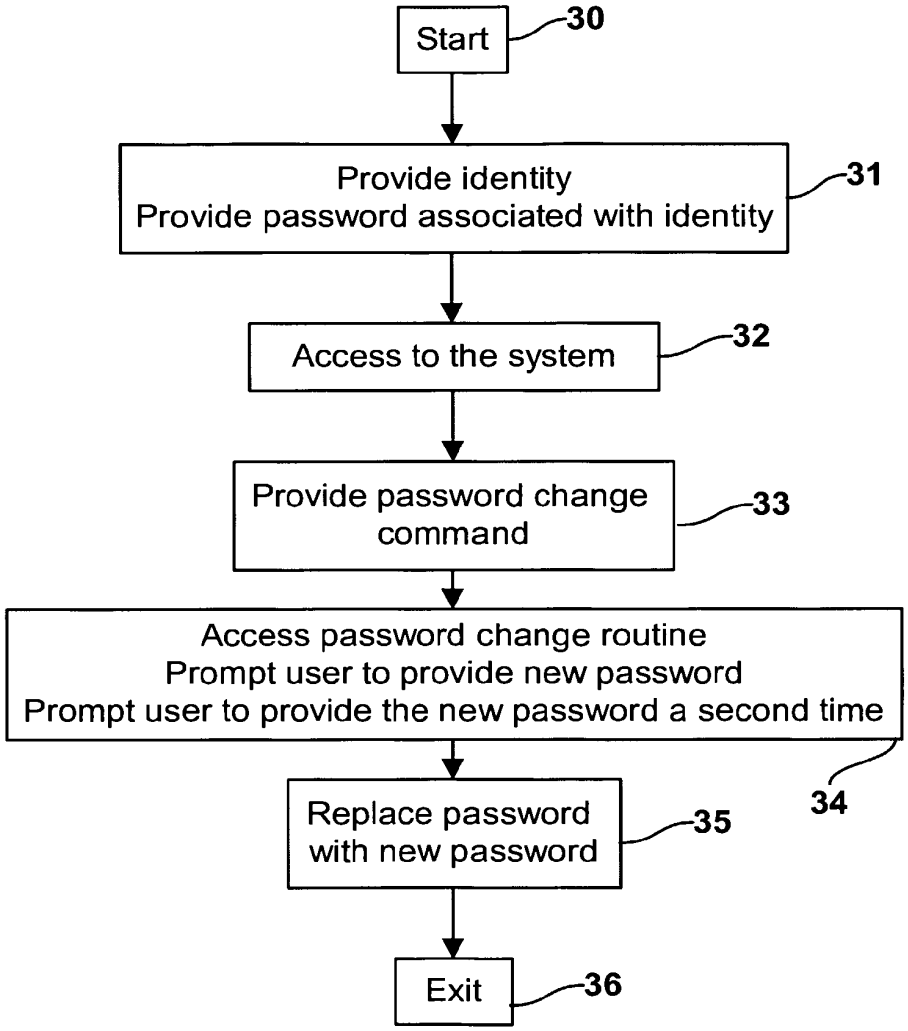


Fig. 3
(PRIOR ART)

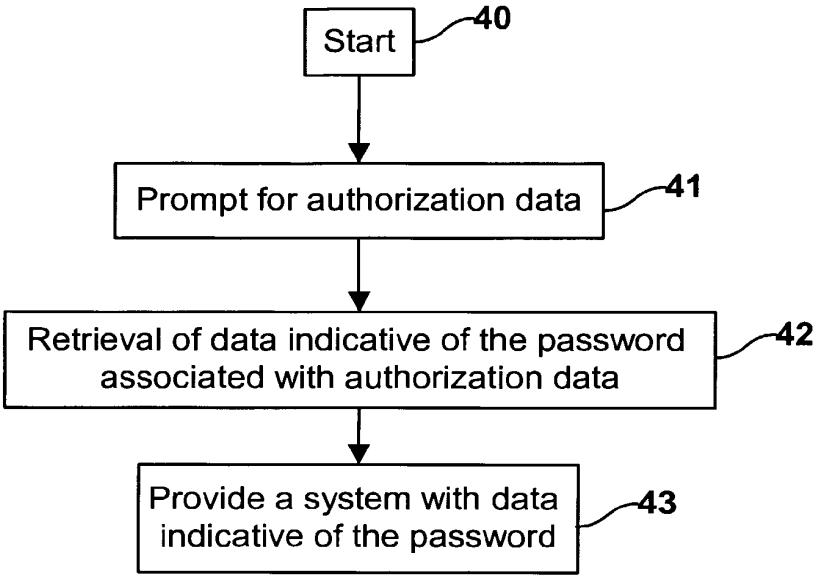


Fig. 4
(PRIOR ART)

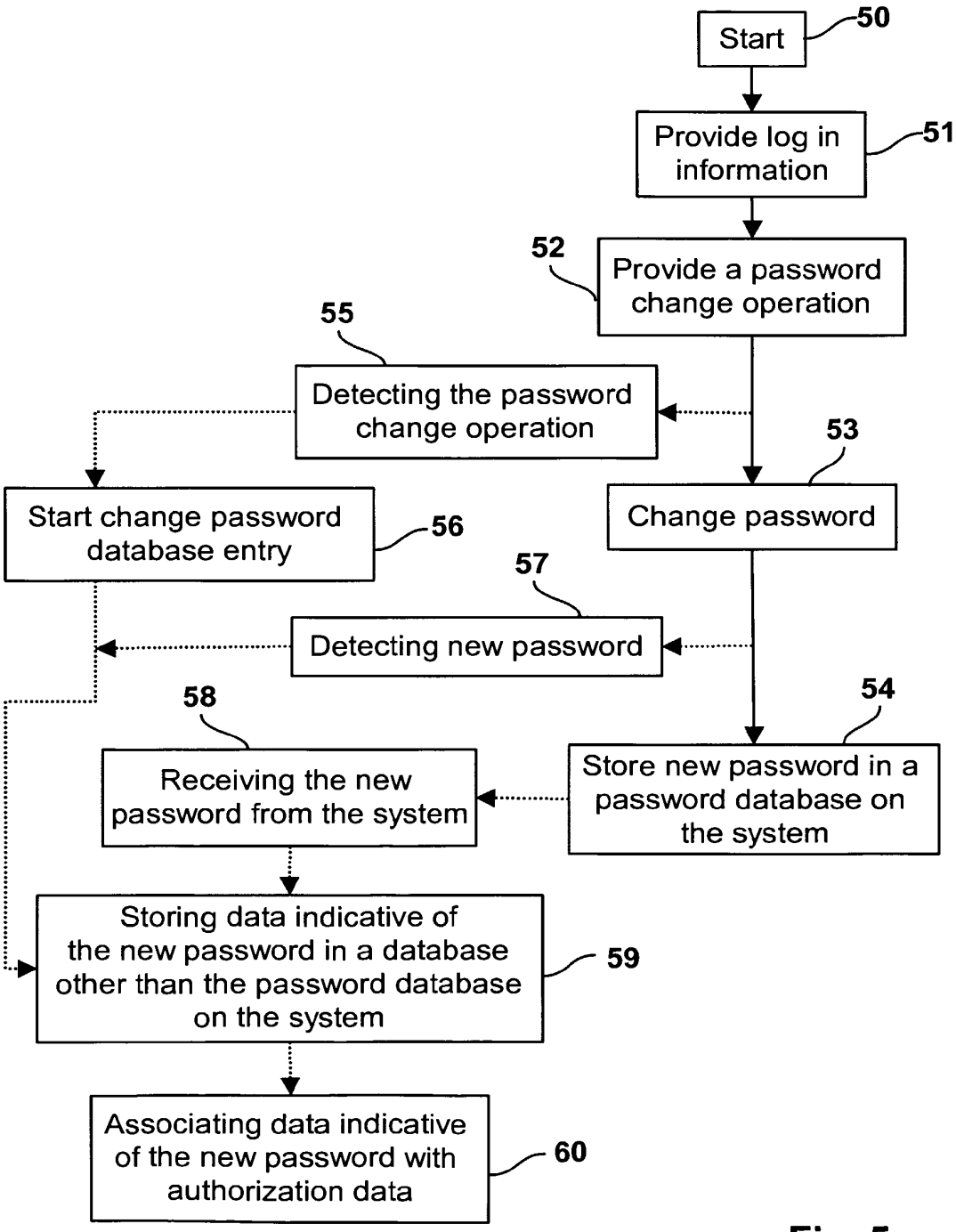

Start
50
Provide log in information
51
52
Provide a password change operation
55
Detecting the password change operation
53
Start change password database entry
56
Change password
57
Detecting new password
58
54
Receiving the new password from the system
Store new password in a password database on the system
Storing data indicative of the new password in a database other than the password database on the system
59
Associating data indicative of the new password with authorization data
60

Fig. 5

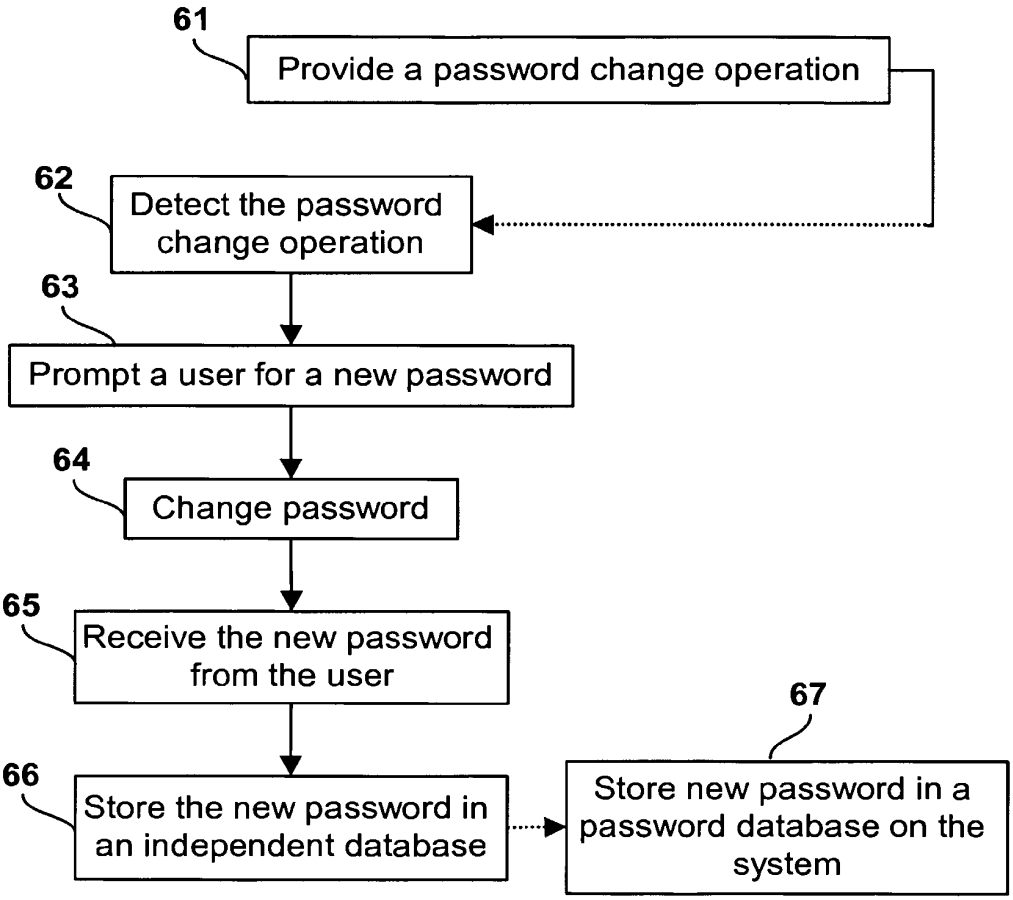

61
Provide a password change operation
62
Detect the password change operation
63
Prompt a user for a new password
64
Change password
65
Receive the new password from the user
66
Store the new password in an independent database
67
Store new password in a password database on the system

Fig. 6

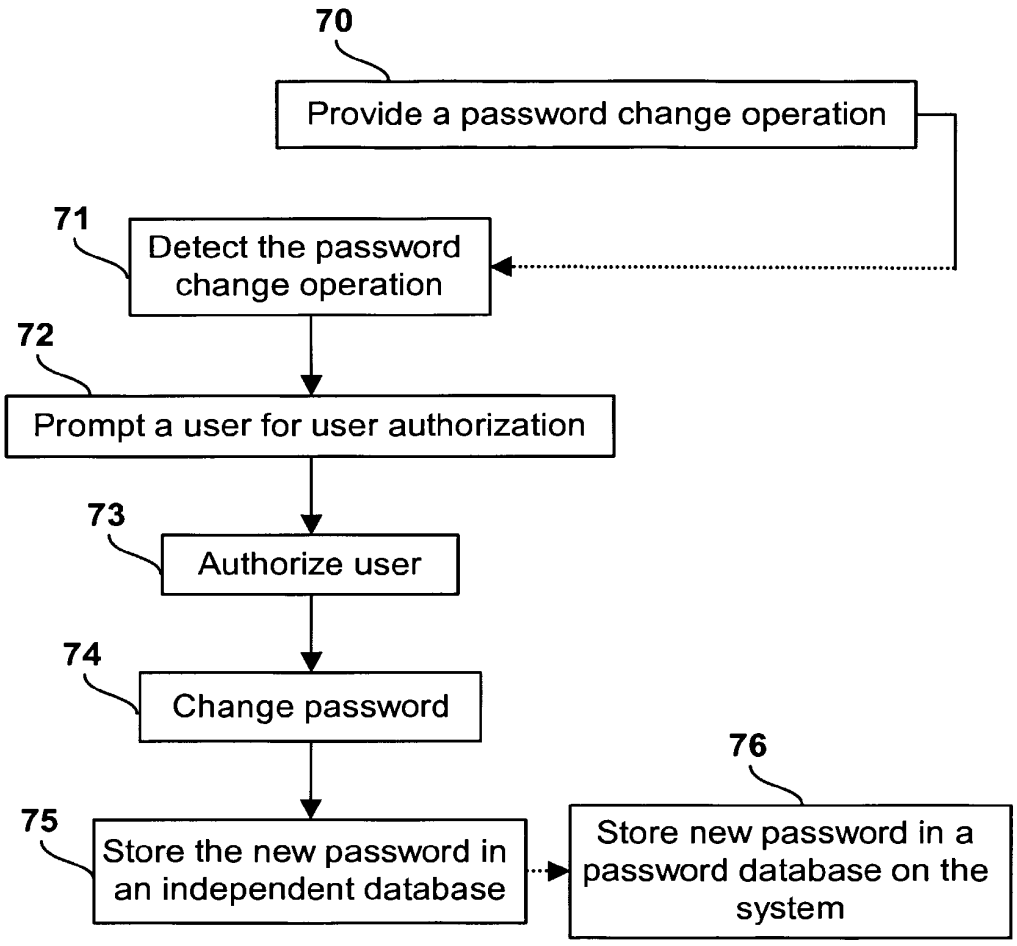

70
Provide a password change operation
71
Detect the password change operation
72
Prompt a user for user authorization
73
Authorize user
74
Change password
75
Store the new password in an independent database
76
Store new password in a password database on the system

Fig. 7

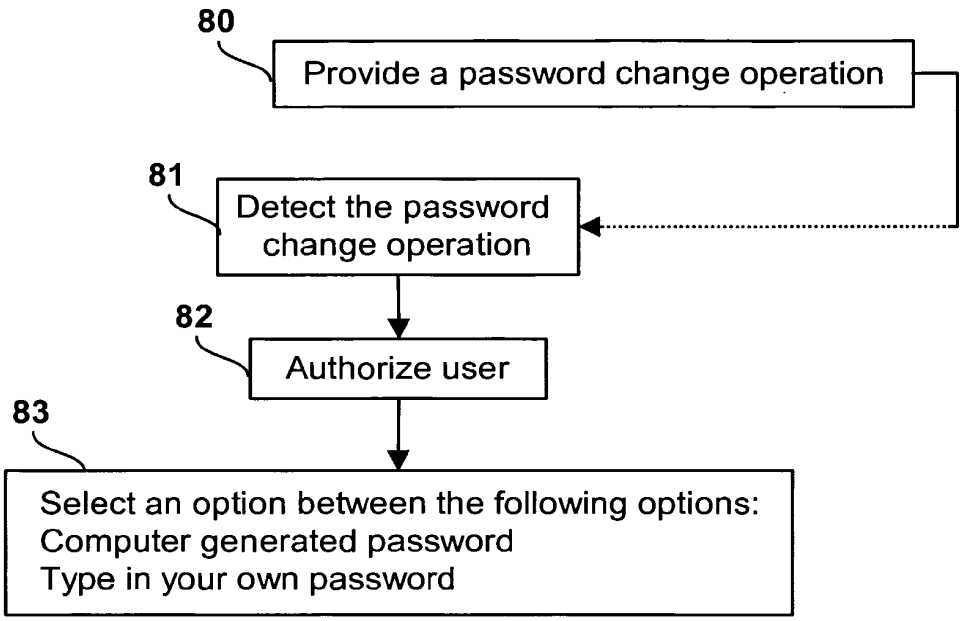

80
Provide a password change operation
81
Detect the password change operation
82
Authorize user
83
Select an option between the following options:
Computer generated password
Type in your own password

Fig. 8

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
31 décembre 2003 (31.12.2003)

PCT

(10) Numéro de publication internationale
WO 2004/002058 A2

(51) Classification internationale des brevets[7] : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR2003/001871

(22) Date de dépôt international : 18 juin 2003 (18.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/07688 19 juin 2002 (19.06.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Parc d'Activités de Gémenos, Avenue du Pic-de-Bertagne, F-13420 Gémenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **FEYT, Nathalie** [FR/FR]; 8, chemin de Raphèle, 7 lotissement l'Oliveraie, F-13780 Cuges les Pins (FR). **JOYE, Marc** [FR/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR).

(74) Mandataire : **AIVAZIAN, Denis**; Gemplus la Vigie, Service brevets, BP 100, F-13705 La Ciotat Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

[Suite sur la page suivante]

(54) **Title:** METHOD OF GENERATING ELECTRONIC KEYS FOR A PUBLIC-KEY CRYPTOGRAPHY METHOD AND A SECURE PORTABLE OBJECT USING SAID METHOD

(54) **Titre :** PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN OEUVRE LE PROCEDE

(57) **Abstract:** The invention relates to a method of generating electronic keys (d) for a public-key cryptography method using an electronic device. The inventive method comprises two separate calculation steps, namely: step A consisting in (i) calculating pairs of prime numbers (p, q), said calculation being independent of knowledge of the pair (e, l) in which e is the public exponent and l is the length of the key of the cryptography method, and (ii) storing the pairs thus obtained; and step B which is very quick and can be executed in real time by the device, consisting in calculating a key d from the results of step A and knowledge of the pair (e, l).

(57) **Abrégé :** L'invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique. Selon l'invention, le procédé comprend deux étapes de calcul dissociées. Une étape A consiste à - calculer des couples de nombres premiers (p, q), ce calcul est indépendant de la connaissance du couple (e, l) e l'exposant public et l la longueur de la clé du procédé de cryptographie et à - stocker les couples ainsi obtenus. Une étape B très rapide qui peut être exécutée en temps réel par le dispositif, consiste à calculer une clé d à partir des résultats de l'étape A et de la connaissance du couple (e, l).

WO 2004/002058 A2

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN ŒUVRE LE PROCEDE

L'invention concerne un procédé de génération de clés électroniques pour procédé de cryptographie à clé publique. Elle concerne également un objet portatif sécurisé mettant en œuvre le procédé.

L'invention concerne plus particulièrement la génération de clés d'un système cryptographique de type RSA et leur stockage sur un objet sécurisé en vue de leur utilisation dans une application nécessitant de la sécurité.

L'invention s'applique tout particulièrement à dés objets sécurisés ne possédant pas d'importante ressource mémoire telle que de la mémoire électriquement programmable, ni de ressources de calcul puissantes comme c'est le cas pour les cartes à puce.

Une application de l'invention est le commerce électronique par l'intermédiaire d'un téléphone portable. Dans ce contexte les clés peuvent se trouver sur la carte SIM du téléphone.

Il est en effet prévu que certains programmes d'applications utilisent de telles clés pour mettre en œuvre un transfert de données confidentielles, dans un contexte de commerce électronique par exemple. Par la suite, on considèrera que ces applications sont fournies par une entité fournisseur de service.

En outre, il est connu que pour garantir l'intégrité de la clé, on lui associe généralement un certificat fourni par une entité de confiance.

Parmi les procédés de cryptographie à clé publique, on s'intéresse dans ce qui suit au protocole de cryptographie RSA (Rivest Shamir et Adleman). Ce protocole met en œuvre une étape de génération de nombres premiers de grande taille, coûteuse en temps de calcul et en place mémoire.

On rappelle que ce protocole de cryptographie RSA permet le chiffrement d'informations et/ou l'authentification entre deux entités et/ou la signature électronique de messages.

Le protocole de cryptographie RSA est le plus utilisé car il possède des propriétés qui lui permettent d'être employé aussi bien en chiffrement qu'en génération de signature.

Pour ce faire, le système de cryptographie RSA comprend un algorithme « public » réalisant la fonction de chiffrement ou de vérification de signature et un algorithme « privé » réalisant la fonction de déchiffrement ou de génération de signature.

Sa sécurité repose sur la difficulté de factorisation d'un nombre entier public N de grande taille qui est le produit de deux nombres premiers secrets p et q de grande taille, le couple (p,q) entrant dans le calcul de la clé secrète d utilisée par la fonction de déchiffrement ou par la fonction de calcul d'une signature.

Afin de mieux comprendre le problème qui va être exposé dans la suite, on va rappeler dans ce qui suit les paramètres entrant dans un schéma de cryptographie RSA :.

1) L'exposant public e :

Il est propre à une application et est fourni par cette application. De ce fait, il est commun à tous les utilisateurs de cette même application.

2) Les paramètres p et q:

Ils sont générés à l'issu d'un calcul coûteux en temps. Ils ont en général la même longueur (même taille). Cette longueur est classiquement de 512 bits. Pour augmenter la sécurité, cette longueur peut aller de 512 bits à 2048, 2048 bits étant envisagés pour le futur.

3) N est le module public et est calculé à partir de la relation suivante :

$N = p*q$

La clé de l'algorithme est dite de longueur ℓ, lorsque le module public N est de longueur ℓ. Cette longueur est fixée par l'application (ou fournisseur de service).

4) les paramètres e et N forment la clé publique.

5) la clé privée d est calculée à partir de la relation suivante :

$d = 1/e[\mathrm{mod}(p-1)(q-1)]$; $(1/e = e^{-1})$

soit encore $ed \equiv 1$ [(mod ppcm(p-1, q-1)] ; ppcm signifie le plus petit commun multiple,

les paramètres secrets sont formés par le triplet (d, p, q).

6) la forme « normale » de la clé privée est:

(d,N).

6) la forme CRT (Chinese Remainder Theorem) de la clé privée est:

dans ce cas la clé privée comporte 5 paramètres :

p, q

d_p avec $d_p = d \bmod (p-1)$

d_q avec $d_q = d \bmod (q-1)$

I_q avec $I_q = q^{-1} \bmod p$.

Le principe de la génération d'une clé selon le, schéma RSA consiste donc comme on peut le voir, à générer une clé privée d à partir d'un exposant public e (ou clé publique) fixé par l'application, les paramètres p, q étant générés de sorte que p*q = N, la longueur ℓ de N étant fixée.

Lorsque plusieurs applications sont prévues, chaque fournisseur de service fournit son exposant public e et la longueur du module public N, de manière à ce que puisse être générée la clé privée d correspondante.

Ainsi, la mise en œuvre d'un calcul de clé RSA nécessite la connaissance de l'exposant public e et celle de la longueur ℓ de la clé de l'algorithme c'est à dire la longueur du modulo N. Avec les données d'entrée e et ℓ, il reste à générer le couple de nombre premier p et q de manière à ce que ces derniers répondent aux conditions suivantes :

(i) p-1 et q-1 premiers avec e et,

(ii) N= p*q un nombre entier de longueur ℓ.

Ces contraintes sont coûteuses en temps de calcul.

On rappelle à ce propos que la génération et le stockage des clés pour des objets portables tels que les cartes à puce s'effectuent à ce jour des deux manières suivantes :

Selon une première manière, le calcul d'une clé RSA est effectué sur un serveur pour profiter d'une puissance de calcul importante. On requiert alors pour plus de sécurité, un certificat que l'on télécharge avec la clé au sein de l'objet sécurisé lors de sa phase de personnalisation.

Cette solution présente deux inconvénients. :

- d'une part malgré le cadre relativement sécurisé de la personnalisation, il peut y avoir vol ou duplication de la clé du fait de son transfert du serveur vers l'objet sécurisé, et

- d'autre part, chaque clé est chargée dans l'objet dans une phase initiale de personnalisation, ce qui nécessite de prévoir un maximum de clés dans chaque objet pour pouvoir anticiper les futurs besoins.

Dans la pratique, on stocke dans l'objet portable des ensembles de clés et de certificats correspondant à chaque application susceptible d'être utilisée, sans savoir si ces clés seront réellement utiles ultérieurement. Un emplacement mémoire important est utilisé inutilement. Par exemple 0,3 Koctets sont nécessaires pour une clé de RSA de module de 1024bits, alors que les cartes actuelles ont au plus 32Koctets de mémoire programmable. En outre, un nombre important de certificats est acheté à l'entité de confiance ce qui est coûteux.

L'inconvénient ultime mais tout aussi important est qu'il n'est pas possible d'ajouter de nouvelles clés au fur et à mesure que de nouvelles applications pourraient être envisagées.

Selon une deuxième solution, le calcul peut être effectué au sein de l'objet sécurisé. Cela résout le premier inconvénient de la solution précédente mais crée une lourdeur de traitement au niveau de l'objet sécurisé qui possède une faible capacité de calcul.

En effet, lorsque la génération d'une clé RSA est réalisée par un objet portatif tel qu'une carte à puce, si la longueur imposée de clé RSA est de 2048 bits, le calcul prend alors 30 secondes avec un algorithme performant.

Même si ce temps de calcul est acceptable pour certaines applications car on génère les clés RSA une seule fois pour une application donnée, ceci n'est pas satisfaisant pour les services de téléphonie mobile (GSM par exemple) car cette opération se renouvelle à chaque changement de carte SIM et qu'un plus grand nombre de clés doit être prévu pour répondre aux besoins de différentes applications.

Du fait d'un besoin en ressources de calcul important, les clés sont toujours crées durant la phase de personnalisation à partir des exposants publics e fournis par les différentes entités fournisseur de service. Cette étape de calcul ne peut pas être mise en œuvre ultérieurement car elle paralyserait le fonctionnement de l'objet.

De façon pratique ce calcul n'est pas mis en œuvre par la carte. En effet, ce calcul est long et il pourrait ralentir la phase de personnalisation, de plus sa durée est variable et elle pourrait se révéler incompatible avec les procédés de personnalisation des cartes à puce.

D'autre part, cette solution présente toujours le second inconvénient de la solution précédente à savoir la nécessité de ressource mémoire.

La présente invention a pour but de résoudre ces problèmes.

Plus précisément l'invention a pour objectif de résoudre le problème de lourdeur du calcul lié à la gestion de génération de clés ainsi que le problème de manque de flexibilité dû au stockage initial et définitif d'un nombre important de clés et de certificats en phase de personnalisation.

A cette fin, un objet de la présente invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique, principalement caractérisé en ce qu'il comprend deux étapes de calcul dissociées :

Etape A

1) Calcul de couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N dudit procédé,
2) Stockage des couples ou des valeurs ainsi obtenus ;

Etape B

Calcul de la clé d à partir des résultats de l'étape A et de la connaissance du couple (e,l).

Selon une première variante, l'étape A-1) consiste à calculer des couples de nombres premiers (p,q) sans connaissance de l'exposant public e ni de la longueur l de la clé, en utilisant un paramètre Π qui est le produit de petits nombres premiers. De cette manière couple (p,q) obtenu à l'étape A, a une probabilité maximale de pouvoir correspondre à un futur couple (e,l) et permettra de calculer une clé d lors de la mise en œuvre de l'étape B.

Selon une autre variante dépendante de la variante précédente, le calcul A-1) tient compte en plus du fait que e a une forte probabilité de faire partie de l'ensemble $\{3, 17, \ldots, 2^{16+1}\}$, on utilise pour cela dans le

calcul de l'étape A, une graine σ qui permet de calculer non pas des couples (p,q) mais une valeur représentative appelée image des couples (p,q).

Le stockage A-2) consiste alors à mémoriser cette image. Ceci permet de gagner de la place mémoire puisqu'une image est plus petite qu'un nombre premier p ou q par exemple 32 octets comparés à 128 octets.

Selon une troisième variante on effectue un calcul de couples (p,q) pour différents couples (e,l) probables. De façon pratique le paramètre Π va contenir les valeurs usuelles de e par exemple 3, 17.

Selon une quatrième variante l'étape A-1) comprend une opération de compression des couples (p,q) calculés et l'étape A-2) consiste alors à stocker les valeurs compressées ainsi obtenues.

L'étape B comprend la vérification des conditions suivantes pour un couple (e, ℓ) donné:

(i) p-1 et q-1 premiers avec e et,

(ii) N= p*q un nombre entier de longueur ℓ.

Selon un mode de réalisation préféré, l'étape A-1) comprend la génération d'un nombre premier q, le choix d'une limite inférieure B_0 pour la longueur ℓ_0 de ce nombre premier à générer telle que $\ell_0 \geq B_0$ par exemple B_0= 256 bits, et elle comprend en outre les sous-étapes suivantes :

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \leq 2^{B_0}$,

2)-choisir un nombre j dans l'intervalle des nombres entiers {v,….,w-1} et calculer ℓ=j Π ;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers {0,…., Π-1} , (k, Π) étant co-premiers, ;

4)-calculer q= k+ℓ,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a\,k \pmod{\Pi}$; a appartenant au groupe multiplicatif Z^*_{Π} des nombres entiers modulo Π;

b) réitérer à partir de la sous-étape 4).

Avantageusement l'étape B comprend, pour un couple (p,q) obtenu à l'étape A,et un couple (e,l) donné :

- La vérification des conditions suivantes :
  (i) p-1 et q-1 premiers avec e et,
  (ii) N= p*q un nombre entier de longueur ℓ,
- Si le couple (p,q) ne répond pas à ces conditions :
- Choix d'un autre couple et réitération de la vérification jusqu'à ce qu'un couple convienne,
- Calcul de la clé d à partir du couple (p,q) obtenu à l'issue de cette vérification.

L'invention a également pour objet, un objet sécurisé portatif apte à générer des clés électroniques d d'un algorithme de cryptographie de type RSA, caractérisé en ce qu'il comprend au moins :

- Des moyens de communication pour recevoir au moins un couple (e,l),

- Une mémoire pour stoker les résultats d'une étape A consistant à :

Calculer des couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N dudit procédé,

- Un programme pour mettre en œuvre une étape B consistant à :

Calculer d'une clé d à partir des résultats de l'étape A et de la connaissance d'un couple (e,l),

L'objet sécurisé portatif comprend en outre un programme pour la mise en œuvre de l'étape A, les étapes A et B étant dissociées dans le temps.

L'objet sécurisé portatif pourra être constitué par une carte à puce.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est donnée ci-après à titre d'exemple non limitatif et en regard de la figure unique représentant un schéma d'un système de mise en œuvre du procédé.

La suite de la description est faite dans le cadre de l'application de l'invention à un objet portatif de type carte à puce et pour simplifier l'expression on parlera de carte à puce.

Selon le procédé proposé la génération de clés se fait en deux étapes dissociées.

La première Etape A comporte un calcul de couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers appelée image.

Les couples (p,q) obtenus sont stockés.

Ce calcul est lourd et il est d'autant plus lourd si on utilise un algorithme de génération de nombres premiers classique.

Il est proposé ici que ce calcul soit effectué de manière indépendante de la connaissance du couple (e,l).

Comme cela va être détaillé dans la suite un mode de réalisation préféré pour mettre en œuvre cette étape permet d'alléger les calculs et de limiter la place mémoire nécessaire pour le stockage des couples (p,q) obtenus en stockant une image de ces couples.

La deuxième Etape B comporte le calcul à proprement parler de la clé d à partir des résultats de l'étape A et de la connaissance du couple (e,l).

Ce calcul comprend, pour un couple (p,q) obtenu à l'étape A, et un couple (e,l) donné :

- La vérification des conditions suivantes :
  (i) p-1 et q-1 premiers avec e et,
  (ii) N= p*q , ce nombre doit être un nombre entier et de longueur ℓ,
- Si un couple (p,q) ne répond pas à ces conditions, on choisit un autre couple et on réitère de la vérification jusqu'à ce qu'un couple convienne parmi les couples obtenus lors de l'étape A.
- On peut procéder alors au calcul de la clé d à partir du couple (p,q) obtenu à l'issue de cette vérification.

La première étape qui correspond à un calcul relativement lourd par rapport à la deuxième étape, peut être exécutée par un autre organe que la carte à

puce par exemple par un serveur. Dans ce cas, les résultats du calcul de cette première étape pourront être chargés sur une carte à puce au moment de la personnalisation.

Le calcul de l'étape A peut également être fait par la carte elle-même à un instant quelconque qui ne gêne pas l'utilisateur de cette carte. Par exemple, ce calcul peut être fait lors de la personnalisation de la carte ou plus tard.

De façon pratique, lors de l'utilisation de la carte, pour obtenir un service, si une clé privée est nécessaire, alors la clé publique est fournie par le fournisseur de service (éventuellement à distance si elle n'est pas déjà stockée dans la carte) afin de générer la clé privée. Cette étape de génération (étape B de calcul) est effectuée de manière rapide par la carte.

On voit donc que de nouvelles applications qui nécessitent le calcul d'une clé privée d peuvent être prévues pour une carte.

On voit également qu'il n'y a pas besoin d'associer un certificat aux couples (p,q) car ils ne sont pas associés à une clé privée.

Ainsi, la génération d'une clé privée peut être faite à bord c'est à dire par la carte elle-même avec un gain d'un facteur 10 en temps d'exécution par rapport aux procédés de génération de clés connus à ce jour.

On va décrire dans ce qui suit un mode préféré de réalisation pour la mise en œuvre de l'étape A. Ce mode de réalisation est particulièrement avantageux pour la mise à bord d'une carte à puce car il permet

d'optimiser à la fois la place mémoire mais aussi le temps de calcul.

Tout d'abord, afin de s'assurer que N=p*q est un entier de ℓ-bit, on choisit p appartenant à l'intervalle :

$$\left[\sqrt{2^{2(l-l0)-1}}, 2^{l-l0}-1\right]$$

Et q appartenant à l'intervalle :

$$\left[\sqrt{2^{2l0-1}}, 2^{l0}-1\right]$$

Pour ℓ_0 compris entre 1 et ℓ.

Ainsi min(p)min(q) est compris entre $2^{\ell 0}$-1 et N, et max(p)max(q) est compris entre N et 2^{ℓ} comme cela est demandé.

De cette façon, la condition ii) ci-dessus mentionnée se réduit à rechercher des nombres premiers dans l'intervalle :

$$\left[\sqrt{2^{2l0-1}}, 2^{l0}-1\right]$$

La solution proposée exploite le paramètre Π. Ce paramètre Π est le produit de petits nombres premiers dans lequel on peut trouver notamment 3, 17, 2^{16+1}, nombres premiers généralement utilisés comme exposants publics. Ainsi, la probabilité pour qu'un couple (p,q) corresponde à un futur couple (e,l) donné, déjà très élevée, augmente encore lorsque Π comporte de telles valeurs.

On choisit les f plus petits nombres premiers, f étant choisi de manière telle que $\Pi_i p_i \leq 2B_0$, B_0 est la

borne inférieure choisie pour ℓ_0. par exemple on peut choisir B_0 égal à 256 bits.

Π est égal au produit : 2.3…..191 et est inférieur à 2^{256}.

On peut alors mémoriser cette valeur Π dans la carte par exemple comme une constante dans la mémoire morte de programme.

La première phase du procédé consiste à générer et à enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombre entiers {0,…., Π-1} , (k, Π) étant copremiers, c'est à dire n'ayant pas de facteur commun.

La deuxième phase consiste ensuite à partir de ce nombre k à construire le premier candidat q qui satisfait la condition d'être copremier avec Π .

Si ce premier candidat ne satisfait pas cette condition, alors il est mis à jour c'est à dire qu'un autre candidat est choisi jusqu'à ce qu'une valeur de q satisfaisant à la condition soit trouvée.

On va présenter dans la suite les différentes étapes de l'algorithme de génération d'un nombre premier entrant dans le calcul d'une clé RSA selon l'invention.

L'algorithme proposé fonctionne quelle que soit la longueur lo donnée pour le nombre premier q qui doit être généré.

La génération du nombre premier p est identique, il suffit de remplacer q par p dans les étapes qui vont être développées et de remplacer lo par l-lo.

Après avoir fixé la limite Bo, on calcule les nombres premiers uniques v et w satisfaisant les conditions suivantes:

$$\sqrt{2}^{2^{\ell_0-1}} \leq v\Pi \leq \sqrt{2}^{2^{\ell_0-1}} + \Pi,$$
$$2^{\ell_0} - \Pi \leq w\Pi \leq 2^{\ell_0}$$

Ceci, se traduit par le calcul de v et w par les relations suivantes :

$$v = \sqrt{2}^{2^{\ell_0-1}} / \Pi$$
$$w = 2^{\ell_0} / \Pi$$

Puis après avoir pris k appartenant au groupe multiplicatif $Z^*\Pi$ des nombres entiers modulo Π, on construit le premier candidat q tel que,

$q = k + j\,\Pi$ pour tout j appartenant à l'intervalle [v, w-1] .

Comme justement k apparient à $Z^*\Pi$, la probabilité pour avoir un premier candidat q premier, est élevée. Si ce n'est pas le cas, on met à jour k en prenant k égal à $ak \pmod{\Pi}$, a appartenant au groupe $Z^*\Pi$ et on réitère jusqu'à trouver une valeur de q correspondant à un nombre premier.

Une manière de tester la primalité d'un nombre est par exemple d'utiliser le test de Rabin-Miller.

Les différentes étapes de l'algorithme proposé sont précisément les suivantes :

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$$v = \sqrt{2}^{2^{\ell_0-1}} / \Pi$$
$$w = 2^{\ell_0} / \Pi$$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \leq 2^{B_0}$,

2)-choisir un nombre j dans l'intervalle des nombres entiers $\{v, \ldots, w-1\}$ et calculer $\ell = j\,\Pi$;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers $\{0,\ldots., \Pi-1\}$, (k, Π) étant co-premiers, ;

4)-calculer $q= k+\ell$,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a\,k \pmod{\Pi}$; a appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π;

b) réitérer à partir de l'étape 4) ;

6) enregistrer a, k' j pour les utiliser afin de retrouver q et ensuite exploiter q pour l'utiliser lors d'un calcul ultérieur de génération d'une clé RSA.

Au lieu de stocker la valeur de q on va procéder avantageusement comme décrit dans la suite.

Une manière simple de mettre en œuvre cet algorithme peut consister pour chaque longueur de clé RSA envisagée, de stocker les valeurs de k et j de manière à re construire q.

Plutôt que de choisir un nombre aléatoire j comme indiqué à l'étape 2) un autre mode de réalisation peut consister à construire j à partir d'un nombre aléatoire court.

On prend par exemple un nombre de longueur 64-bit, que l'on désigne par graine et que l'on dénote σ. Cette graine est alors prise comme valeur d'entrée d'un générateur de nombres pseudo-aléatoires PRNG, lequel va permettre de générer j.

j est alors défini comme $PRNG_1(\sigma) \pmod{(w-v)+v}$.

Ce mode d'exécution permet de réduire considérablement les besoins en place mémoire car il n'y a à stocker que les valeurs de σ et de k en mémoire

EEPROM. La valeur de Π est en mémoire morte (dans le programme de calcul).

On peut encore réduire les besoins en place mémoire en constatant que : si $k_{(o)}$ est la première valeur de k appartenant au groupe $Z^*\prod$, alors, les nombres premiers générés ont la forme :

$q = a^{f-1} k_{(o)} \bmod \Pi + j\,\Pi$

f étant le nombre d'échec du test de l'étape 4).

Cette valeur $k_{(o)}$ qui appartient au groupe $Z^*\prod$, peut être facilement calculée à partir d'une graine aléatoire courte comme σ par exemple et en utilisant la fonction de Carmichael de Π^2 dénotée $\lambda(\Pi)$.

En utilisant cette fonction on peut exprimer $k_{(o)}$ par la relation suivante :

$k_{(o)} = [PRNG_2(\sigma) + b^{PRNG3(\sigma)} (PRNG_2(\sigma)^{\lambda(\Pi)} - 1)] \pmod{\prod}$

b étant un élément d'ordre $\lambda(\Pi)$ appartenant à $Z^*\prod$.

Ces deux modes d'exécution permettent de réduire les besoins en place mémoire puisqu'on ne va devoir stoker dans ce cas, que la valeur de la graine σ et différentes valeurs de f pour les longueurs désirées de clés.

Pour des clés RSA de modulo supérieur à 2048 bits, les expériences numériques qui ont été faites par les inventeurs montrent que f est égal à 2^8. Ceci signifie que f peut être codé sur 1 byte soit 8 octets.

A titre d'exemple, pour générer des clés RSA de longueur allant de 512 à 2048 bits avec une granulité de 32 bits, il y a 49 longueurs de clé possibles. Il est donc nécessaire de stocker sur la carte un byte soit 8 octets correspondant à la valeur de σ. Il est également nécessaire de stocker les valeurs de f pour les nombres premiers p et q soit 2*49=98 octets. Ceci

fait au total 106 bytes soit 848 bits en mémoire EEPROM.

Un dernier mode d'exécution permettant de réduire la place mémoire, consiste à stoker dans le programme de calcul, c'est à dire en mémoire de programme, plusieurs valeurs de Π et les valeurs de $\lambda(\Pi)$ correspondantes pour différentes longueurs de clés envisagées. On peut remarquer qu'une grande valeur de Π conduit aux plus petites valeurs pour f.

Le nombre premier q généré selon l'étape 4) par l'algorithme qui vient d'être décrit satisfait comme on l'a vu précédemment à la condition :

$q = a^{f-1} k_{(o)} \bmod \Pi + j*\Pi$

Si e divise Π on peut exprimer q par la relation suivante :

$q = a^{f-1} k_{(o)} \bmod (e)$

Afin que la condition i) énoncée au début de la description soit remplie, il faut choisir a tel que $a=1 \pmod e$ et forcer $k_{(o)}$ de manière à ce qu'il soit différent de $1 \pmod e$.

Ainsi le nombre premier q obtenu satisfait la relation $q = k_{(o)}$ différent de $1 \pmod e$.

La génération du nombre premier p est identique, q est remplacé par p dans les étapes qui ont été développées et lo par l-lo.

Comme cela a été dit, le programme mettant en œuvre le procédé de la carte n'a pas besoin de connaître à priori l'exposant public e. Cet exposant peut donc être fourni à tout moment par une application chargée dans la carte.

Toutefois, on sait que pour la plupart des applications (plus de 95%), les valeurs de e utilisées sont les valeurs $\{3, 17, 2^{16}+1\}$.

Afin de couvrir le plus grand nombre d'applications, on va de façon préférentielle choisir a tel que $a= 1 \bmod(\{3, 17, 2^{16}+1\})$ et forcer $k_{(o)}$ différent de cette valeur : $1 \bmod(\{3, 17, 2^{16}+1\})$.

On choisit par exemple comme candidat possible pour a, le nombre premier $R= 2^{64}-2^{32}+1$ à condition que le plus grand commun diviseur de Π et de R soit égal à 1.

La condition requise pour $k_{(o)}$ peut être obtenue par le théorème du reste chinois.

Comme cela a été dit une autre alternative peut consister pour l'étape A-1) à calculer des couples de nombres premiers (p,q) pour différents couples (e,l) probables.

En conclusion, l'invention propose un procédé en deux étapes dissociées, la deuxième étape très rapide par rapport aux solutions connues, peut être exécutée en temps réel. Ce procédé est également peu coûteux en place mémoire.

En outre, il n'y a pas de limite pour de nouvelles applications non prévues à la personnalisation de la carte.

REVENDICATIONS

1. Procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique, principalement caractérisé en ce qu'il comprend deux étapes de calcul dissociées :

Etape A

1) Calcul de couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N dudit procédé,
2) Stockage des couples ou des valeurs ainsi obtenus ;

Etape B

Calcul d'une clé d à partir des résultats de l'étape A et de la connaissance du couple (e,l).

2. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) consiste à calculer des couples de nombres premiers (p,q) sans connaissance de l'exposant public e ni de la longueur l de la clé, en utilisant un paramètre Π qui est le produit de petits nombres premiers, de manière à ce que chaque couple (p,q) ait une probabilité maximale de pouvoir correspondre à un futur couple (e,l) et puisse permettre de calculer une clé d.

3. Procédé de génération de clés électroniques selon la revendication 2, caractérisé en ce que le

calcul de l'étape A-1) tient compte en plus du fait que e a une forte probabilité de faire partie de l'ensemble $\{3, 17, \ldots, 2^{16+1}\}$, on utilise pour cela dans ce calcul une graine σ qui permet de calculer non pas des couples (p,q) mais une valeur représentative appelée image des couples (p,q).

4. Procédé de génération de clés électroniques selon la revendication 1 et 3, caractérisé en ce le stockage A-2) consiste à mémoriser l'image des couples.

5. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) consiste à calculer des couples de nombres premiers (p,q) pour différents couples (e,l) probables.

6. Procédé de génération de clés électroniques selon les revendications 2 et 5, caractérisé en ce que le paramètre Π contient les valeurs usuelles de l'exposant public e par exemple 3, 17.

7. Procédé de génération de clés électroniques selon la revendications 1, caractérisé en ce que l'étape A-1) comprend une opération de compression des couples (p,q) calculés et l'étape A-2) consiste alors à stocker les valeurs compressées ainsi obtenues.

8. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) comprend la génération d'un nombre premier q, pour lequel on fixe une limite inférieure B_0 pour la longueur ℓ_0 de ce nombre premier à générer, telle que $\ell_0 \geq B_0$ par exemple B_0= 256 bits, et en ce qu'elle comprend les sous étapes suivantes :

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$

$w = 2^{\ell_0} / \Pi$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \leq 2^{B_0}$,

2)-choisir un nombre j dans l'intervalle des nombres entiers $\{v, \ldots, w-1\}$ et calculer $\ell = j \Pi$;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers $\{0, \ldots, \Pi - 1\}$, (k, Π) étant co-premiers, ;

4)-calculer $q = k + \ell$,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a k \pmod{\Pi}$; a appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π;

b) réitérer à partir de l'étape 4) ;

9. Procédé de génération de clés électroniques selon les revendications 3 et 8, caractérisé en ce que les nombres j et k peuvent être générés à partir de la graine σ stockée en mémoire.

10. Procédé de génération de clés électroniques selon la revendication 8, caractérisé en ce que le nombre premier p est généré en réitérant toutes les sous étapes précédentes en remplaçant q par p et en remplaçant ℓ_0 par $\ell - \ell_0$.

11. Procédé de génération de clés électroniques selon l'une quelconque des revendications précédentes, caractérisé en ce que :

L'étape B comprend, pour un couple (p,q) obtenu à l'étape A, :

- La vérification des conditions suivantes :
  (i) p-1 et q-1 premiers avec e donné et,
  (ii) N= p*q un nombre entier de longueur ℓ donnée,
- Si le couple (p'q) ne répond pas à ces conditions :
- Choix d'un autre couple et réitération de la vérification jusqu'à ce qu'un couple convienne,
- Calcul de la clé d à partir du couple (p,q) obtenu.

12. Objet sécurisé portatif apte à générer des clés électroniques d d'un algorithme de cryptographie de type RSA, caractérisé en ce qu'il comprend au moins :

- Des moyens de communication pour recevoir au moins un couple (e,l),
- Une mémoire pour stoker les résultats d'une étape A consistant à :

  Calculer des couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N de ce p,
- Un programme pour mettre en œuvre une étape B consistant à :

  Calculer une clé d à partir des résultats de l'étape A et de la connaissance d'un couple (e,l),

13. Objet sécurisé portatif selon la revendication 12, caractérisé en ce qu'il comprend en outre un programme pour la mise en œuvre de l'étape A, les étapes A et B étant dissociées dans le temps.

14. Objet sécurisé portatif selon la revendication 13, caractérisé en ce que le programme de mise en œuvre de l'étape A met en œuvre les sous-étapes :

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \leq 2^{B_0}$, B_0 est une limite inférieure fixée pour la longueur ℓ_0 du nombre premier à générer telle que $\ell_0 \geq B_0$ par exemple $B_0 = 256$ bits,

2)-choisir un nombre j dans l'intervalle des nombres entiers $\{v, \ldots, w-1\}$ et calculer $\ell = j\ \Pi$;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers $\{0, \ldots, \Pi - 1\}$, (k, Π) étant co-premiers, ;

4)-calculer $q = k + \ell$,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a\ k\ (mod\ \Pi)$; a appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π;

b) réitérer à partir de l'étape 4).

15. Objet sécurisé portatif selon la revendication 12 ou 13 ou 14, caractérisé en ce qu'il est constitué par une carte à puce.

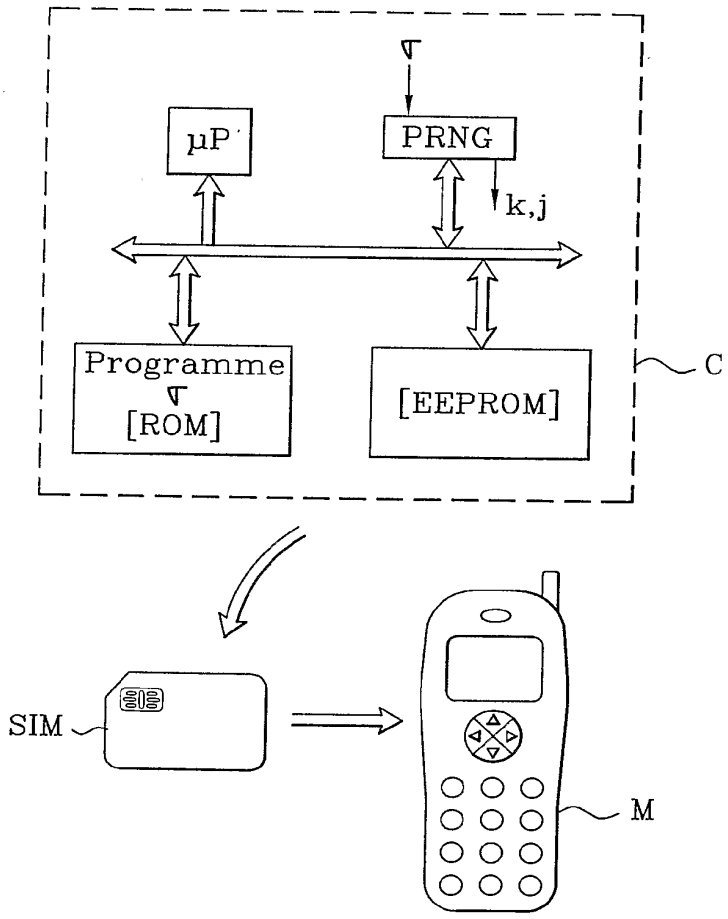


Figure unique

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2004 (23.09.2004)

PCT

(10) International Publication Number
WO 2004/081706 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/SG2004/000024

(22) International Filing Date: 27 January 2004 (27.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003901095 11 March 2003 (11.03.2003) AU

(71) Applicant *(for US only)*: **DIGISAFE PTE LTD** [SG/SG]; 100 Jurong East St 21, Singapore 609602 (SG).

(72) Inventors; and

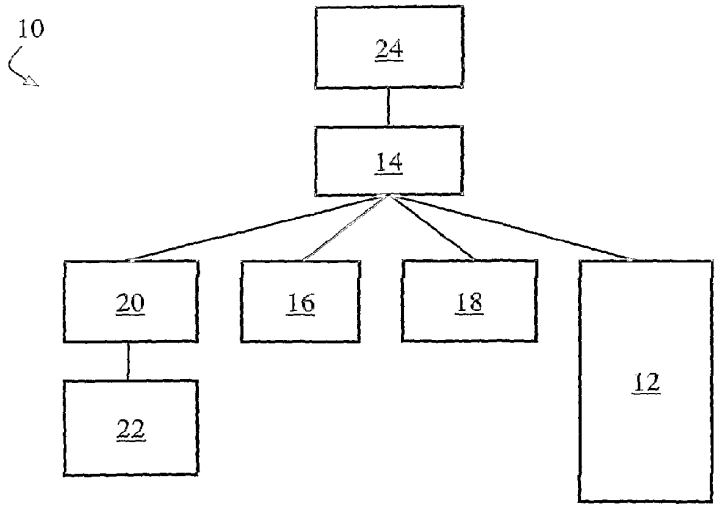
(75) Inventors/Applicants *(for US only)*: **CHOW, Andrew** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **LEE, Ser, Yen** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **LAU, Puay, Hui** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **CHIA, Boon, Quee** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **TAN, Teck, Weng, Paul** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **NG, Chee, We** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **SOO, Hin, Meng, Timothy** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **GATTAMENI, Venkateswara, Rao** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **LOO, Whye, Ho, Jamez** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG).

(74) Agent: **SIM, Yuan, Meng, Andrew**; Shook Lin & Bok, 1 Robinson Road, #18-00 AIA Tower, Singapore 048542 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR CONTROLLING THE PROVISION OF DIGITAL CONTENT



(57) Abstract: An apparatus for controlling the provision of digital content, comprising a data storage device controller for receiving a data storage device on which is provided the content, an authentication data storage device for storing authentication data, a data port connectable to a host device so that the apparatus can be placed into electronic communication with the host device, and a communications hub to mediate electronic communication between the data storage device controller, the authentication data storage device and the data port, wherein the apparatus is configured to permit content provided on the data storage device to be outputted from the data port according to the authentication data.

WO 2004/081706 A2

MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

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.

METHOD AND APPARATUS FOR CONTROLLING THE PROVISION OF DIGITAL CONTENT

FIELD OF THE INVENTION

The present invention relates to a digital security method and apparatus, of particular but by no means exclusive application in controlling the distribution of electronic content such as software (and, in one particular example, software drivers), the distribution of digital content or media with copy protection, digital personal identification devices (typically carrying personal identity and other data), data management and portable devices for the secure storage of electronic content (such as data or software).

BACKGROUND OF THE INVENTION

Software including software drivers are presently commonly distributed with corresponding hardware on computer readable media such as CD-ROM, or over the Internet. These approaches, however, require the provision of such media or an Internet connection, both restrictions on the portability of the hardware.

Currently techniques exist for preventing the copying of digital content on music CDs, but few particular effective approaches exist for digital media such as floppy diskettes, zip diskettes, CD-ROMs and USB-flash devices.

In the field of smart cards and other devices for storing personal data or for data management, techniques such as the use of secret keys and digital certificates are presently employed to identify a person's identity. Personal Digital Assistants (PDAs) carry personal information but are not generically designed to prove a person's identity. No such device exists that combines the storage of a person's identity with personal information such as electronic mail.

There also exist a number of mass storage USB tokens, including that of Trek Technology (Singapore) Pte Ltd as described in WO 01/61692. Further, WO 00/42491 (Rainbow Technologies Inc) describes a cryptographic USB token.

Existing approaches for the portable secure storage of digital data also include the encryption of files on diskettes.

SUMMARY OF THE INVENTION

The present provides, in a first broad aspect, an apparatus for controlling the provision of digital content, comprising:

a data storage device controller for receiving a data storage device on which is provided said content;

an authentication data storage device for storing authentication data;

a data port connectable to a host device so that said apparatus can be placed into electronic communication with said host device; and

a communications hub to mediate electronic communication between said data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit content provided on said data storage device to be outputted from said data port according to said authentication data.

Preferably said data storage device is a non-volatile data storage device. More preferably said data storage device is a flash memory device. In these embodiments, the data storage device controller is preferably a controller suitable for the respective device.

Thus, content (which could comprise software, audio,

video, personal or other information, etc.) can be provided on the data storage device (such as a flash memory device, for example a flash card), but only copied to the data port (and thence to, for example, a computer or a playback device) if a suitable correspondence exists between the authentication data and the content. For example, the content may be configured to be read from the data storage device only if a particular password, security key or digital certificate is provided: that password or security key would be stored as the authentication data on the authentication data storage device. The authentication data storage device could take any suitable form, as will be understood by those in the art, such as a smart card chip or a biometric device.

It should be understood, however, that the apparatus - though configured to permit content provided on said data storage device to be outputted from the data port according to said authentication data - may be configured so that this outputting is limited in a predetermined way. Thus, the data storage device may include a first storage portion for storing at least one software viewer or player for viewing or playing said content, and a second storage portion for storing said content, wherein said apparatus is configured to permit the accessing of said software viewer or player and of said content (such as by a computer when said apparatus is connected to that computer) such that said content can be viewed or played by means of said software viewer or player without allowing said content to be copied (such as to another device, storage medium or printer).

Preferably the apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device. The cryptographic key may comprise or be derived from the

authentication data.

Thus, the authentication data (whether comprising a password, a secret key and/or a digital certificate, or otherwise) can additionally be used for encryption and copy protection, and the apparatus is preferably operable to encrypt and/or decrypt said content on the basis of the authentication data (i.e. using the authentication data as a cryptographic key, or deriving a cryptographic key from the authentication data).

The authentication data storage device may also comprise a combination of secure microcontrollers and EEPROM chips.

The invention thereby provides an apparatus that can be used as both a mass storage token and as a cryptographic token (the latter preferably in the form of a cryptographic processor).

Preferably said communications hub comprises a Universal Serial Bus (USB) hub.

Preferably the data port comprises a USB connector.

In one embodiment, said content comprises software.

In another embodiment, said content comprises software device drivers.

Preferably said apparatus includes a communications port for connecting said apparatus to a hardware device associated with said content.

Alternatively, said apparatus is provided in a hardware device and in electronic communication with said hardware device.

Thus, the hardware device would typically be a hardware peripheral that the software device drivers will be working with. The data storage device is then used to contain the software drivers for the hardware device, or digital media, personal data and other data to be secured. The authentication data storage device can then also store unique secret keys for identifying the hardware device and/or for ensuring the authenticity and originality of the hardware.

In another embodiment, when the content comprises digital media for distribution with copy protection, the data storage device contains software portions or drivers for reading, displaying or playing said digital media.

Thus, these software components would typically be designed to prevent unauthorized duplication of the digital media stored on the data storage device by using techniques such as encryption and capturing operating system functions.

In one embodiment, further authentication data is stored on said data storage device.

Thus, for data management (such as of personal data), the content comprises software modules for the host device that are designed to be incorporated into software applications so that personal identity data, such as secret keys and digital certificates, may be stored in the data storage device as well as in the authentication data storage device. Other personal data, such as email and personal calendar, can be stored in the data storage device.

In another embodiment, for portable secure storage of digital data, the data storage device contains said digital data in encrypted form while the authentication

data storage device contains secret keys for the encryption.

In all the applications above, the data in the data storage device may be in clear or in encrypted form, depending on the application.

The present also provides, in a second broad aspect, a method for controlling the provision of digital content, comprising:

providing said content on a data storage device readable by means of a data storage device controller;

providing authentication data on an authentication data storage device;

placing said data storage device controller and authentication data storage device in data communication with a host device;

controlling the provision of said content to said host device according to at least said authentication data.

The present provides, in a third broad aspect, a method for controlling access to digital content, comprising:

providing said content on a computing or other electronic device;

providing authentication data and control software on an authentication apparatus comprising:

a control software storage device controller for receiving a control software storage device on which is provided control software;

an authentication data storage device for storing authentication data;

a data port connectable to said computing or other electronic device so that said apparatus can be placed into electronic communication with said computing or other electronic device; and

a communications hub to mediate electronic

communication between said authentication data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit said control software provided on said control software storage device storage device to be used to control application software on said computing or other electronic device according to said authentication data.

The electronic device could be a computer peripheral, such as a printer, a scanner or a digital camera. By this means, the software drivers can be distributed with the electronic device itself, rather than on a separate CD-ROM or the like.

Preferably the authentication apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device. More preferably, the cryptographic key comprises or is derived from the authentication data.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the present invention may be more clearly ascertained, preferred embodiments will now be described, by way of example, with reference to the accompanying drawing, in which:

Figure 1 is a schematic diagram of an apparatus for distributing content associated with a hardware device according to a preferred embodiment of the present invention, together with the hardware device;

Figure 2 is a schematic diagram of an apparatus for distributing software device drivers associated with a hardware device according to another preferred embodiment of the present invention, together with the hardware device;

Figure 3 is a schematic diagram of an apparatus

for distributing digital storage media with copy protection according to a further preferred embodiment of the present invention;

Figure 4 is a schematic diagram of an authentication apparatus for personal identity and data management and for portable secure storage of digital data according to another preferred embodiment of the present invention;

Figure 5 is a schematic diagram of a system for centrally programming and managing the apparatus of figure 4; and

Figure 6 is a perspective view of an example of the apparatus of figure 4.

DETAILED DESCRIPTION OF THE DRAWINGS

An apparatus 10 for distributing digital content associated with a hardware device according to an embodiment of the present invention, together with the hardware device 12, is shown in figure 1.

The apparatus 10 comprises a Universal Serial Bus (USB) hub 14, an authentication device in the form of a smart card chip 16 or a biometric device 18, a flash controller 20 for reading flash memory 22 and a USB connector 24.

The authentication device 16,18 and the flash controller 20 communicate via USB hub 14 with a host device (not shown: typically a computer) by means of USB connector 24. The apparatus 10 is in fact incorporated within the hardware device 12 and connected thereto by means of a further USB connector (not shown) to the USB hub 14. The USB hub 14 in this embodiment will typically be the USB hub of the hardware device 12 itself.

The content on flash memory 22 (provided with the hardware device 12) to the host device is permitted only if the correct and corresponding authentication data is detected

on the authentication device 16,18.

Particular examples of applications of this approach are given below by reference to figures 2 to 4.

(1) Software Driver Distribution

Figure 2 is a schematic diagram of an apparatus 30 for distributing software device drivers associated with a hardware device according to an embodiment of the present invention, together with the hardware device 32.

The apparatus 30 comprises USB hub 34, an authentication device in the form of a smart card chip 36, a flash controller 40 for reading flash memory 42 and a USB connector 44. Flash memory 42 contains the content (here in the form of the software device drivers for hardware device 32) that are needed for the operating system of the host device (not shown, but connected at USB connector 44) to operate with the hardware device 32. The hardware device 32 could be a computer peripheral such as a printer, or scanner, or it could represent a smart card that itself acts as the authentication device.

The smart card chip 36 contains secret keys, etc., for establishing authenticity of the hardware device 32 and the software device driver: the software device driver performs authentication with the smart card chip 36 to ensure that the device driver has not been modified and the hardware device 32 is original.

(2) Digital Media Distribution with Copy Protection

Figure 3 is a schematic diagram of an apparatus 50 for distributing digital storage media with copy protection according to an embodiment of the present invention. The content in this example may be digitized music and video such as MP3 and MPEG or software packages.

The apparatus 50 comprises USB hub 54, an authentication device in the form of a smart card chip 56, a flash controller 60 for reading flash memory 62 and a USB connector 64. Flash memory 62 contains the content, in this example in the form of audio/video digital content to be distributed, and software applications to view, play and install the content on the host device (not shown, but connected at USB connector 64).

The content stored in the flash memory 62 is in encrypted form to prevent unauthorized duplication. Software viewers, players or installers also reside in the flash memory. The viewers, players and installers are written in a way that they only allow the media and applications to be viewed, played or installed, but do not allow them to be duplicated. Strong cryptographic protocols are used in these viewers, players and installers to prevent unauthorized duplication.

The smart card chip 56 contains secret keys or other parameters to prove the authenticity and originality of the media. Other information regarding the number of times a digital data has been accessed or the identity of the computer or player can be recorded in the smart card chip. This allows the number of times or the location the digital data or the software package has been accessed or installed can be restricted.

(3) Personal Identity and Data Management and Portable Secure Storage of Digital Data

Figure 4 is a schematic diagram of an authentication apparatus 70 for personal identity and data management and for portable secure storage of digital data in the form of personal identity data according to an embodiment of the present invention. The authentication data is in the form of personal identity data such as digital certificates and passwords while the content (or personal data) could be

electronic mail, personal documents, passwords, and other data.

The apparatus 70 comprises USB hub 74, an authentication device in the form of a smart card chip 76, a flash controller 80 for reading flash memory 82 and a USB connector 84. Flash memory 82 contains the content which, as mentioned above, in this example is in the form of electronic mail, personal documents, passwords and other data.

The flash memory 82 is used to store these data in clear or encrypted form. The more sensitive data (together with the digital certificates or passwords for proving identity or the secret keys used to sign, encrypt and decrypt the data in the flash card 82) is securely stored in the smart card chip 76.

Digital certificates are used for secure computer applications such as secure email (S/MIME) and secure internet connection (Secure Socket Layer, SSL), for signing and encrypting email.

Figure 5 is a schematic diagram of a system 90 for centrally programming and managing the authentication apparatus 70 of figure 4, in use with such the authentication apparatus 70 and a computer network 92.

The system 90 comprises a central management system 94 and a programmer 96. The programmer 96 includes a USB port for connecting to the USB port of USB connector 84 of authentication apparatus 70, so that the system 90 can be used to program each such authentication apparatus 70 by installing in an authentication apparatus 70 keys belonging to each user.

The keys are held in a Public Key Depository 98, which

holds such keys for secure applications such as S/MIME. The Public Key Depository 98 is accessible by the central management system 94 by computer network.

The system 90 installs - into the flash memory 82 of each authentication apparatus 70 - installation and configuration programs for subsequently configuring the software applications on networked computers 100 (each running secure applications such as S/MIME) on computer network 92; a user can take an authentication apparatus that has been programmed in this manner (such as authentication apparatus 70') and use it to gain ready access to those applications on any of computers 100. This enables each user to use these applications easily without the necessity of a system administrator installing applications or performing configuration for the user. The user also does not need to carry along another medium (such as an installation disk), and is free to perform this installation at all the computers that the user is authorized to use.

This convenience for the user is enabled by the flash storage space, in addition to the smart card chip, the latter of which is responsible for the key storage.

This system thus reduces the complexity of deployment by incorporating all the installation program and information within the device itself.

Figure 6 is a perspective view of an example of an authentication apparatus 102 according to this embodiment (such as authentication apparatus 70 of figures 4 and 5). As is apparent in this figure, the authentication apparatus 102 includes a UBS plug 104 (for plugging into a USB port) and a body 106 that encases the data storage and processing components of the apparatus. The apparatus 102 is designed to be hand-held, so it is of appropriate

dimensions and provided with finger grips 108 for ease of manipulation.

Thus, the present invention allows device drivers to be distributed together with the hardware device itself, and for a single architecture to be used for multiple applications.

Modifications within the scope of the invention may be readily effected by those skilled in the art. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

In the claims that follow and in the preceding description of the invention, except where the context requires otherwise owing to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" is used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

CLAIMS:

1. An apparatus for controlling the provision of digital content, comprising:

a data storage device controller for receiving a data storage device on which is provided said content;

an authentication data storage device for storing authentication data;

a data port connectable to a host device so that said apparatus can be placed into electronic communication with said host device; and

a communications hub to mediate electronic communication between said data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit content provided on said data storage device to be outputted from said data port according to said authentication data.

2. An apparatus as claimed in claim 1, wherein said apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device.

3. An apparatus as claimed in claim 2, wherein said cryptographic key comprises or is derived from said authentication data.

4. An apparatus as claimed in any one of the preceding claims, wherein said data storage device includes a first storage portion for storing at least one software viewer or player for viewing or playing said content, and a second storage portion for storing said content, wherein said apparatus is configured to permit the accessing of said software viewer or player and of said content such

that said content can be viewed or played by means of said software viewer or player without allowing said content to be copied.

5. An apparatus as claimed in any one of the preceding claims, wherein said authentication data storage device comprises a combination of secure microcontrollers and EEPROM chips and said data storage device is a flash memory device.

6. An apparatus as claimed in any one of the preceding claims, wherein said communications hub comprises a Universal Serial Bus hub.

7. An apparatus as claimed in any one of the preceding claims, wherein said data port comprises a Universal Serial Bus connector.

8. An apparatus as claimed in any one of the preceding claims, wherein said content comprises software.

9. An apparatus as claimed in any one of preceding claims, wherein said content comprises software device drivers.

10. An apparatus as claimed in any one of preceding claims, including a communications port for connecting said apparatus to a hardware device associated with said content.

11. An apparatus as claimed in any one of preceding claims, wherein said apparatus is provided in a hardware device and in electronic communication with said hardware device.

12. An apparatus as claimed in claim 1, wherein said content comprises digital media for distribution with copy

protection, and said data storage device contains software portions or drivers for reading, displaying or playing said digital media.

13. An apparatus as claimed in claim 1, wherein further authentication data is stored on said data storage device.

14. A method for controlling the provision of digital content, comprising:

providing said content on a data storage device readable by means of a data storage device controller;

providing authentication data on an authentication data storage device;

placing said data storage device controller and authentication data storage device in data communication with a host device;

controlling the provision of said content to said host device according to at least said authentication data.

15. A method as claimed in claim 14, including encrypting or decrypting said content by means of at least one cryptographic key stored in said authentication data storage device.

16. A method as claimed in claim 15, wherein said cryptographic key comprises or is derived from said authentication data.

17. A method for controlling access to digital content, comprising:

providing said content on a computing or other electronic device;

providing authentication data and control software on an authentication apparatus comprising:

a control software storage device controller for receiving a control software storage device

on which is provided control software;

an authentication data storage device for storing authentication data;

a data port connectable to said computing or other electronic device so that said authentication apparatus can be placed into electronic communication with said computing or other electronic device; and

a communications hub to mediate electronic communication between said authentication data storage device controller, said authentication data storage device and said data port;

wherein said authentication apparatus is configured to permit said control software provided on said control software storage device storage device to be used to control application software on said computing or other electronic device according to said authentication data.

18. A method as claimed in claim 17, wherein said authentication apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device.

19. A method as claimed in claim 18, wherein said cryptographic key comprises or is derived from said authentication data.

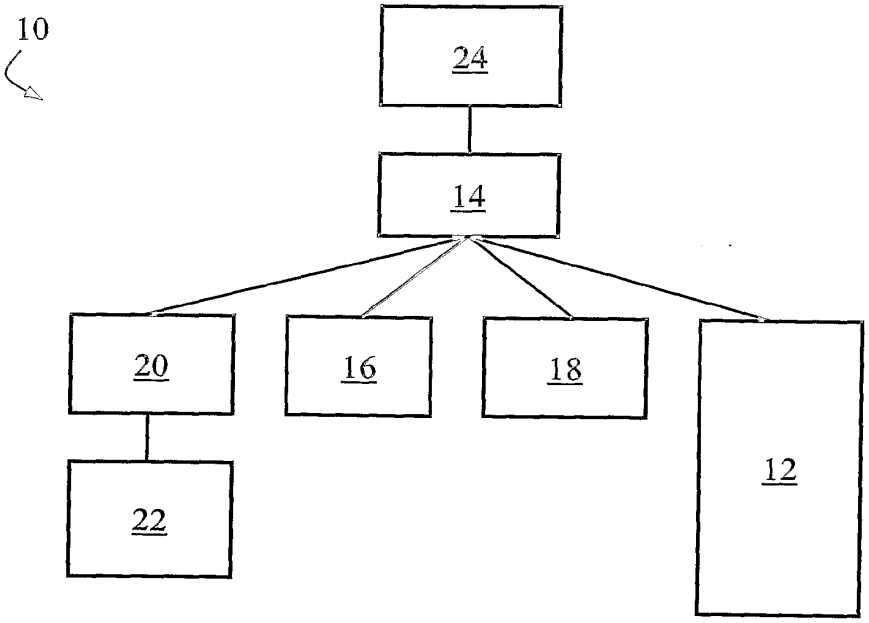


Figure 1

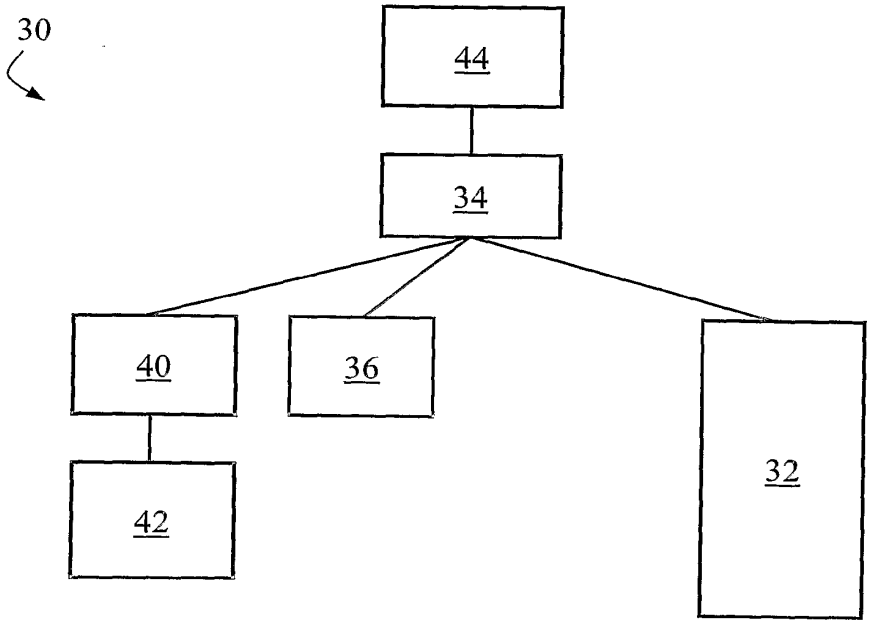


Figure 2

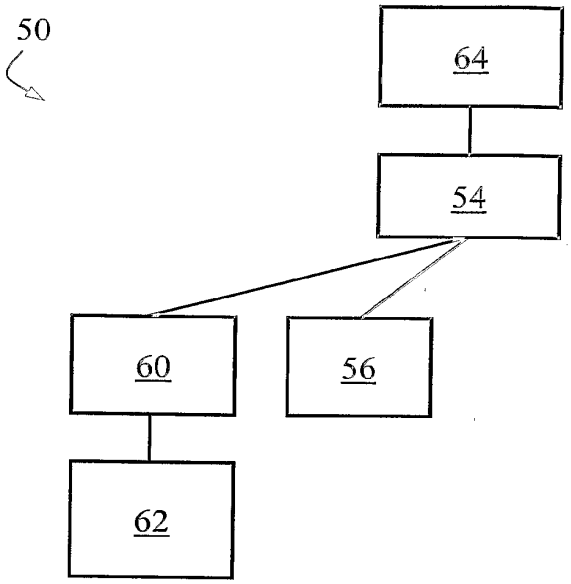


Figure 3

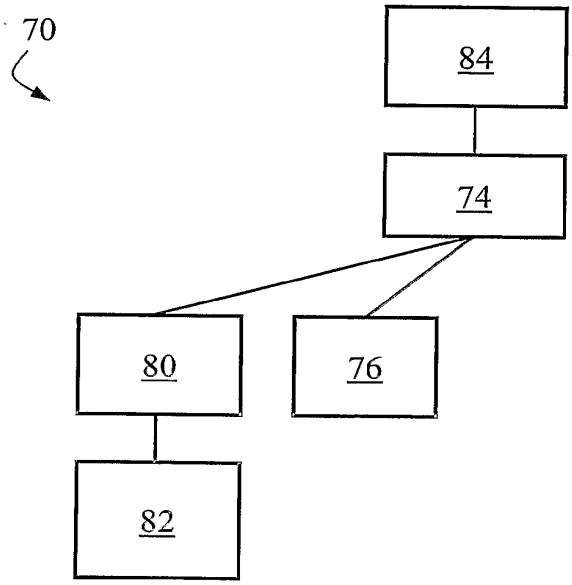


Figure 4

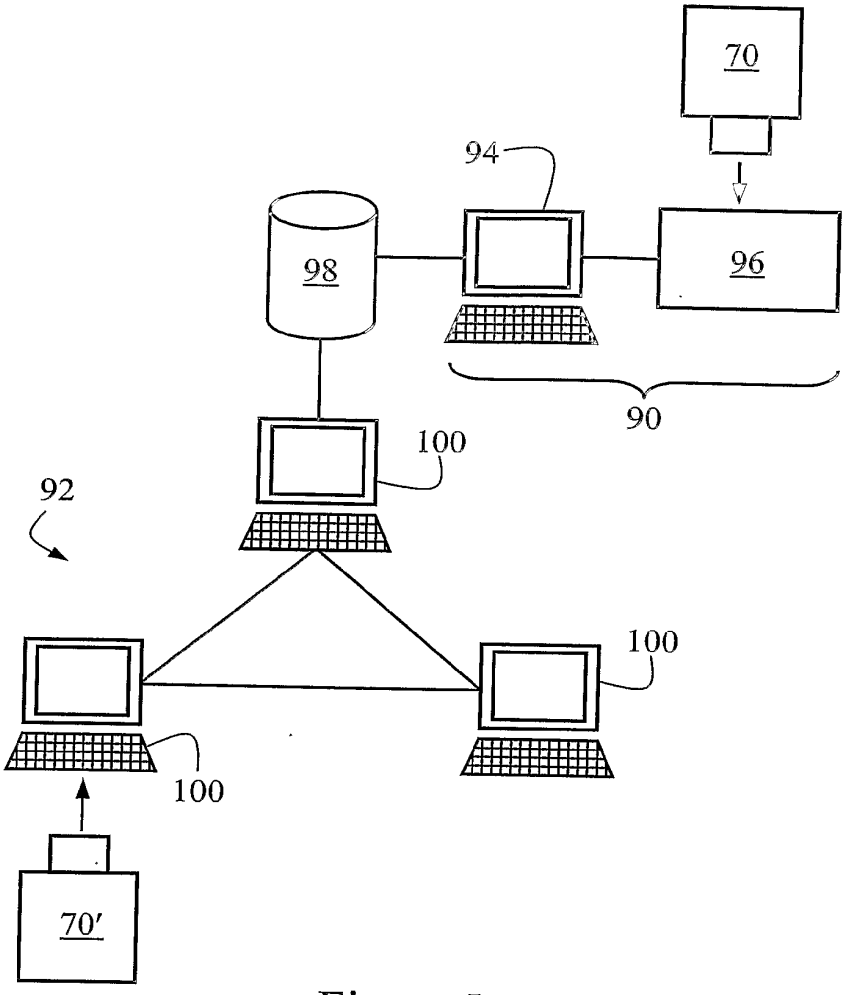


Figure 5

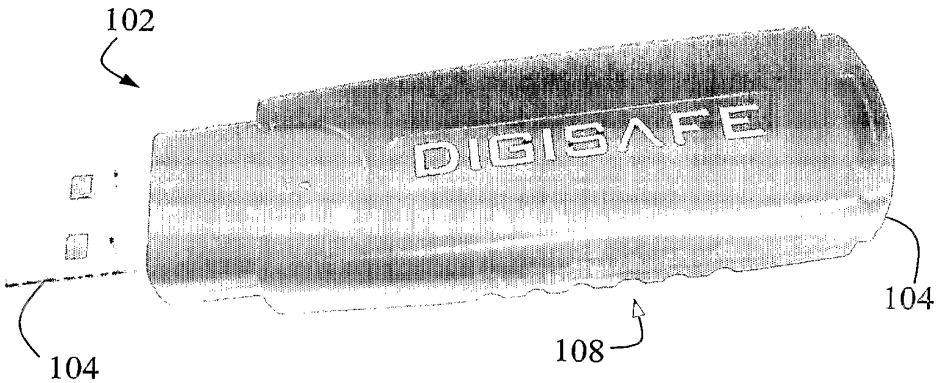


Figure 6

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2004 (23.09.2004)

PCT

(10) International Publication Number
WO 2004/081769 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/IB2004/000738

(22) International Filing Date: 12 March 2004 (12.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03290655.4 14 March 2003 (14.03.2003) EP

(71) Applicant *(for all designated States except US)*: **AXALTO SA** [FR/FR]; 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR).

(71) Applicant *(for MC only)*: **SCHLUMBERGER MALCO INC** [US/US]; 9800 Reistertown, OwinG Mills, Owing Mills, MD 21117 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **AKKAR, Mehdi-Laurent** [FR/FR]; 17 Rue Lafouge, F-94250 Gentilly (FR).

(74) Common Representative: **SCHLUMBERGER SYSTEMES**; C/O Patrice GUILLERM, 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

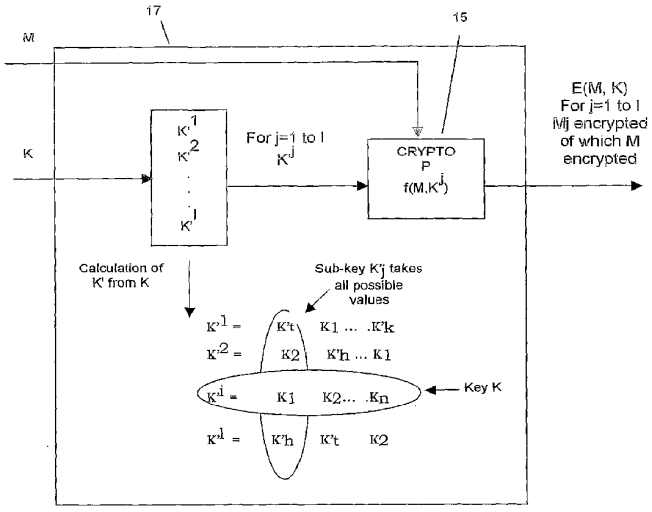
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

[Continued on next page]

(54) Title: PROCESS OF SECURITY OF A UNIT ELECTRONIC UNIT WITH CRYPTOPROCESSOR



(57) Abstract: The invention concerns a process for securing an electronic device incorporating a hardware component capable of autonomous implementation of calculation process f using one key K. the process involves calculating at least two new keys K^i such that at least one of said new keys is identical to key K, and one of said new keys is different from key K, and executing said calculation process f successively with each of said calculated keys K^i, using said hardware component.

WO 2004/081769 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

PROCESS OF SECURITY OF A UNIT ELECTRONIC WITH CRYPTOPROCESSOR

The invention concerns a process for securing an electronic device incorporating a hardware component such as a cryptoprocessor, for the purpose of autonomous implementation of a cryptographic algorithm using a secret quantity such as a secret key. In more precise terms, the process is designed to secure said cryptoprocessor against a certain type of physical attacks referred to as Differential Power Analysis (first order electronic attacks or higher) which seek to obtain information concerning the secret key by studying the power consumption of the electronic device during execution of calculations.

TECHNICAL DOMAIN

Certain components incorporate a hardware DES algorithm. The DES algorithm has the advantage of being extremely fast – of the order of 20 microseconds – and can apparently withstand SPA and DFA type attacks. Unfortunately, it cannot withstand a first order DPA attack. Indeed, with a reasonable number of samples – of the order of 10,000 – it is possible to extract the key. Faced with this vulnerability, it can be necessary to reprogram a secure software DES in full.

One purpose of this invention is to propose a process and system for securing components incorporating cryptoprocessors or equivalent devices, in particular against DPA type attacks.

The cryptographic algorithms considered here use a secret key to calculate output information according to input information. This can involve an encryption, decryption, signature or signature verification, authentication or non-repudiation operation. The

algorithms are constructed in such a way that an attacker with knowledge of the inputs and outputs, cannot in practice deduce any information concerning the secret key itself. Numerous applications base their security on secret key cryptographic algorithms such as the DES, or the more recent AES algorithm, which has now taken its place as the world-wide encryption standard (see John Daemen, Vincent Rijmen; AES proposal; Rijndael: http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf).

We are interested in a broader class than that traditionally designated by the expression *secret key algorithm* or *symmetrical algorithm*. In particular, all that is described in this patent application also applies to the so-called public key or asymmetrical algorithms, which in fact incorporate two keys, one public and the other private and not disclosed, the latter being the target for the attacks described below.

The Power Analysis type attacks described by Paul Kocher and Cryptography Research (see document "Introduction to Differential Power Analysis and Related Attacks" by Paul Kocher, Joshua Jaffe and Benjamin Jun, Cryptography Research, 870 Market St., Suite 1008, San Francisco, CA 94102, HTML version of the document accessible at URL address: http://www.cryptography.com/dpa/technical/index.html, mentioned in this application for reference purposes) are based on the observation that, in reality, the attacker can acquire information other than simple input and output data, on execution of calculations, such as the power consumption of the microcontroller or the electromagnetic radiation emitted by the circuit, for example. This information, which depends on secret quantities such as the key, leaks from the card.

Differential Power Analysis, abbreviated to DPA, is an attack which makes it possible to obtain information concerning the secret

key contained in the electronic device, by making a statistical analysis of records of power consumption for a large number of calculations with the same key.

We can consider, as a non-exhaustive example, the case of the DES (Data Encryption Standard) algorithm, a description of which can be found in any of the following documents:

FIPS PUB 46-2, Data Encryption Standard, 1994;

FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, 1981;

ANSI X3.92, American National Standard, Data Encryption Algorithm, 1981;

ISO/IEC 8731:1987, Banking - Approved Algorithms for Message Authentication - Part 1: Data Encryption Algorithm (DEA).

Or in the following work:

Bruce Schneier, Applied Cryptography, 2nd edition, John Wiley & Sons, 1996, page 270.

The above-mentioned documents are indicated in this application for reference purposes.

The DES algorithm is executed in 16 steps referred to as rounds (see Figure 1a). In each of these 16 rounds, conversion F is executed on 32 bits. This conversion F uses eight 6-bit to 4-bit non-linear conversions, each coded in a table referred to as an S-box (see Figure 1b), where the S-boxes are noted S1, S2, ..., S8.

A DPA attack on the DES algorithm can be implemented as follows:

1st step: Consumption is measured on the first round for 1,000 DES calculations. The input values for these 1,000 calculations are noted E[1], ..., E[1000]. The 1,000 curves corresponding to power consumption measured for these calculations are noted C[1], ..., C[1,000]. Mean curve CM is also calculated for the 1,000 consumption curves.

2nd step: We consider the first output bit from the first S-box on the first round, for example. The value of this bit is noted b. It is easy to see that b only depends on 6 bits of the secret key. The attacker makes an assumption concerning the 6 bits concerned. The attacker calculates the theoretical values expected for b from these 6 bits and the E[i]. This makes it possible to separate the 1,000 inputs E[1], ..., E[1,000] into two categories: those which give b=0, and those which give b=1.

3rd step: Mean value CM' is then calculated for the curves corresponding to the first category inputs, namely those for which b=0. If CM and CM' show a marked difference, it is considered that the values adopted for the 6 bits of the key were correct. If CM and CM' do not show a marked difference in the statistical sense, namely no difference substantially greater than the typical variance for the noise measured, the 2nd step is repeated with a different selection for the 6 bits.

4th step: Steps 2 and 3 are repeated with a target bit b from the second S-box, and then from the third S-box, and so on up to the eighth S-box. Forty-eight bits of the secret key are finally obtained in this way.

5th step: The 8 remaining bits can be found by exhaustive search.

This attack requires no knowledge concerning the individual power consumption of each instruction, nor the position in time of each of these instructions. It applies in the same way if we assume that the attacker knows the outputs of the algorithm and corresponding consumption curves. It is based solely on the following fundamental assumption:

Fundamental assumption: An intermediate variable exists, appearing during the course of calculation of the algorithm, such that knowledge of a few key bits, in practice less than 32 bits, is sufficient to decide whether two inputs, respectively two outputs, give the same

value for this variable or not.

All algorithms using the S-box principle, such as the DES algorithm, are potentially vulnerable to DPA attack, as the customary methods of implementation generally lie within the framework of the assumption mentioned above.

So-called High-Order Differential Power Analysis attacks, abbreviated to HO-DPA, correspond to generalisation of the DPA type attack described above. They can use a number of different information sources apart from consumption, and can involve measurement of electromagnetic radiation, temperature, etc., and employ more sophisticated statistical processing than the simple notion of average, with less elementary intermediate variables (generalising bit b defined above). Nevertheless, they are based on precisely the same fundamental assumption as the DPA attack.

SUMMARY OF THE INVENTION

The invention concerns a process for securing an electronic device incorporating a hardware component capable of autonomous implementation of a calculation process using key K, characterised by the fact that it involves calculating at least two new keys $K^{'i}$ such that for at least one given i=j, $K^{'j}$=K and for at least one i=t, $K^{'t}$<> K, and executing said calculation process with each of said calculated keys $K^{'i}$ in succession, using said hardware component.

According to one particular form of implementation, the process involves calculating I=α m new keys K'^1, ..., K'^l, so that for a given j (0<j<n+1), sub-keys K'^i_j (0<i<l+1) take all the possible values, including the value of sub-key Kj, and executing hardware cryptographic function f with these l new keys K'^1, ..., K'^l, in a random manner.

The invention also concerns an electronic device and a smart card for example, and a program for implementation of the process.

BRIEF DESCRIPTION OF THE DRAWINGS

Other purposes, advantages and characteristics of the invention will emerge from the following description of implementation of the process according to the invention, and of a method of execution of an electronic device adapted for this implementation, given for non-exhaustive example purposes referring to the appended drawings where:

- Figure 1 shows an electronic device according to the invention in schematic form;

- Figure 2 shows a hardware component of said device according to Figure 1 in schematic form;
- Figure 3 shows the process according to the invention in schematic form.

IMPLEMENTATION OF THE INVENTION

The process according to the invention is designed to secure an electronic device, for example an on-board system such as a smart card implementing a cryptographic calculation process which uses a secret key. The electronic device incorporates means to process information, such as a processor, and means to store information such as a memory.

As a non-exhaustive example, the electronic device described below corresponds to an on-board system incorporating electronic module 1 as shown in Figure 1. Modules of this type usually take the form of a monolithic integrated electronic microcircuit or chip, which, once protected physically by any known means, can be mounted on a portable object such as a smart card, microcircuit card or other which can be used in various domains, for example.

Microprocessor electronic module 1 comprises CPU microprocessor 3, connected bidirectionally via internal bus 5 to a non-volatile memory 7 of the ROM, EEPROM, Flash, FeRam or other type containing an executable program, RAM memory 11, I/O device 13 for communication with the exterior, and cryptoprocessor calculation unit 15 (CRYPTO P), this component being capable of autonomous cryptographic calculation, such as calculation of a DES algorithm, for example. As shown in Figure 2, cryptoprocessor 15 of said module 1 executes calculation process f using secret key K, stored in a secret zone of a memory, for example of the EEPROM type, on a message M.

We will firstly consider the solution in its general form. As shown in Figure 3, the objective is to calculate result E(M,K) of cryptographic function E on message M, using key K. For this purpose, we have function f, which, in its capacity as a black box, executes the same calculation as E but cannot withstand DPA attack in particular. We also consider that key K acts in regard to the algorithm in the form of n small sub-keys mb (taking mb<10 bits, or $m=2^{mb}$ possible values for each sub-key), which will then be noted K1,K2, ... , Kn, and which will be susceptible to DPA attack in particular. The sub-keys are of the same size in the form of implementation described below. The invention also applies for sub-keys of a different size.

The invention involves associating external software module 17 with the cryptoprocessor, to secure the cryptographic function implemented by said cryptoprocessor 15.

As shown in Figure 3, the invention involves calculating $I=\alpha$ m new keys K'^1, ..., K'^I, so that for a given j ($0<j<n+1$), each sub-key K'^i_j ($0<i<l+1$) takes all the possible values, and according to a special form of implementation α times, including the value of sub-key Kj, and executing hardware cryptographic function f with these I new keys K'^1, ..., K'^I in a random manner.

In other words, the idea is to execute $I = \alpha$ m successive calculations with keys K'^i, $0 \leq i < l$, such that:

there exists i such that $K'^i = K$.

For all the j, we have $\{ K'^i j, 0 \leq i<n \} = \{0,1, \ldots ,n-1\}$, with each sub-key appearing exactly α times.

This means in fact that we will execute a number of successive calculations with different keys (including the true key), in such a way that each possible sub-key appears the same number of times.

The calculations will also be executed in a random order. Consequently, the attacker has no chance of identifying the correct sub-key by DPA attack, as this sub-key appears neither more nor less frequently than any other.

We will now see how this countermeasure (noted CM in the following paragraphs) applies to different algorithms.

Simple application to the DES algorithm

Notations

We will adopt the following notations for the DES algorithm:
PC1 represents the initial permutation of the key, reducing the key from 64 to 56 bits.
IPC1 represents the inverse of PC1 (56 bits to 64), where the 8 missing bits are completed (parity bits are frequently used).
PC2 represents the combination of compressive permutation (56 bits to 48 bits) and shift of the key to the first round.
IPC2 represents the inverse of PC2 (48 to 56 bits), where the 8 undetermined bits (8=56-48) are selected arbitrarily (for example randomly).
The permutation from 48 bits to 64 bits (combination of IPC2 and IPC1) is noted PP.

We see that PP makes it possible, starting from key K48 with 48 bits, used in the first round of the DES algorithm, to reach global key K64 =PP(K48) having the following property: using K64 as the key for a DES calculation, we obtain K48 as the first sub-key in the first round.

We will now see how we can apply our countermeasure in concrete terms.

1.1 Initial implementation of the CM

In the case of the DES algorithm, the sub-keys are used in the form of n=8 sub-keys of mb=6 bits each, giving m=64 possibilities. We shall then execute 64 successive calculations (α =1) with the following derivative keys:

$K_{00} = K \oplus PP(000000 \mid 000000 \mid \ldots \mid 000000 \mid 000000)$
$K_{01} = K \oplus PP(000001 \mid 000001 \mid \ldots \mid 000001 \mid 000001)$
$K_{02} = K \oplus PP(000010 \mid 000010 \mid \ldots \mid 000010 \mid 000010)$
$K_{03} = K \oplus PP(000011 \mid 000011 \mid \ldots \mid 000011 \mid 000011)$
.
.
.
$K_{61} = K \oplus PP(111101 \mid 111101 \mid \ldots \mid 111101 \mid 111101)$
$K_{62} = K \oplus PP(111110 \mid 111110 \mid \ldots \mid 111110 \mid 111110)$
$K_{63} = K \oplus PP(111111 \mid 111111 \mid \ldots \mid 111111 \mid 111111)$

It is thus easy to see that for each of the eight sub-keys used in the first round, the 64 possible values are represented equally, and that true key K00 is present in the list. It is then merely necessary to execute 64 DES calculations with the 64 derivative keys in a random order, and select the final result as being that where the correct key has been used.

This can be done in the following way. Sixteen memory bytes are allocated to store the result. An additional byte is also allocated for each Ki (initialised in this case at 0 or 8), which will indicate the byte from which the result is stored in memory. Thus, this byte will take the value 8 for all keys except K00 for which it will take the value 0. This makes it possible to use a relatively generic code, which could resemble the next pseudo-code C, considering that we have one

function executing a memory copy, one which calculates the PP(i | ... | i) and one which randomizes the 64 keys.

```
void
DES_encrypt_DPA( unsigned char in[8],
                 unsigned char cle[8],
                 unsigned char out[8] )
{
   int i;
   unsigned char M1[8], M2[16], K[64][9];

   memcopy(K[0],cle,8);
   K[0][8] = 0;

   for(i=1; i<64; i++)
   {
      memcopy(K[i], cle XOR PP(i | ... | i), 8);
      K[i][8] = 8;
   }

   randomize_0_63(K);

   for(i=0; i<64; i++)
   {
      memcopy(M1, in, 8);
      DES_encrypt_non_DPA(M1,K[i]);

      for(j=0;j<8;j++)
      {
         M2[K[i][8] + j] = M1[j];
      }
   }

   memcopy(out, M2, 8);
}
```

1.2 General security considerations

From the DPA point of view, it is easy to see that any attacker, unable to distinguish for each of the 64 executions of the DES algorithm whether the true key is concerned or not, cannot attack the algorithm with a conventional DPA. However, it must be remembered that programming of the method requires a very strict approach, as any analysis making it possible to distinguish – even rarely – the

correct key destroys the CM completely! Attention must therefore be paid to the following critical points:

- Randomization: this step shifts the true key to location $0 \leq i < 64$ which must be unknown to the exterior.
- Result copy (loop to j): here again, the two values (0 or 8), which would enable the attacker, if revealed, to know which DES algorithm uses the true key, are involved.

3.4 CM extensions and various aspects

- If we take a closer look at function PP, it is easy to see that it is not necessary to use the same value for the eight sub-keys, as was done previously, to mask the key. Taking sub-key i, it is merely necessary for the 64 possible values to appear. It is not necessary for the order of the 64 values to be the same for a given sub-key as for another sub-key! The only requirement is that the value 0 of the sub-key (for which the true sub-key is used) appears at the same time for the eight sub-keys, so that one of the 64 calculations gives the correct result. We can thus imagine a derivation of the following type:

$K_{00} = K \oplus PP(\ 000000 \mid 000000 \mid \ldots \mid 000000 \mid 000000\ )$
$K_{01} = K \oplus PP(\ 011000 \mid 001101 \mid \ldots \mid 001001 \mid 111100\ )$
$K_{02} = K \oplus PP(\ 010101 \mid 001111 \mid \ldots \mid 001011 \mid 010000\ )$
$K_{03} = K \oplus PP(\ 110011 \mid 100010 \mid \ldots \mid 000011 \mid 010010\ )$

$K_{61} = K \oplus PP(\ 101011 \mid 011100 \mid \ldots \mid 110001 \mid 101000\ )$
$K_{62} = K \oplus PP(\ 100111 \mid 101010 \mid \ldots \mid 000110 \mid 010111\ )$
$K_{63} = K \oplus PP(\ 001110 \mid 010111 \mid \ldots \mid 011100 \mid 110001\ )$

This merely requires a function which executes a random permutation of the values [1,63].

It should be noted that the fact that the mask (000000 | ... | 000000) always appears in the initial position does not represent a problem, as the derivative keys are then permutated randomly before being used. If we consider that we have a function PP2(i,val) which replaces the 6 bits of value val in the correct position for it to correspond to sub-key i, we then obtain the following pseudo-code C:

```
void
DES_encrypt_DPA(unsigned char in[8],
                unsigned char cle[8],
          unsigned char out[8] )
{
   int i,j;
   unsigned char M1[8], M2[16], K[64][9];

   memcopy(K[0],cle,8);
   K[0][8] = 0;

   for(i=0;i<64;i++)
   {
      memcopy(K[i],cle,8);
   }

   for(i=0; i<8; i++)
   {
      unsigned char Perm63[63];

      randomize_1_63(Perm63);
      for(j=1; j<64; j++)
      {
        K[j] = K[j] XOR PP2(i,Perm[j]);
      }
   }

   randomize_0_63(K);

   for(i=0; i<64; i++)
   {
      memcopy(M1, in, 8);
      DES_encrypt_non_DPA(M1,K[i]);

      for(j=0;j<8;j++)
      {
         M2[K[i][8] + j] = M1[j];
      }
   }
```

```
    memcopy(out, M2, 8);
}
```

- Randomization of the 64 derivative keys can be performed using the following conventional method (cf. Crypto'2002 or Akkar/Goubin article on HODPA attacks on the DES algorithm), which involves scanning the keys from 0 to 63 with index i, and exchanging the key with index i with a key with an index selected randomly between 0 and 63:

```
void
randomize(unsigned char table[64])
{
   int i, i_temp;
   unsigned char temp;

   for(i=0; i<64; i++)
   {
      table[i] = i;
   }

   for(i=0; i<64; i++)
   {
      i_temp = random() % 64;
      temp = table[i];
      table[i] = table[i_temp];
      table[i_temp] = temp;
   }
}
```

3.5 Other DES rounds

We have seen how to protect the first DES round against DPA attack. Where the DES is more vulnerable on the 16th round in the protocol used, a similar method can naturally be envisaged. Only function PP will change, and correspond to the key-scheduling for the 16th round! It is then possible to use 64 key masks which protect both the first and last rounds. The following 64 key mask keys possess this property:

0000000000000000 8444054405410000 410900B100033003
C54D05F505423003
0093420342004141 84D7474747414141 419A42B242037142
C5DE47F647427142
0021000000950C9C 8465054405D40C9C 412800B100963C9F
C56C05F505D73C9F
00B2420342954DDD 84F6474747D44DDD 41BB42B242967DDE
C5FF47F647D77DDE
2200300918288100 A644354D1D698100 630930B8182BB103
E74D35FC1D6AB103
2293720A5A28C041 A6D7774E5F69C041 639A72BB5A2BF042
E7DE77FF5F6AF042
2221300918BD8D9C A665354D1DFC8D9C 632830B818BEBD9F
E76C35FC1DFFBD9F
22B2720A5ABDCCDD A6F6774E5FFCCCDD 63BB72BB5ABEFCDE
E7FF77FF5FFFFCDE
18008800A0000321 9C448D44A5410321 590988B1A0033322
DD4D8DF5A5423322
1893CA03E2004260 9CD7CF47E7414260 599ACAB2E2037263
DDDECFF6E7427263
18218800A0950FBD 9C658D44A5D40FBD 592888B1A0963FBE
DD6C8DF5A5D73FBE
18B2CA03E2954EFC 9CF6CF47E7D44EFC 59BBCAB2E2967EFF
DDFFCFF6E7D77EFF
3A00B809B8288221 BE44BD4DBD698221 7B09B8B8B82BB222
FF4DBDFCBD6AB222
3A93FA0AFA28C360 BED7FF4EFF69C360 7B9AFABBFA2BF363
FFDEFFFFFF6AF363
3A21B809B8BD8EBD BE65BD4DBDFC8EBD 7B28B8B8B8BEBEBE
FF6CBDFCBDFFBEBE
3AB2FA0AFABDCFFC BEF6FF4EFFFCCFFC 7BBBFABBFABEFFFF
FFFFFFFFFFFFFFFF

Obviously, this countermeasure (or at least the critical parts) must be implemented in the assembler mode, so as to avoid introducing vulnerability due to unfamiliarity with the methods used by the compiler.

2. Application to the AES algorithm

Obviously, this method can apply in a similar way to the AES algorithm. This is even simpler to explain, as the first sub-key used – which is frequently the target – comprises the key with no other conversion! Another practical difference stems from the fact that the key occurs 8 bits by 8 bits. Thus, in the case of an AES algorithm with key and 128-bit message, we obtain key derivation and a

pseudo-code C as follows:

$K_{00} = K \oplus (00000000 \mid 00000000 \mid ... \mid 00000000 \mid 00000000)$
$K_{01} = K \oplus (00000001 \mid 00000001 \mid ... \mid 00000001 \mid 00000001)$
$K_{02} = K \oplus (00000010 \mid 00000010 \mid ... \mid 00000010 \mid 00000010)$
$K_{03} = K \oplus (00000011 \mid 00000011 \mid ... \mid 00000011 \mid 00000011)$
.
.
.
$K_{61} = K \oplus (11111101 \mid 11111101 \mid ... \mid 11111101 \mid 11111101)$
$K_{62} = K \oplus (11111110 \mid 11111110 \mid ... \mid 11111110 \mid 11111110)$
$K_{63} = K \oplus (11111111 \mid 11111111 \mid ... \mid 11111111 \mid 11111111)$

```
void
AES_encrypt_DPA( unsigned char in[16],
                                 unsigned char cle[16],
                 unsigned char out[16] )
{
   int i;
   unsigned char M1[16], M2[32], K[256][17];

   memcopy(K[0],cle,16);
   K[0][16] = 0;

   for(i=1; i<256; i++)
   {
      memcopy(K[i], cle XOR (i | ... | i), 16);
      K[i][8] = 16;
   }

   randomize_0_255(K);

   for(i=0; i<256; i++)
   {
      memcopy(M1, in, 16);
      AES_encrypt_non_DPA(M1,K[i]);

      for(j=0;j<16;j++)
      {
         M2[K[i][16] + j] = M1[j];
      }
   }

   memcopy(out, M2, 16);
}
```

The only real difference is that key-scheduling for the AES algorithm is not linear, in contrast to the DES, except for the first

sub-key. Thus, if we wish to protect the last round by this method, a method similar to the DES cannot be considered. It is then necessary to store the set of 256 keys specific to a given key, instead of the key derivation plan.

5

3. Conclusion

We thus see that it is possible, by execution of 64 DES (or 256 AES) algorithms and a number of ancillary calculations, to protect a cryptographic algorithm (DES or AES, for example) against DPA attack by means of a rapid although unprotected brick. Sixty-four DES or 256 AES may appear long, nevertheless in practice these hardware operations take a practically negligible amount of time.

10

15

CLAIMS

1. Process for securing an electronic device incorporating a hardware component capable of autonomous implementation of calculation process f using key K, characterised by the fact that it involves calculating at least two new keys K'^i such that at least one of said new keys is identical to key K, and at least one of said new keys is different from key K, and executing said calculation process f successively with each of said calculated keys K'^i using said hardware component.

2. Process according to claim 1, characterised in that it involves executing said calculation process with said keys K'^i in a random order.

3. Process according to claim 1 or 2, characterised in that key K is sub-divided into sub-keys K_1, ..., K_n, and that there exists at least one i such that key K'^i is different from K for at least one sub-key K'^i_j.

4. Process according to one of claims 1 to 3, characterised in that key K is sub-divided into sub-keys K_1, ..., K_n, and that the procedure involves calculating $l=\alpha$ m new keys K'^1, ..., K'^l, where m represents the number of possible values for one of sub-keys K'^i_j of K'^i, in such a way that for a given j ($0<j<n+1$), sub-keys K'^i_j ($0<i<l+1$) take all the possible values, including the value of sub-key Kj of K.

5. Process according to claim 4, characterised in that sub-keys K'^i_j ($0<i<l+1$) take all the possible values α times.

6. Electronic device incorporating means to store a calculation process, means to execute said process and a hardware component capable of autonomous implementation of a calculation process using

key K, characterised in that it incorporates a software module associated with the hardware component, capable of calculating at least two new keys K^i, such that at least one of new said keys is identical to key K, and one of said new keys is different from key K, and in that the software module is associated with the hardware component in such a way as to be able to transmit in succession to said hardware component, the new keys calculated to implement said calculation process with each of said new keys K^i.

7. Electronic device according to claim 6, characterised in that said software module transmits in succession the new keys calculated in a random order.

8. Computer program incorporating program code instructions for execution of the steps of the process according to one of claims 1 to 5, when said program is executed in an electronic device.

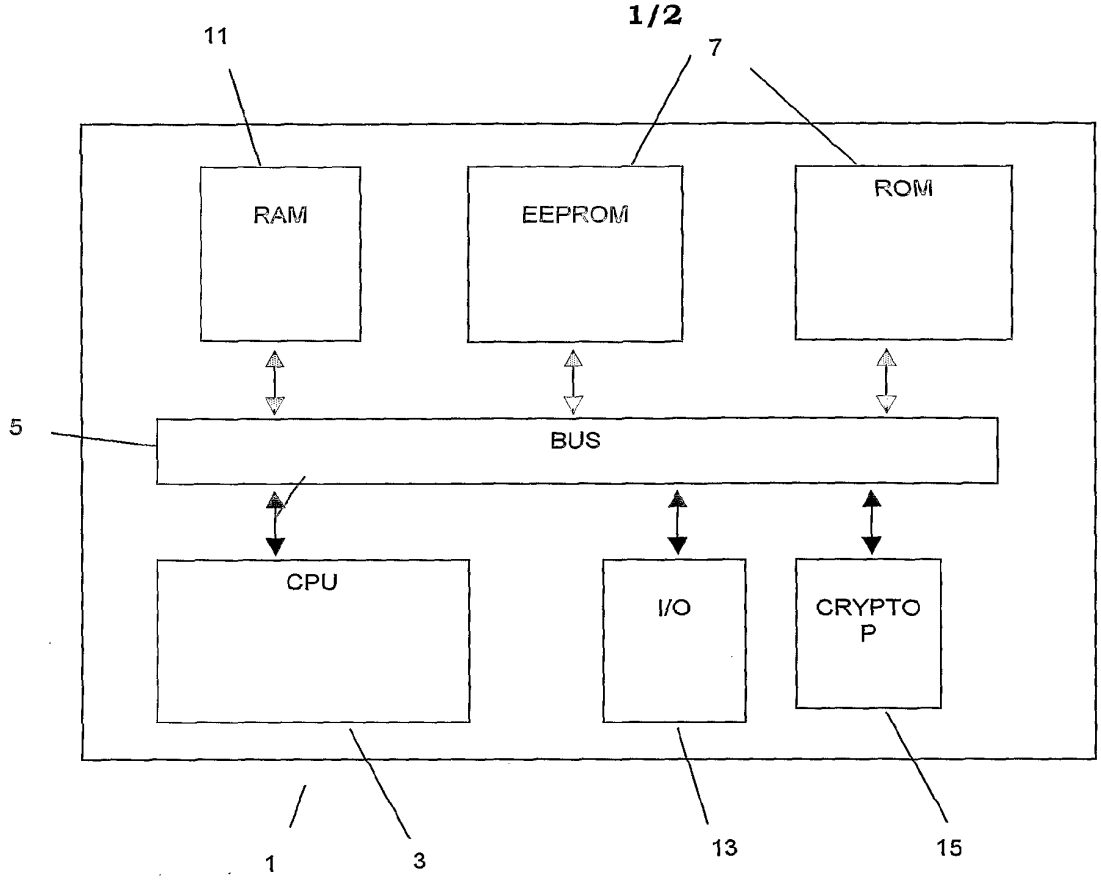

11
7
RAM
EEPROM
ROM
5
BUS
CPU
I/O
CRYPTO P
1
3
13
15

FIG. 1

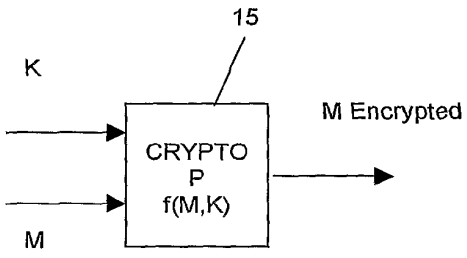

15
K
M Encrypted
CRYPTO P f(M,K)
M

FIG. 2

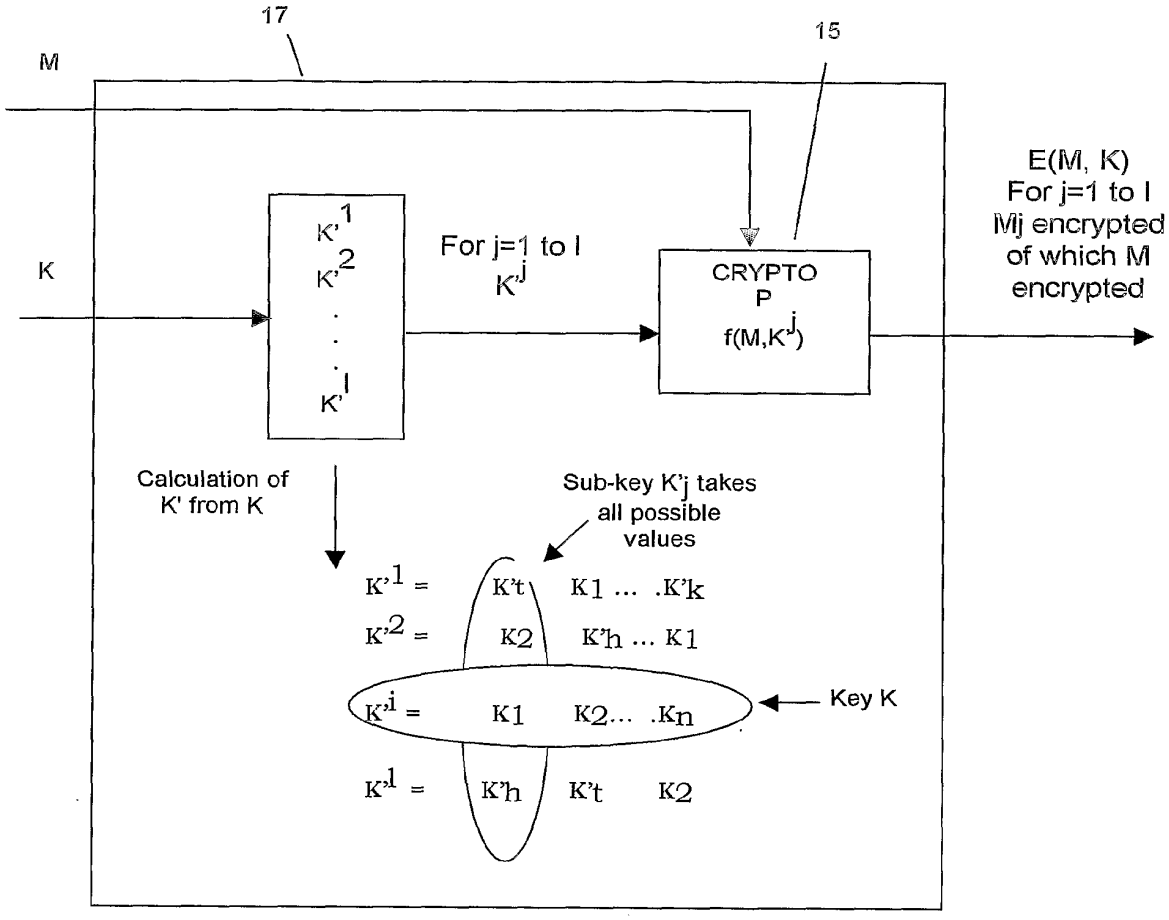

17
15
M
K
K'1
K'2
K'l
For j=1 to l
K'j
CRYPTO
P
f(M,K'j)
E(M, K)
For j=1 to l
Mj encrypted
of which M
encrypted
Calculation of
K' from K
Sub-key K'j takes
all possible
values
K'1 = K't K1 ... .K'k
K'2 = K2 K'h ... K1
K'i = K1 K2... .Kn
K'l = K'h K't K2
Key K

FIG. 3

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/IB2004/000738

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/31422 A (VON WILLICH MANFRED) 3 May 2001 (2001-05-03) page 3, line 11 - line 37 page 5, line 26 - page 6, line 37 page 8, line 27 - page 9, line 20 page 11, line 17 - line 29 page 12, line 7 - line 14 claims 1,3 figures 8,9 ----- -/--	1-8

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2004	05/08/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bichler, M

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

In ɔnal Application No
PCT/IB2004/000738

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHARI S ET AL: "TOWARDS SOUND APPROACHES TO COUNTERACT POWER-ANALYSIS ATTACKS" ADVANCES IN CRYPTOLOGY. CRYPTO '99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, CA, AUG. 15 - 19, 1999. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1666, BERLIN: SPRINGER, DE, 1999, pages 398-412, XP000911819 ISBN: 3-540-66347-9 abstract page 402 - page 404	1-8
A	EP 1 109 350 A (SAGEM) 20 June 2001 (2001-06-20) page 3, paragraph 24 - page 4, paragraph 30	1-8

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB2004/000738

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0131422 A	03-05-2001	AU 773982 B2	10-06-2004
		AU 2301401 A	08-05-2001
		CA 2388971 A1	03-05-2001
		CN 1413398 T	23-04-2003
		EA 3874 B1	30-10-2003
		EP 1226681 A2	31-07-2002
		JP 2003513490 T	08-04-2003
		WO 0131422 A2	03-05-2001
		ZA 200202798 A	10-07-2003
EP 1109350 A	20-06-2001	FR 2802741 A1	22-06-2001
		EP 1109350 A1	20-06-2001

Form PCT/ISA/210 (patent family annex) (January 2004)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 March 2005 (10.03.2005)

PCT

(10) International Publication Number
WO 2005/022288 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/IL2004/000628

(22) International Filing Date: 13 July 2004 (13.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/649,169 27 August 2003 (27.08.2003) US

(71) Applicant *(for all designated States except US)*: **ALADDIN KNOWLEDGE SYSTEMS LTD.** [IL/IL]; 15 Beit Oved St., 61110 Tel Aviv (IL).

(72) Inventors: **AGAM, Leedor**; 3 Simtat Harakefet St., 56905 Savion (IL). **MARGALIT, Yanki**; 6 Carmeli St., 52223 Ramat Gan (IL). **MARGALIT, Dany**; 10 Kiriati St., Ramat Chen (IL).

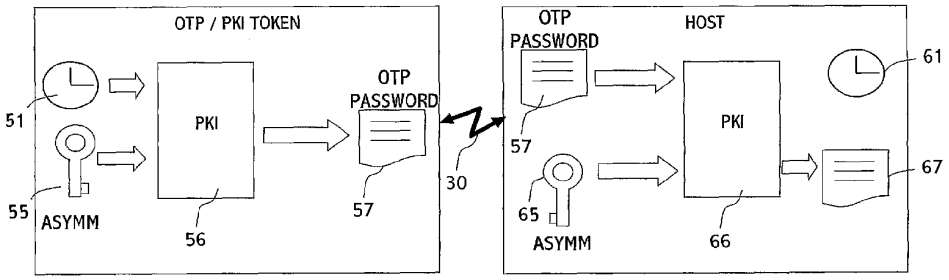
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

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.

(54) Title: SECURITY TOKEN



(57) Abstract: A security token, a security system and a method for authenticating a client are disclosed. The security token comprising: one-time password mechanism, for rendering one-time password functionality; public-key mechanism, for rendering public-key functionality with respect to the one-time password functionality; and wired communication means with a host, for connecting the security token to the host and for providing the security token the power supply required for operating at least the public-key mechanism; whereby enabling rendering one-time password functionality and/or public-key functionality by the security token. The method for authenticating a client by a host system, comprising: At the client side: (a) generating a first one-time value; (b) performing public-key functionality with respect to the one-time value; (c) providing the value to the host system. At the host system side: (d) performing public-key functionality which correspond to the public key functionality performed at step (b) with the provided value; (e) generating a second one-time value in substantially the same manner as the first one-time value is generated; authenticating the client by the correspondence of the second value to the first value; whereby obtaining a better security level of authenticating the client.

WO 2005/022288 A2

SECURITY TOKEN

Field of the Invention

The present invention relates to the field of security tokens. More particularly, the invention relates to a security token that enables both OTP and PKI functionality, and the combination thereof.

Background of the Invention

OTP, the acronym of One-Time Password, refers in the prior art to a password that is valid only for a single session, i.e. differs each time it is requested or generated. Using OTP methods, passwords that have been stolen by eavesdropping on a network are actually useless. Therefore, OTP are commonly used in security systems in which a user has to be authenticated to a server.

For example, the RSA SecurID is a mobile device which generates a pseudo-random string per minute, and displays it on a built-in display. Whenever a user is asked to enter a password into a system, he types the password which is presented on the display of the RSA SecurID security token.

The common way OTP tokens operate is as follows: the one-time password is displayed on a built-in display on the token. The user has to provide to the host his PIN and the password which is displayed at that moment on the OTP token. This is usually carried out by typing the data on a keyboard connected to the host. Another problem regarding OTP tokens is that they use their own power source, i.e. a

battery, which involves some inconvenience since they should be replaced from time to time.

Since in the current OTP tokens the same key is used in both the token and the server ("symmetric key"), using the same key for more than one application is risky.

Another developing technology in the security token field is the PKI (Public Key Infrastructure) token technology, e.g. the RSA and ECC. The PKI technology is based on asymmetric keys, contrary to how the OTP is implemented, i.e. based on symmetric keys. The PKI technology enables the use of a token not only as an authentication device, but also as a security engine , i.e. a device which performs a variety of security-related functionality, such as encryption, decryption, digital signature, and so forth.

From the practical aspect, PKI requires much more processing power than OTP. The problem becomes extremely acute when dealing with 1024 bit keys and higher, e.g. 2048 bit keys. Therefore OTP tokens can be easily implemented as mobile devices, contrary to PKI tokens, which are typically plugged into another device, through which they are connected to an xternal power source.

From the application aspect, applications that use OTP tokens are very limited, and consequently OTP tokens are used mainly for remote access, network logon, etc. The PKI token technology may be used for a variety of implementations, e.g., a variety of authentication schemes, rendering digital signatures, encryption and decryption, secure e-mail, and so forth.

An organization that already uses the OTP tokens for its purposes and wishes to expand the use by adding PKI tokens, has to deal with two major problems: From the server point of view there are logistical problems like holding two separate data bases. From the user point of view there is a great deal of inconvenience, since the user has to hold at least two tokens, an OTP token and a PKI token.

It is therefore an object of the present invention to provide a security token, which supports both the OTP token technology and the PKI technology, and the combination thereof, thereby gaining the functionality of both, the OTP functionality and the PKI functionality, and the combination thereof.

It is another object of the present invention to provide a security token, which achieves a better level of security than that provided by each technology separately.

It is a further object of the present invention to provide a security token which is more user friendly than an OTP token and a PKI token.

It is a still further object of the present invention to provide a security system, which enables the use of the same database of keys for both the OTP and the PKI functionality.

Other objects and advantages of the invention will become apparent as the description proceeds.

In this matter, it should be mentioned that although behind the SecurID stands the RSA Company, the enterprise

that invented the famous public-key algorithm RSA , the RSA Company doesn't manufacture any security token which uses public keys for creating OTP values, nor do they manufacture a device that combines the PKI technology with OTP technology in an offline mode, i.e. display an OTP value on an LCD, when not connected to the PC.

Summary of the Invention

In one aspect, the present invention is directed to a security token, comprising: one-time password mechanism, for rendering one-time password functionality; public-key mechanism, for rendering public-key functionality with respect to the one-time password functionality; and wired communication means with a host, for connecting the security token to the host and for providing the security token the power supply required for operating at least the public-key mechanism; whereby enabling rendering one-time password functionality and/or public-key functionality by the security token.

In a second aspect, the present invention is directed to an OTP security token, for securely providing a one-time (e.g. the real-time, the value of a counter, a list of random numbers, etc.) value to a host system, the OTP security token comprising: means for generating said one-time value; a PKI mechanism for performing public-key functionality with respect to said one-time value; and communication means with said host, for providing said encrypted one-time value to said host.

In a third aspect, the present invention is directed to a security system comprising: one or more security tokens, each of which comprising: one-time password

mechanism, for rendering one-time password functionality; public-key mechanism, for rendering public-key functionality with respect to the one-time password functionality; and wired communication means with a host, for connecting the security token to the host and for providing the security token the power supply required for operating at least the public-key mechanism. The system comprises a host system, comprising: a one-time password mechanism, corresponding to the one-time password mechanism of the security tokens, for rendering one-time password functionality; a public-key mechanism, corresponding to the public-key mechanism of the security tokens, for rendering public-key functionality; communication means, corresponding to the communication means of the security tokens, for communicating with the security tokens and for providing to a token the power supply required for operating at least the public-key mechanism of the security token.

In the fourth aspect, the present invention is directed to a method for authenticating a client by a host system, comprising: At the client side: (a) generating a first one-time value; (b) performing public-key functionality with respect to the one-time value; (c) providing the value to the host system. At the host system side: (d) performing public-key functionality which correspond to the public key functionality performed at step (b) with the provided value; (e) generating a second one-time value in substantially the same manner as the first one-time value is generated; authenticating the client by the correspondence of the second value to the first value; whereby obtaining a better security level of authenticating the client.

Brief Description of the Drawings

The present invention may be better understood in conjunction with the following figures:

Fig. 1 schematically illustrates an authentication process carried out by an OTP token, according to the prior art.

Fig. 2 schematically illustrates an authentication process carried out by an OTP token, according to a preferred embodiment of the invention.

Fig. 3 schematically illustrates a security system, according to one embodiment of the invention.

Fig. 4 visually illustrates a security token, according to a preferred embodiment of the invention.

Detailed Description of Preferred Embodiments

Fig. 1 schematically illustrates an authentication process carried out by an OTP token, according to the prior art.

At the token side: The one-time value 51 (illustrated by a real time clock) and the symmetric key 52 are used by a process 53 to generate a one-time password 54. The one-time password 54 is displayed on a display embedded within the token. The one-time password is provided to the host by typing its content on input means, e.g. keypad, connected to the host.

At the host side: The one-time value 61 (which should correspond to the one-time value 51) and the symmetric key

62 (which should be the same as key 52) are used by a process 63 (which should be the same as the process 53) to generate a one-time password 64. If the generated one-time password 64 corresponds to the one-time password 54 which has been generated by the token, then the authentication is considered as positive.

Fig. 2 schematically illustrates an authentication process carried out by an OTP token, according to a preferred embodiment of the invention.

At the token side: The one-time value 51 (illustrated by a real time clock) is encrypted by the PKI module 56 with the asymmetric key 55, generating the encrypted one-time value 57, which is provided to the host.

At the host side: The one-time value 57 which has been received from the token is decrypted by the asymmetric key 65 (which corresponds to the asymmetric key 55) by the PKI module 66, resulting with a one-time password 67. If the one-time value 67 corresponds to the expected value, then the authentication is considered as positive.

Those skilled in the art will appreciate that in addition to the authenticating method described herein there may be other authentication methods which combines OTP and PKI. The method described herein is only an example of the variety of possibilities opened by combining the OTP technology with the PKI technology. For example, instead of encrypting and decrypting the one-time value as described in Fig. 2, a digital signature (or digital certificate) can be added to the one-time value 57, even without using encryption. Thus, module 56 performs some PKI-related activity in conjunction with the security of the one-time

value, and module 66 performs some PKI-related activity which corresponds to the PKI-related activity of module 56.

It should be noted that the provided value doesn't necessarily equal the expected value, but should correspond to the expected value. For example, if the one-time value is the real time, and if the difference between the value 57 and the value 67 is less than, e.g., one minute, then the authentication can be considered as positive. It should also be noted that the clock of the token may not be tuned exactly to the clock of the host, and therefore a slight difference between the time of the host and the time provided by the token should be taken into consideration.

Another one-time mechanism known in the art is the counter. Each time a password is provided, the value of the counter is increased by one or another predetermined portion, not necessarily linear. Of course, this other one-time mechanism can be implemented for this purpose, e.g. a list of random numbers.

A counter mechanism may be implemented by a button installed on the token. Each time the user clicks on the button, the counter is increased, and a new one-time value is generated and displayed on the display. Since the user can push the button unintentionally, the value of the counter of the token and the value of the counter on the host may not be equal, but just correspond , i.e. they have a difference of not more that, e.g., 10. Thus, the host checks not only the current value of the counter, but also the next 10 values to be generated.

According to a preferred embodiment of the invention, the key 55 is the public key of the host, while the key 65 is the corresponding private key. According to another preferred embodiment of the invention, key 55 is the private key of the token, while key 65 is the corresponding public key.

It is obvious that more sophisticated encryption / decryption schemes may be used. For example, encrypting the one-time value with a symmetric key, and then encrypting the result with a private key.

Fig. 3 schematically illustrates a security system, according to one embodiment of the invention. An OTP / PKI token 10 (the client) is connected to a host system 20 (the server) by wired communication 30.

The token 10 comprises:

- A controlling module 11, for performing the PKI and OTP functionality, and for controlling / managing the operation of the token. The controlling module can be embodied as a CPU, memory and appropriate software.
- One or more keys 12, for the OTP / PKI functionality.
- A one time value generator 13, e.g. a real time clock, a counter or another element that changes each time it is accessed (e.g. a list of random numbers), for generating a one-time value.
- Wired communication interface 14, for communicating with the host 20.
- A display 15, for displaying one-time passwords.
- A power supply 16, e.g. a battery, for providing the power supply for operating the token.

According to a preferred embodiment of the invention, at least the keys 12 may be stored within a smartcard 17, which provides a relatively high security level. Typically, smartcards are also a processing unit coupled with memory, and therefore they may perform other functionality, e.g. the functionality of the controlling module 11, the PKI, and so forth.

The host 20 comprises:

- A controlling module 21, for performing the PKI / OTP functionality. The functionality of the controlling module 21 can be carried out as a part of the operating system of the host 20, by an application executed on the host 20, and so forth.
- A database 22, for storing the keys, user ID of the authorized users, and so forth, in relevance with the OTP / PKI.
- A one time value generator 23, e.g. a real time clock, a counter, a random list or another element that provides a different value each time it is accessed, corresponding to the one-time value generator 13 of the token 10.
- Wired communication interface 24, corresponding to the wired communication 14 of the token 10.

Fig. 4 visually illustrates a security token, according to a preferred embodiment of the invention. The display 19 of the token 10 displays the one-time password, like in the prior art. The traditional way of providing the one-time password is by typing the displayed value onto the input means of the host 20, e.g. a keypad. According to a preferred embodiment of the present invention, instead of typing the password, the user inserts the connector 18 (e.g. a USB plug) to the corresponding socket of the host,

and the token interacts with the host via the communication channel 30 (whether wired or wireless), for providing the one-time password.

Those skilled in the art will appreciate that the invention can be embodied by other forms and ways, without losing the scope of the invention. The embodiments described herein should be considered as illustrative and not restrictive.

CLAIMS

1. A security token, comprising:
   - one-time password mechanism, for rendering one-time password functionality;
   - public-key mechanism, for rendering public-key functionality with respect to said one-time password functionality; and
   - wired communication means with a host, for connecting said security token to said host and for providing to said security token the power supply required for operating at least said public-key mechanism;

   whereby achieving better security performance by said security token.

2. A security token according to claim 1, further comprising a display, for displaying said one-time password and/or any other information.

3. A security token according to claim 1, further comprising a smartcard chip, for secure storage of keys and for rendering security-related functionality.

4. A security token according to claim 1, wherein said one-time password mechanism comprising means for generating a one-time value, said means selected from a group comprising: a real-time clock, and a counter.

5. A security token according to claim 1, wherein said communication means is selected from a group comprising: a display for displaying the password and thereafter manually providing the displayed value to a host, wired

communication means with a host, wireless communication means with a host.

6. A security token according to claim 5, wherein said wired communication means further comprising provision of power supply, for providing power supply to said security token.

7. A security token according to claim 5, further comprising chargeable power source, to be charged by the power supplied via said communication means, for providing the power for operating said security token while not connected to said host.

8. An OTP security token, for securely providing a one-time value to a host system, said OTP security token comprising:
   - means for generating said one-time value;
   - a PKI mechanism, for performing public-key functionality with respect to said one-time value; and
   - communication means with said host, for providing said encrypted one-time value to said host.

9. An OTP security token according to claim 8, wherein said public-key functionality with respect to said one-time value is selected from a group comprising: encrypting said one-time value by said public-key functionality, and digitally signing said one-time password.

10. An OTP security token according to claim 8, further comprising a display, for displaying the encrypted one-time value and other information.

11. An OTP security token according to claim 8, further comprising a smartcard chip, for rendering security-related functionality.

12. An OTP security token according to claim 8, wherein said one-time value is selected from a group comprising: the real-time, the value of a counter, and a group of random numbers.

13. An OTP security token according to claim 8, wherein said communication means is selected from a group comprising: a display for displaying the password and thereafter manually providing the displayed value to said host, wired communication means with said host, wireless communication means with said host.

14. An OTP security token according to claim 11, wherein said wired communication means further comprising provision of power supply, for providing power supply to said security token.

15. An OTP security token according to claim 8, further comprising chargeable power source, to be charged by the power supplied by said communication means, for providing the power for operating said security token while not connected to said host.

16. A security system comprising:

- at least one security token comprising: one-time password mechanism, for rendering one-time password functionality; public-key mechanism, for rendering public-key functionality with respect to said one-time password; and wired communication means with a host, for connecting said security token to said host and

for providing to said security token the power supply required for operating at least said public-key mechanism;

- a host system, comprising: a one-time password mechanism, corresponding to the one-time password mechanism of said at least one security token, for rendering one-time password functionality; a public-key mechanism, corresponding to the public-key mechanism of said at least one security token, for rendering public-key functionality; communication means, corresponding to the communication means of said at least one security token, for communicating with said at least one security token and for providing to said token the power supply required for operating at least the public-key mechanism of said security token.

17. A system according to claim 16, wherein said communication means is selected from a group comprising: a display embedded within each of said at least one security token, for displaying the password and thereafter manually providing the displayed value to said host, wired communication means through which said at least one security token can be provided with the power supply required for performing public-key operations.

18. A system according to claim 16, wherein each of said at least one security token further comprising chargeable power source, to be charged via the power supply provided by said communication means, for providing the power for operating said at least one processor while not connected to said host, thereby

enabling to operate said security token without external power supply.

19. A method for authenticating a client by a host system, said method comprising:

at said client side:

(a) generating a first one-time value;

(b) performing public-key functionality with respect to said one-time value;

(c) providing said value to said host system;

at said host system side:

(d) performing public-key functionality which correspond to the public key functionality performed at step (b) with the provided value;

(e) generating a second one-time value in substantially the same manner as said first one-time value is generated;

authenticating said client by the correspondence of said second value to said first value;

whereby obtaining a better security level of authenticating said client.

20. A method according to claim 19, wherein said public-key functionality with respect to said one-time value is selected from a group comprising: encrypting said one-time value, and digitally signing said one-time value.

21. A method according to claim 19, wherein said client is a security token.

22. A method according to claim 19, wherein providing the encrypted value to said host is carried out by a member of a group comprising: displaying said encrypted value at the client side and thereafter manually providing the

displayed value to said host, wired communication means between said client and said host, wireless communication means between said client and said host.

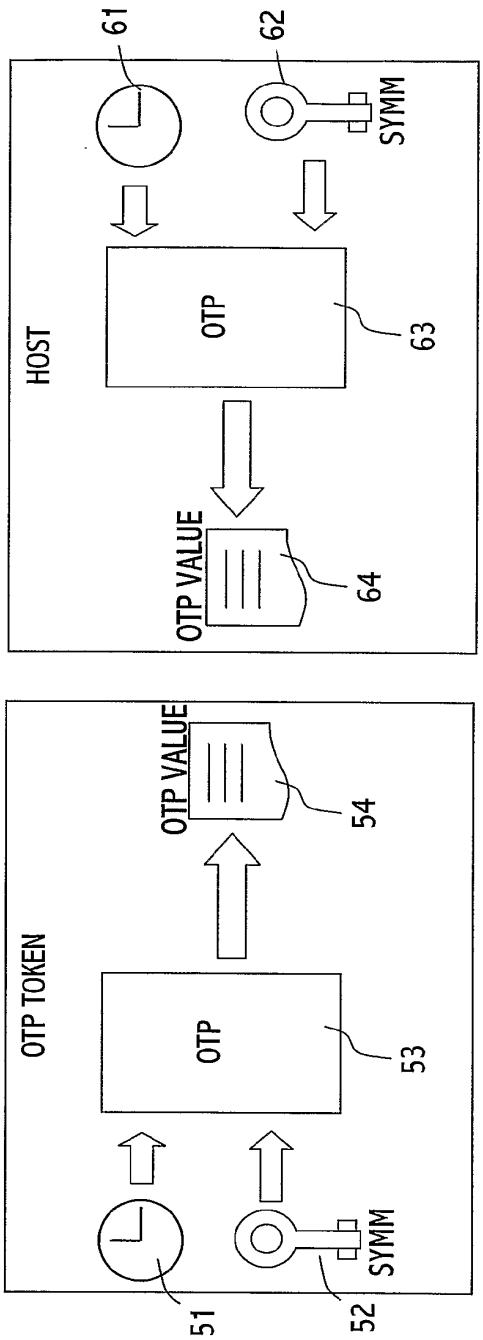


Fig. 1
PRIOR ART

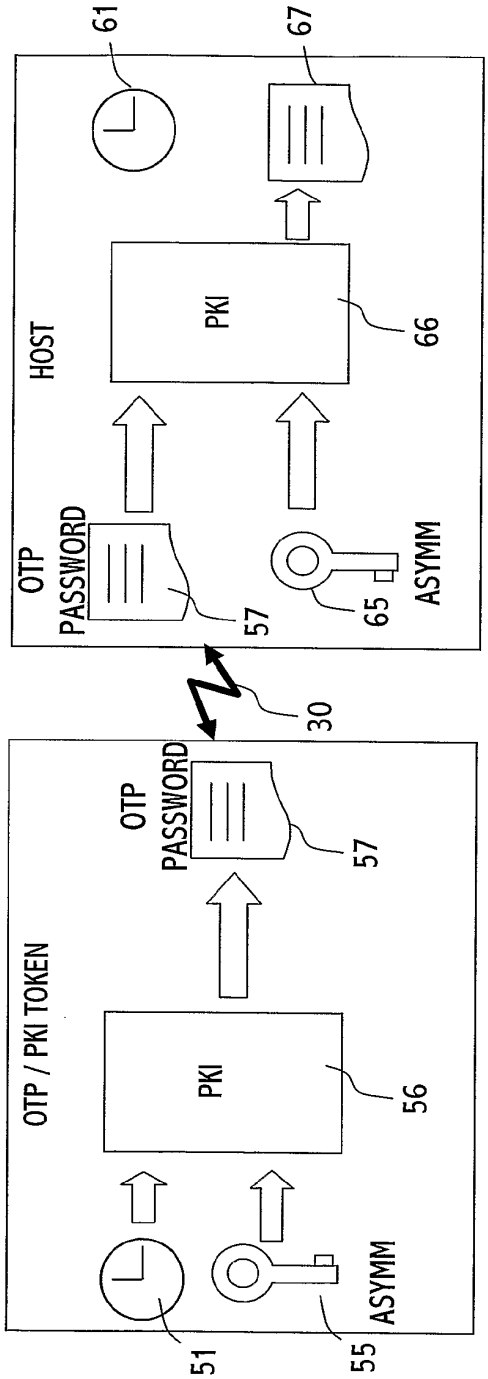

61
67
HOST
PKI
66
OTP
PASSWORD
57
65
ASYMM
30
OTP / PKI TOKEN
OTP
PASSWORD
57
PKI
56
51
55
ASYMM

Fig. 2

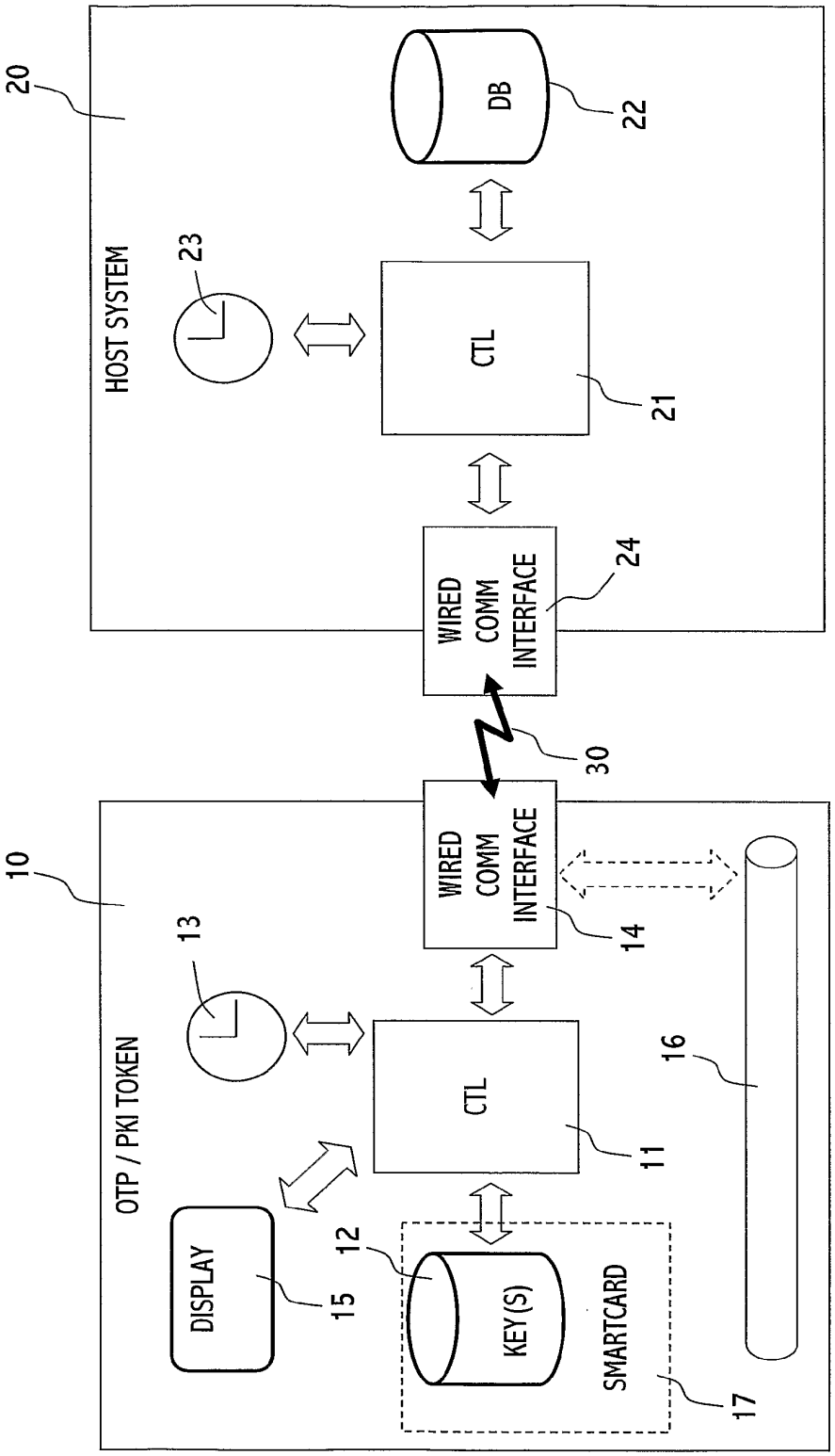

20
HOST SYSTEM
DB
22
23
CTL
21
WIRED COMM INTERFACE
24
30
10
OTP / PKI TOKEN
13
WIRED COMM INTERFACE
14
CTL
11
16
DISPLAY
15
12
KEY(S)
SMARTCARD
17

Fig. 3

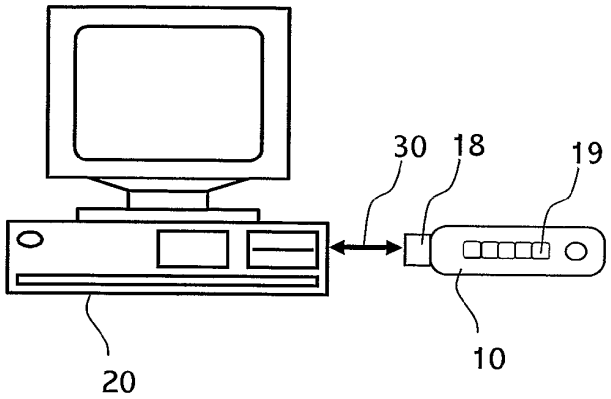


Fig. 4

Electronic Acknowledgement Receipt

EFS ID:	2039912
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	02-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	13:08:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO200188693.pdf	862354 3c06d448df025a2dccbf8758ca621adc670dc044	no	22
Warnings:					

Information:					
2	Foreign Reference	WO200196990.pdf	1414674 db4d2fcf7829ea88a85adee5e009b820e560160f	no	33
Warnings:					
Information:					
3	Foreign Reference	WO2003014887.pdf	908231 488a02d43b84f633db781736ed8f2d7fd99a59cd	no	21
Warnings:					
Information:					
4	Foreign Reference	WO2003034189.pdf	820620 6708d7e3b2baaa0e736aa4e1d73cd194e109836e	no	24
Warnings:					
Information:					
5	Foreign Reference	WO2004002058.pdf	1049219 a46647730b96cefa41cb7fc3a838071d9322d69a	no	28
Warnings:					
Information:					
6	Foreign Reference	WO2004081706.pdf	1042944 26531f116a800a63584d17e464487b40fe6efab5	no	22
Warnings:					
Information:					
7	Foreign Reference	WO2004081769.pdf	1009649 145c82a12c2ee06112620f8b94afd6ecdcf55fe9	no	26
Warnings:					
Information:					
8	Foreign Reference	WO2005022288.pdf	741072 1c60e2130086b2fbccbb5dea9fe2c2345118a5a6	no	22
Warnings:					
Information:					
		Total Files Size (in bytes):	7848763		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Electronic Acknowledgement Receipt

EFS ID:	2039943
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical and Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	Finn-C18
Receipt Date:	02-AUG-2007
Filing Date:	18-JUL-2007
Time Stamp:	13:15:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	NPL Documents	NPL-1_ACR38CT.pdf	231033 1ff1a29e05221128e4ff7e09d49830e159c2fc8d	no	4
Warnings:					

Information:					
2	NPL Documents	NPL-2_ACR38DT.pdf	467142 04f15877bcb136314e6f86fa1957aa5d03d4e9e4	no	4
Warnings:					
Information:					
3	NPL Documents	NPL-3__Dallas-DS1490F.pdf	139760 49ece4b3b21ceae8e6f24cbc60b0fffab7c991a2	no	3
Warnings:					
Information:					
4	NPL Documents	NPL-4_DS9490R-DS9490B.pdf	212025 68d7acf55097c16fb0ec3b1ff7a219f52f3bfae2	no	5
Warnings:					
Information:					
5	NPL Documents	NPL-5_Hara-ee-times-FeRAM.pdf	28457 8effcd22af986c5d1a282c2d532a8059433a4a01	no	1
Warnings:					
Information:					
6	NPL Documents	NPL-6__JP-Matsushita-Mercury-New.pdf	44980 4f3c90ab3aa1c2d82755b34982bacbe7d5317d63	no	2
Warnings:					
Information:					
7	NPL Documents	NPL-7_Oti-6828.pdf	380125 4ebed19da24a41516d4674fa402a3e84ecfbff75	no	7
Warnings:					
Information:					
8	NPL Documents	NPL-8__Panasonic-palm-info-cente.pdf	87632 ab859d50449fb9b8adb02cdf369345610abf6cce	no	3
Warnings:					
Information:					
9	NPL Documents	NPL-9_Panasonic-contactless-JCNN_htm.pdf	36896 6e3d3ab58ed654c2e0755fd8ba5090915059ad1c	no	3
Warnings:					
Information:					
10	NPL Documents	NPL-10__Rojas-Panasonic-smart-SD.pdf	104731 25626a0250c34d631fdc024460e65e8125f058f6	no	4
Warnings:					

Information:					
11	NPL Documents	NPL-11_Philips-Delivering-SmartMX_tif.pdf	34270 f6d279451d3d0bb0b80afe4836dbd34dcf87f0d0	no	1
Warnings:					
Information:					
12	NPL Documents	NPL-12_Balaban-SIMS_v_Flash-Cards_tif.pdf	451360 dd3ac39fd1e070eb3361fd6a6fb2a8e4a25fe0fd	no	5
Warnings:					
Information:					
13	NPL Documents	NPL-13_SmartMX-P5CT072.pdf	539555 5faf5bd06d1c8dc316cd477d5c77490bb8ed5d84	no	12
Warnings:					
Information:					
14	NPL Documents	NPL-14__Vodafone-Develops_htm.pdf	36700 3af60fc0b654a53d510f8f48906c168bec29da2c	no	2
Warnings:					
Information:					
15	NPL Documents	NPL-15_Panasonic-Smart-SD-Card_jpg.pdf	41613 5bd4337c3c5023b9a3d025ed595cd7557b79a455	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	2836279	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
11/779,299	07/18/2007		425	Finn-C18	9	3

CONFIRMATION NO. 1938

63397
GERALD E. LINDEN
12925 LAROCHELLE CR.
PALM BEACH GARDENS, FL33410

FILING RECEIPT

Date Mailed: 07/30/2007

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

Applicant(s)

David Finn, Tourmakeady, IRELAND;

Assignment For Published Patent Application

Advanced Microelectronic and Automation Technology Ltd., Tourmakeady, IRELAND

Power of Attorney:
Gerald Linden--30282
Dwight Stauffer--47963

Domestic Priority data as claimed by applicant

This application is a CIP of 11/420,747 05/27/2006
and claims benefit of 60/832,799 07/24/2006
and is a CIP of 11/355,264 02/15/2006
and is a CIP of 10/990,296 11/16/2004 PAT 7,213,766

Foreign Applications

If Required, Foreign Filing License Granted: 07/28/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US11/779,299**

Projected Publication Date: 11/08/2007

Non-Publication Request: No

Early Publication Request: No

** SMALL ENTITY **

Title

Portable Identity Card Reader System For Physical and Logical Access

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

PTO/SB/14 (08-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	Finn-C18
	Application Number	
Title of Invention	Portable Identity Card Reader System For Physical and Logical Access	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	David		Finn	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Tourmakeady, County Mayo	Country Of Residence	IE
Citizenship under 37 CFR 1.41(b)	IE		

Mailing Address of Applicant:

Address 1	Lower Churchfield		
Address 2			
City	Tourmakeady, County Mayo	State/Province	
Postal Code		Country	IE

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	63397		
Email Address	gelpatents@yahoo.com	Add Email	Remove Email

Application Information:

Title of the Invention	Portable Identity Card Reader System For Physical and Logical Access		
Attorney Docket Number	Finn-C18	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

PTO/SB/14 (08-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	Finn-C18
	Application Number	
Title of Invention	Portable Identity Card Reader System For Physical and Logical Access	

Publication Information:
☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not been and will not be the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ US Representative (37 CFR 11.9)
Customer Number	63397		

Domestic Priority Information:

This section allows for the applicant to claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c). Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	11420747	2006-05-27
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	60832799	2006-07-24
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	11355264	2006-02-15
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	10990296	2004-11-16
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)

Additional Domestic Priority Data may be generated within this form by selecting the **Add** button. Add

PTO/SB/14 (08-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	Finn-C18
	Application Number	
Title of Invention	Portable Identity Card Reader System For Physical and Logical Access	

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ◉ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Remove

Assignee 1

If the Assignee is an Organization check here. ☒

Organization Name	Advanced Microelectronic and Automation Technology Ltd.		
Mailing Address Information:			
Address 1	Lower Churchfield		
Address 2			
City	Tourmakeady, County Mayo	**State/Province**	
Country [i]	IE	Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Gerald E. Linden/			Date (YYYY-MM-DD)	2007-07-18
First Name	Gerald	Last Name	Linden	Registration Number	30282

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PORTABLE IDENTITY CARD READER SYSTEM
FOR PHYSICAL AND LOGICAL ACCESS

CROSS-REFERENCE TO RELATED APPLICATIONS

This patent application claims benefit of the following US Provisional and/or non-provisional patent applications, all of which are incorporated by reference in their entirety herein:

This is a continuation-in-part of 11/420,747 filed 27 May 2006 by Finn (hereinafter "C16").

This is a non-provisional filing of 60/832,799 filed 24 July 2006 by Finn (hereinafter "C18").

This is a continuation-in-part of 11/355,264 filed 2/15/2006 by Finn (hereinafter "C11"), which is a continuation-in-part of 10/990,296 filed 11/16/2004 by Ryan et al. (hereinafter "C4", now USP 7,213,766 issued May 8, 2007).

TECHNICAL FIELD OF THE INVENTION

This invention relates to contactless smart card technology and to RFID (radio frequency identification) reader technology.

BACKGROUND OF THE INVENTION

US patents 6,913,196 discloses a dual mode smart card controller (USB and ISO7816) that determines the type of card that is inserted into a slot. If the smart card is a USB smart card, the controller is adapted to pass control of the smart card to an external PC host USB hub circuit. If the smart card is an ISO7816 card, then control is handled by the dual mode controller. In another embodiment, the controller includes an embedded USB hub circuit to permit the controller to directly control both USB and ISO7816 smart cards. Exemplary control sequencing includes monitoring a C4 signal line for a pre-selected time period, or generating an enable signal if a USB smart card is detected. See also USP 7,150,397

US patent publication 2006/0226217 discloses a sleeve for electronic transaction card. A sleeve provides communications between an electronic transaction card and an intelligent electronic device. The intelligent electronic device may be a mobile phone or other device with or without network connectivity. The electronic transaction card may have magnetic

field producing circuitry compatible with magnetic card readers, smartcard circuitry, other point-of-sale interfaces, or any combination thereof.

US patent publication 2005/0269402 discloses a financial transaction system utilizing multi-factor authentication to secure financial transactions. The following is claimed:

1. A portable transaction device comprising: memory to hold information regarding a financial card; a slot to interface with a re-programmable card; and software to generate single use transaction numbers.

2. The portable transaction device of claim 1 further comprising a biometric scanner where the portable transaction device is configured to combine biometric information with one or more additional authentication factors to secure financial transactions.

3. The portable transaction device of claim 1 further comprising a wireless interface to communicate with a secondary wireless device for an additional authentication factor.

US patent application 2006/0213982 discloses a smartcard-enabled BPID Security Device integrates a smartcard reader with a biometric authentication component to provide secured access to electronic systems. The device allows for an individual to insert a smartcard into an aperture in the physical enclosure of the BPID Security Device, allowing the smartcard and the BPID Security Device to electronically communicate with each other. The smartcard-enabled BPID Security Device is based on a custom application specific integrated circuit that incorporates smartcard terminals, such that the BPID Security Device can communicate directly with an inserted smartcard. In an alternative embodiment of the invention, the smartcard-enabled BPID Security Device is based on a commercial off-the-shelf microprocessor, and may communicate with a commercial off-the-shelf microprocessor smartcard receiver using a serial, USB, or other type of communication protocol. The device allows for enrolling a user's credentials onto the smartcard-enabled BPID Security Device. The device also allows for authenticating an individual using the smartcard-enabled BPID Security Device.

US patent application 2006/0230437 discloses a secure and transparent digital credential sharing arrangement which utilizes one or more cryptographic levels of indirection to obfuscate a sharing entity's credentials from those entities authorized to share the credentials. A security policy table is provided which allows the sharing entity to selectively authorize or revoke digital credential sharing among a plurality of entities. Various embodiments of the

invention provide for secure storage and retrieval of digital credentials from security tokens such as smart cards. The secure sharing arrangement may be implemented in hierarchical or non-hierarchical embodiments as desired.)

Glossary & Definitions

Unless otherwise noted, or as may be evident from the context of their usage, any terms, abbreviations, acronyms or scientific symbols and notations used herein are to be given their ordinary meaning in the technical discipline to which the disclosure most nearly pertains. The following terms, abbreviations and acronyms may be used throughout the descriptions presented herein and should generally be given the following meaning unless contradicted or elaborated upon by other descriptions set forth herein. Some of the terms set forth below may be registered trademarks (®).

Energy harvesting Also known as power harvesting, energy scavenging is the process by which energy may be captured and stored. Frequently this term is applied when speaking about small autonomous devices, like those used in sensor networks. A variety of different methods exist for harvesting energy, such as solar power, ocean tides, piezoelectricity, thermoelectricity, and physical motion.

Lanyard A lanyard, also spelled laniard, is a rope or cord often worn around the neck or wrist to carry something. Lanyards have started to appear on consumer electronics devices. With increasing miniaturization, many digital cameras, MP3 players, and USB memory sticks include lanyards, providing easy portability, and insurance against loss or dropping.

Proximity Card Proximity card is a generic name for contactless integrated circuit devices used for security access or payment systems. It can refer to the older 125 KHz devices or the newer 13.56 MHz contactless RFID cards, most commonly known as contactless smartcards. Modern proximity cards are covered by the ISO 14443 (Proximity Card) standard. There is also a related ISO 15693 (Vicinity Card) standard. Proximity cards use an LC circuit. An IC, capacitor, and coil are connected in series. The card reader presents a field that excites the coil and charges the capacitor, which in turn energizes the IC. IC then transmits the card number via the coil to the card reader. The card readers

communicate in Wiegand protocol that consists of a data 0 and a data 1 circuit. The earliest cards were 26 bit. As demand has increased bit size has increased to continue to provide unique numbers. Often, the first several bits can be made identical. These are called facility or site code. The idea is that company "Alice" has a facility code of xn and a card set of 0001 through 1000 and company "Bob" has a facility code of yn and a card set also of 0001 through 1000.

USB CCID USB is short for Universal Serial Bus. CCID is short for Chip/Smart Card Interface Devices. ICCD is short for Integrated Circuit(s) Card Devices). CCID is intended to use one generic device driver for different types of Smart Card readers without the need of each vendor having to supply its own software driver.

Wiegand refer to the following paragraphs regarding the Wiegand effect, Wiegand interface, Wiegand protocol, Wiegand wire.

The **Wiegand effect** is a pulse-generating phenomenon in a special alloy wire that is processed in such a way as to create two distinct magnetic regions in the same homogeneous piece of wire, referred to as a shell and a core. It occurs when such a specially processed wire (a "**Wiegand wire**") is moved past a magnetic field. The two distinct magnetic regions react differently to any applied magnetic field: the shell requires a strong magnetic field to reverse its magnetic polarity, whereas the core will revert under weaker field conditions. The polarity of the wire will very rapidly shift and generate strong, short (~10 μs) electrical pulses without any additional external power being supplied. This is known as the "Barkhausen jump" or "Barkhausen effect". The Barkhausen jump can be detected by a coil wrapped around the material, when the small amount of voltage described above is generated.

The **Wiegand interface** is a defacto wiring standard, which arose from the popularity of Wigand effect RFID card readers in the 1980's. A Wiegand-compatible reader is normally connected to a Wiegand-compatible security panel.

The **Wiegand interface** uses two signal lines, termed data0 and data1. To transmit a zero bit, the data0 line is pulsed from 5V to 0V. To transmit a one bit, the data1 line is pulsed.

Wiegand protocol is a name for a system of sending data from a sensor such as a card reader or proximity sensor. It is commonly used to connect a card swipe mechanism to the rest of an electronic entry system. The sensor in such a system is often a Wiegand wire based on the **Wiegand effect** discovered by John R. Wiegand. The **Wiegand protocol** is apparently not formally defined in any one place.

The **Wiegand protocol** consists of three wires, one of which is a common ground, and two data transmission wires, usually called DATA0 and DATA1, but sometimes also labeled Data High and Data Low. When no data is being sent both DATA0 and DATA1 are at the high voltage. When a 0 is sent, the Data Low wire (also called DATA0) is at a low voltage while the Data High wire (also called DATA1) stays at the high voltage. When a 1 is sent, Data High is at the low voltage while Data Low stays at the high voltage. The high and low voltage levels are usually the TTL (transistor-transistor logic) voltage levels. A series of bits are sent, followed by a parity bit or bits. The number of bits sent at once varies according to the device, with 26 bits being common.

Contact Interfaces

As used herein, "contact interfaces" (or “mechanical interface”) refers to mechanical (wired) connections between one device and another, such as via a cable or inserting a module into a socket. The following are examples of contact interfaces and/or devices that typically connect via a contact interface.

Ethernet A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100Base-T (or Fast Ethernet),

supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet supports data rates of 1 gigabit (1,000 megabits) per second.

IEEE 1394 IEEE 1394 (also known as FireWire® and iLINK™) is a high-bandwidth isochronous (real-time) interface for computers, peripherals, and consumer electronics products such as camcorders, VCRs, printers, PCs, TVs, and digital cameras. With IEEE 1394-compatible products and systems, users can transfer video or still images from a camera or camcorder to a printer, PC, or television (TV), with no image degradation.

ISO 7816 ISO7816 defines specification of smart card contact interface IC chip and IC card. The main ISO standard relating to smart cards is ISO7816: "Identification cards: integrated circuit cards with contacts".

SD Short for "Secure Digital". SD is a technology standard for providing portable devices with non-volatile memory/storage and peripheral I/O expansion capability. On some devices this standard is implemented in the form of SD memory expansion cards, used to store digital information like applications, databases, photos, text, audio, video or MP3 music files, and an SD/SDIO expansion slot. The SD standard makes it possible to transfer information between devices that support SD expansion cards (e.g. transfer photos between a digital camera and a PDA by exchanging the SD expansion card), assuming both devices support the file format used for the transferred information (e.g. JPEG image file).

SDIO Short for "Secure Digital Input/Output". SDIO is a part of the SD memory specification. It enables I/O (input/output) expansion for add-ons such as serial, modem, camera or GPS (global positioning system) cards. Whereas SD is only used for storage expansion cards, an SDIO capable expansion slot can also support SD expansion cards, while an SD-capable slot may not support an SDIO expansion card.

SIM Short for "Secure Identity Module" or "Subscriber Identification/Identity Module". A SIM card inscribed with a customer's information and designed to

be inserted into any mobile telephone. Usually SIM card phones work by GSM technology. The SIM card contains a user's GSM mobile account information. SIM cards are portable between GSM devices— the user's mobile subscriber information moves to whatever device houses the SIM.

USB Short for "Universal Serial Bus". USB is a serial bus standard (standardized communications protocol) that enables data exchange between electronic devices. USB supports data transfer rates of up to 12 Mbps (megabits per second). A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, and keyboards. USB also supports plug-and-play installation and "hot plugging". USB is expected to completely replace serial and parallel ports. Hi-Speed USB (USB 2.0) similar to FireWire technology, supports data rates up to 480 Mbps.

Wireless Interfaces

As used herein, "wireless interfaces" refers to ultra-high radio frequency (RF) connections between one device and another, typically over a moderate distance, such as up to 100 meters, and in some cases (such as WiMAX) over long distances such as 50 km. The following are examples of wireless interfaces and/or devices that typically connect via a wireless interface.

Wireless Technology that allows a user to communicate and/or connect to the Internet or mobile phone networks without physical wires. Wi-Fi, Bluetooth®, CDMA and GSM are all examples of wireless technology.

Bluetooth A wireless technology developed by Ericsson, Intel, Nokia and Toshiba that specifies how mobile phones, computers and PDAs interconnect with each other, with computers, and with office or home phones. The technology enables data connections between electronic devices in the 2.4 GHz range at 720 Kbps (kilo bits per second) within a 10 meter range. Bluetooth uses low-power radio frequencies to transfer information wirelessly between similarly equipped devices. A Bluetooth interface typically has a range of up to 10 meters, and is typically intended for private/personal communications such as

connecting a user's mobile phone with his computer, or with a Bluetooth headset. Bluetooth bandwidth is specified at 720 Kbps.

IEEE 802.11 The IEEE standard for wireless Local Area Networks (LANs). It uses three different physical layers, 802.11a, 802.11b and 802.11g.

PAN short for private area network. Using a wireless connection such as Bluetooth, a PAN has a range of only several meters, such as up to 10 meters.

UWB UWB is short for "Ultra Wide Band". UWB is a wireless communications technology that transmits data in short pulses which are spread out over a wide swath of spectrum. Because the technology does not use a single frequency, UWB enjoys several potential advantages over single-frequency transmissions. For one, it can transmit data in large bursts because data is moving on several channels at once. Another advantage is that it can share frequencies, which is used by other applications because it transmits only for extremely short periods, which do not last long enough to cause interference with other signals.

UWB is a signaling technique using very short pulses to achieve very high transfer speeds. UWB it is not limited to wireless communication, UWB can also use mains-wiring, coaxial cable or twisted-pair cables to communicate. In a wireless mode, UWB may be similar in range to Bluetooth (typically up to 10 meters), but with a much greater bandwidth. Theoretically, WAN can achieve transfer speeds of up to 1 Gbit/s, versus only up to 3 Mbps for Bluetooth.

WAN short for wireless area network. Using a WAN connection such as 802.11, a WAN has a range of up to approximately 100 meters.

Wibree Wirebee is a digital radio technology (intended to become an open standard of wireless communications) designed for ultra low power consumption (button cell batteries) within a short range (10 meters / 30 feet) based around low-cost transceiver microchips in each device. Wibree is designed to work side-by-side with and complement Bluetooth. It operates in 2.4 GHz ISM band with physical layer bit rate of 1 Mbps. Main applications include devices such as

wrist watches, wireless keyboards, toys and sports sensors where low power-consumption is a key design requirement. The technology was announced 2006-10-03 by Nokia. Partners that currently license the technology and cooperate in defining the specification are Nordic Semiconductor, Broadcom Corporation, CSR and Epson.

Wi-Fi Short for "Wireless Fidelity". Wireless technology, also known as 802.11b, enables you to access the Internet, to send and receive email, and browse the Web anywhere within range of a Wi-Fi access point, or HotSpot. Wi-Fi typically has a range of up to 100 meters, and is typically intended for connectivity to an Internet-capable appliance at a hot-spot. Wi-Fi bandwidth is specified at up to 54 Mbps (802.11 a – 5.0 GHz or 802.11 b/g – 2.4 GHz).

WiMAX short for Worldwide Interoperability for Microwave Access. (IEEE 802.16) WiMAX is a standards-based wireless technology that provides high-throughput broadband connections over long distances, such as several kilometers (up to 50km with direct line-of-sight, up to 8km without direct line-of-sight). WiMAX can be used for a number of applications, including "last mile" broadband connections, hotspots and cellular backhaul, and high-speed enterprise connectivity for business.

WLAN Short for "wireless local-area network". Also referred to as LAWN. A WLAN is a type of local-area network that uses high-frequency radio waves rather than wires for communication between nodes (e.g., between PCs).

ZigBee ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). ZigBee is targeted at RF applications that require a low data rate, long battery life, and secure networking.

Contactless Interfaces

As used herein, "contactless interfaces" refers to high radio frequency (RF) connections between one device and another, typically over a very short distance, such as only up to 50

cm. The following are examples of contactless interfaces and/or devices that typically connect via a contactless interface.

ISO 14443 ISO 14443 RFID cards; contactless proximity cards operating at 13.56 MHz with a read/write range of up to 10 cm. ISO 14443 defines the contactless interface smart card technical specification.

ISO 15693 ISO standard for contactless integrated circuits, such as used in RF-ID tags. ISO 15693 RFID cards; contactless vicinity cards operating at 13.56 MHz with a read/write range of up to 100 cm. (ISO 15693 is typically not used for financial transactions because of its relatively long range as compared with ISO 14443.)

NFC Short for "Near Field Communication". NFC is a contactless connectivity technology that enables short-range communication between electronic devices. If two devices are held close together (for example, a mobile phone and a personal digital assistant), NFC interfaces establish a peer-to-peer protocol, and information such as phone book details can be passed freely between them. NFC devices can be linked to contactless smart cards, and can operate like a contactless smart card, even when powered down. This means that a mobile phone can operate like a transportation card, and enable fare payment and access to the subway. NFC is an open platform technology standardized in ECMA (European Computer Manufacturers Association) 340 as well as ETSI (European Telecommunications Standards Institute) TS 102 190 V1.1.1 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds, and frame format of the RF interface of NFC devices, as well as initialization schemes and conditions required for data collision-control during initialization – for both passive and active modes.

RFID Short for "Radio Frequency Identification". An RFID device interacts, typically at a limited distance, with a "reader", and may be either "passive" (powered by the reader) or "active" (having its own power source, such as a battery).

Wireless versus Contactless Interfaces

Wireless and Contactless are two types of radio frequency (RF) interfaces. In a most general sense, both are "wireless" in that they do not require wires, and that they use RF. However, in the art to which this invention most nearly pertains, the terms "wireless" and "contactless" have two very different meanings and two very different functionalities.

The wireless interfaces of interest in the present invention are principally WLAN, Zigbee, Bluetooth, Wibree and UWB. These wireless interfaces operate at a distance of several meters, generally for avoiding "cable spaghetti" for example, Bluetooth for headsets and other computer peripherals. WLAN is typically used for networking several computers in an office.

The contactless interfaces of interest in the present invention are principally RFID contactless interfaces such as ISO 14443, 15693 and NFC. RFID operates at a maximum distance of 100 cm for the purpose of identification in applications such as access control. In a payment (financial transaction) application, the distance is restricted to 10 cm. For example, a contactless RFID smart card protocol according to ISO 14443 can be used for private, secure financial transactions in "real world" applications such as payment at a retailer.

Wireless and contactless use different communications protocols with different capabilities and are typically used for very different purposes. Note, for example, that 100 cm (ISO 15693, an RFID contactless protocol) is considered to be too great a distance to provide appropriate security for (contactless) financial transactions. But 100 cm would not be enough to provide a (wireless) network between office computers! Additionally, generally, contactless technology is primarily passive (having no power source of its own), deriving power to operate from the electromagnetic field generated by a nearby reader. Also, contactless technology, using the smart card protocol, is used for secure identification, authentication and payment. Wireless technologies, on the other hand, generally require their own power source (either batteries, or plugged in) to operate. Contactless is different than wireless; different protocol, different signal characteristics, different utility, different energy requirements, different capabilities, different purposes, different advantages, different limitations.

Further Distinctions between Wireless Interfaces

A distinction has been made between contactless interfaces operating at very short distances (such as only up to 10cm, 50cm or 100cm) such as for secure financial transactions, and wireless interfaces operating at moderate distance, such as up to 100m.

A further distinction can be made within the definition of wireless (short distances, such as up to 10 meters) between wireless connections for a private area network (PAN) operating at close range of only several meters (and ensuring a reasonable level of privacy), and wireless connections for a wireless area network (WAN) operating at a medium/moderate range of up to 100 meters to provide public access to the Internet, at hot spots, or to set up a wireless LAN within an office environment.

Thus, for purposes of this disclosure there are identified (and defined) 4 different "levels" (or types) of communication interfaces using radio frequency (RF) for transferring data between compatible devices, as follows:

- "contactless", for very short distances, up to 100 cm (less than one meter), such as for performing secure applications such as access control, or financial transactions. (When carrying a smart card, a user needs to feel confident that the contents of the card cannot be snooped or skimmed from a nearby stranger wielding a laptop.) Within contactless, a further distinction can be made between extremely short distances (such as ISO 14443 operating at up to 10 cm distance, and useful for secure financial transactions) and moderately short distances (such as ISO 15693 having a read/write range of up to 100 cm, and useful for RFID used to collect tolls electronically).
- "PAN wireless", effective at short distances, up to several meters (such as 10 meters), for providing a personal network, generally for a single user (telephone, computer, Bluetooth headset, computer peripherals), and providing a small measure of privacy based on the limited range of the signal. Also, Infrared (optical transmission), Zigbee, Bluetooth and UWB are used in private area networks.
- "WAN wireless", effective at moderate distances, such as up to 100 meters, such as for networking computers in an office environment. .
- "WiMAX wireless", effective at long distances, such as up to 50 kilometers, for providing broadband access to the public (simultaneously to many users), which can hardly be considered to be private, without accompanying encryption of data / signal packets.

Prior Art Publications

The following patents and applications are incorporated by reference in their entirety herein.

US Patent Nos. 6,763,315; 6,745,042; 6,560,711; 6,307,471; 6,070,240; 6,456,958.

US patent application nos. 20050044424, 20020104012, 20020069030, 20020065625.

SUMMARY OF THE INVENTION

According to an embodiment of the invention, a portable RFID reader / card system comprises: a generally rectangular body; circuitry disposed within the body portion; and a contactless ID card disposed in close proximity to the body portion. The circuitry may be arranged to communicate with the contactless ID card in a contactless mode and with an external reader in a wireless mode. The contactless ID card may be disposed in a recess in a surface of the body portion. The contactless ID card may be clipped to a lanyard which is attached to the body portion.

According to an embodiment of the invention, a method of using a contactless ID card for physical entry comprises: disposing the ID card in close proximity to a portable reader system; and presenting the combination of card and reader apparatus to a mullion reader.

According to an embodiment of the invention, a method of using a contactless ID card for logical access comprises: disposing the ID card in close proximity to a portable reader system; and presenting the combination of card and reader apparatus to a wireless token associated with a personal computer. When the user is in the vicinity of their computer, a communication event may be opened up between the wireless token and combination of reader and ID card, thereby allowing the user to access a network after checking the credentials on the proximity (ID) card via the reader / card system. When the user moves away from their computer, the communication signal between the reader / card system and the wireless token deteriorates, and the computer automatically logs-off from the network or goes into password protected security mode. Once the reader / card system carried by the user is out of range of the Zigbee / Bluetooth The token may use a standard selected from the group consisting of Zigbee, Bluetooth, and Wibree.

BRIEF DESCRIPTION OF THE DRAWINGS

Reference will be made in detail to embodiments of the disclosure, examples of which may be illustrated in the accompanying drawing figures (FIGs). The figures are intended to be illustrative, not limiting. Although the invention is generally described in the context of these embodiments, it should be understood that it is not intended to limit the invention to these particular embodiments.

Certain elements in selected ones of the figures may be illustrated not-to-scale, for illustrative clarity. The cross-sectional views, if any, presented herein may be in the form of "slices", or "near-sighted" cross-sectional views, omitting certain background lines which would otherwise be visible in a true cross-sectional view, for illustrative clarity. In some cases, hidden lines may be drawn as dashed lines (this is conventional), but in other cases they may be drawn as solid lines.

If shading or cross-hatching is used, it is intended to be of use in distinguishing one element from another (such as a cross-hatched element from a neighboring un-shaded element). It should be understood that it is not intended to limit the disclosure due to shading or cross-hatching in the drawing figures.

Elements of the figures may (or may not) be numbered as follows. The most significant digits (hundreds) of the reference number correspond to the figure number. For example, elements of Figure 1 (FIG. 1) are typically numbered in the range of 100-199, and elements of FIG. 2 are typically numbered in the range of 200-299. Similar elements throughout the figures may be referred to by similar reference numerals. For example, the element 199 in FIG. 1 may be similar (and possibly identical) to the element 299 in FIG. 2. Throughout the figures, each of a plurality of elements 199 may be referred to individually as 199a, 199b, 199c, etc. Such relationships, if any, between similar elements in the same or different figures will become apparent throughout the specification, including, if applicable, in the claims and abstract.

FIG. 1 is a perspective, exploded view of a portable card reader, according to an embodiment of the invention.

FIG. 2 is a schematic plan view of the card reader of FIG. 1.

FIG. 3 is a diagram of a portable card reader in the context of physical and logical access(es), according to an embodiment of the invention.

FIG. 4 is a diagram of major functional blocks of a portable card reader, according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The invention relates to a portable identity card / reader system for logical and physical access, is a continuation-in-part of the C16 patent application and a non-provisional filing of the C18 provisional patent application.

Summary of the C16 patent application

The C16 patent application describes a pocket-size RFID reader apparatus having a contactless interface and a slot for insertion of a contactless smart card fob, and having a biometric sensor, thereby providing two levels of personalization. The apparatus may have a wireless interface, and a slot for insertion of a wireless SD I/O device. The apparatus may have a slot for insertion of an external memory device. The apparatus may have a mechanical connection (contact) interface. The apparatus may also have an RF interface for reading an electronic immobilizer within the apparatus.

As set forth in the C16 patent application, the RFID reader has a contactless interface selected from the group consisting of ISO 14443, ISO 15693, NFC, and any similar interface. And it has an interface for communicating with an Internet-capable appliance; and the interface with the Internet-capable appliance in a Private Area Network is selected from the group consisting of Zigbee, NFC, Bluetooth, UWB, wireless USB, Infrared; and the interface with the Internet-capable appliance for a Local Area Network is selected from the group consisting of 802.11 a/b/g, 802.11n and WIMAX.

In addition, the RFID reader has a biometric membrane sensor with actuator for powering up the apparatus and authenticating the user. The apparatus can generate "One-Time-Passwords" and can synchronize itself with an Internet atomic clock. The apparatus battery can be charged through inductive coupling with a docking station.

The RFID reader can also be paired with an external Bluetooth / Zigbee dongle or token.

The dongle or token is inserted into an USB port of an Internet connected PC or host computer for the purpose of transmitting and receiving data in wireless mode to and from the RFID reader.

An important feature of the C16 patent application is the functional combination of the contactless card or fob with the reader, in applications (uses), meaning that the user carries the contactless card or fob in the RFID reader with multiple interfaces when performing a transaction or an exchange.

The traditional identification cards are proximity cards operating at low frequency (125 KHz) and communicating with an RFID reader in Wiegand protocol. However, there is a move in the access control market towards high frequency cards operating at 13.56 MHz in accordance with the ISO 14443 standard, but this is a slow process because of the installed base of low frequency systems.

In application, the user carries their ID card or badge attached to a lanyard which hangs from their neck. The ID card or badge has a slot to allow the lanyard to be clipped on. Alternatively the ID card or badge fits into a plastic sleeve with a corresponding slot.

In entering a building, a facility or a secure area, the user presents the ID card to an RFID reader usually mounted on a wall (mullion reader) at eye level. As the ID card is attached to a lanyard hanging from the neck of the user, the ID card is not forgotten by the user when the verification process is completed and the user is allowed to physically access the building, facility or secure area.

For computer logon at the user's desk, the situation is completely different, the user is required to remove their ID card from the lanyard and place it on an RFID reader to allow the user to logically access the network system.

Irrespective of the operating frequency of the ID card, a desktop RFID reader needs to be permanently attached to the user's computer.

A major disadvantage of the current solution for the dual purpose of physical and logical access is users tend to forget their ID card on the desktop RFID reader when leaving the building, and thus preventing them from re-entering.

As the installed base of desktop readers for logical access control is in its infant stage of business growth, integrators are presented with the problem of selecting a low or high frequency reader to match with the current in-house physical access control system.

The RFID reader apparatus described in 11/420,747 (C16) is RFID agnostic, supporting a variety of international standards. The apparatus can incorporate a thumbprint biometric membrane sensor with actuator which can be depressed to power-up the apparatus and to acknowledge a transaction. Slots are provided in the apparatus for the insertion of removable color-coded Secure Digital (SD) memory and SD input/output (I/O) devices. The apparatus can generate "One-Time Passwords" when in an electromagnetic field, in a wireless hot spot or can synchronize itself with an Internet atomic clock and precisely record all events and transactions with an exact time/date stamp. As the insertable contactless smart card fob can be personalized with encrypted keys (Login ID & Passwords), the RFID reader apparatus can issue an authorization signal or transmit keys for access to password protected sites via it's contactless or wireless interfaces when the biometric sensor captures a digital image of a live fingerprint which coincides with the template stored in the memory of the reader or contactless chip. As the keys can be updated on a regular basis using the Internet Atomic Clock for synchronization, secure Single Sign-on for a number of websites (specific to the personalized fob) can be achieved.

The contactless interface of the RFID reader apparatus can be in accordance with ISO 14443 & ISO 15693 and/or NFC. The contactless interface typically operates at 13.56 MHz.

The wireless interface of the RFID reader apparatus can be selected from the group; Zigbee, Bluetooth, WLAN 802.11, Wibree, UWB, USB wireless and / or any similar interface.

The traditional approach to authenticate the identity of a person or computer is the direct online communications via Online Certificate Status Protocol (OCSP) to a secured, trusted authority that can verify the validation of a digital certificate. OCSP is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC

2560 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed "OCSP responders".

The C16 patent application describes an RFID reader apparatus that can validate whether a person is allowed to access a network (logical access) or enter a facility (physical access) using its wireless interface. Real time upgrading & revoking of privileges or authorizing certain activities and access permissions can be implemented when the user is in a WPAN (wireless personal area network) or a WLAN (wireless local area network) such as a hot spot or office building. Revoking or granting of privileges can be via the wireless interface of the apparatus and such messages can be embedded in the EEPROM of the RFID device or in mass storage. The transmission of real time credentials can be via the host, contactless or wireless interface.

The privileges are stored on the contactless smart card fob and have to be updated on a regular basis. As the fob is inserted into the RFID reader apparatus, the privileges are upgraded or revoked by communicating in wireless mode with a central server and then with the fob in contactless mode with these updates.

The Present Invention

Building on the C16 patent application concept of reader and contactless card being used in combination as paired devices for applications such as access control, ticketing and payment, it is proposed herein to improve on concept by changing the housing to resemble a card body with an opening to accommodate the attachment of a lanyard and grooves on each side of the housing to allow the user to slide in their identification card for physical access control.

The present invention resolves the problem of using proximity cards for physical access as well as for logical access, by replacing the desktop reader with a portable RFID reader and a Zigbee / Bluetooth / Wibree USB token.

The portable reader with multiple interfaces takes the place of the ID card as described above and may be attached to a lanyard. The user simply slides their proximity ID card into the

grooves provided in the housing. Alternatively, the lanyard is clipped both to the portable reader and to the ID card.

For logical access, the portable reader communicates with the ID card in contactless mode at either 125 KHz or 13.56 MHz, and with the Zigbee / Bluetooth / Wibree USB token inserted into a port of the host computer in wireless mode.

In another embodiment of the invention, the portable reader can communicate with an UHF card.

As in the C16 patent application, the ID card can be in the form of a fob for insertion into a slot in the portable reader.

When the user is in the vicinity of their computer, a communication event is opened up between the Zigbee / Bluetooth / Wibree token and the portable reader, allowing the user to access the network after checking the credentials on the ID card via the reader. As soon as the user moves away from their computer, the communication signal between the portable reader and the Zigbee / Bluetooth / Wibree token deteriorates. Once a certain distance is reached between the token and the portable reader, the host computer is logged off automatically.

The user can download files from the host computer to the memory of the portable reader or to an extended memory inserted into a slot in the reader.

The reader can have a mechanical interface such as a mini USB socket to allow a hardwire connection to a USB port of the host computer.

In another embodiment of the invention, the portable reader can fit into a plastic sleeve which can also accommodate an ID card. To increase the read / write range of the ID card or ID fob a compensating antenna can be integrated into the plastic sleeve.

The reader can have slots to accommodate a payment fob, a customer loyalty fob or a coupon fob in applications as described in 10/990,296 filed 11/16/2004 (C4). To increase the read / write range as described above, compensating antennae can be assembled at each contactless fob slot as well as around the perimeter of the portable reader.

The lanyard can also be used to pickup radio signals. Conversely, an antenna in the portable reader can be used to inductively charge the internal battery.

This engaged arrangement of a portable reader in the format of a card operating in conjunction with an ID card in close proximity and a Zigbee / Bluetooth / Wibree USB token connected to a host computer, enables multiple applications to be achieved using legacy technology.

This bundling of usages into an arrangement as described above can also be transferred to a keyless entry system for a motor vehicle. The portable reader with a slot or hatch to accommodate an immobilizer could be used for vehicle entry and ignition. The reader / immobilizer combination can be detected by the vehicle. Or, the reader / immobilizer in the format of a card can be inserted into an aperture in the console of the vehicle.

As described in the C16 patent application, the user can insert an SD memory stick containing MP3 files into a slot in the reader which can be played back on the vehicle entertainment system.

Not only can the reader transmit the MP3 files to the vehicle entertainment system when inserted into an aperture in the console, but also the reader battery can be charged up simultaneously.

The reader / immobilizer can have a biometric sensor, switching elements, an LED, a display, SD/IO slots and with the same functionalities as described in the C16 patent application.

In another embodiment of the invention, the USB Zigbee / Bluetooth / Wibree token can be replaced by a computer peripheral device such as a mouse with a Zigbee / Bluetooth / Wibree interface.

The signal strength from the Zigbee / Bluetooth / Wibree token determines the maximum distance in which the user can move away from their computer, before it logs-off from the network or goes into password protected security mode. Once the portable reader carried by the user is out of range of the Zigbee / Bluetooth / Wibree signal, the computer logs off

automatically.

The arrangement of the portable reader and ID card may be referred to as a "reader / ID card system" in the remainder of this application.

In the work place, all employees will have a reader / ID card system hanging from the lanyard around their neck and the employee's computer will have a Zigbee / Bluetooth / Wibree token plugged into one of its USB ports (or equivalent). Although the token is paired with the user's reader and ID card for security, the token can detect the signal from other reader / ID card combinations. Hence, the Zigbee / Bluetooth / Wibree token can be used to determine the location of a person or an employee who carries a reader / ID card system in the work place.

The Zigbee / Bluetooth / Wibree token can also act as a wireless access point (AP).

The reader / ID card system can also be used in time & attendance applications. As soon as a token receives a signal from the reader in the work place, a time-of-arrival is detected. The internal clocks of the token and reader can be synchronized with an Internet atomic clock.

The Zigbee / Bluetooth / Wibree token can also have an RFID / NFC interface for the purpose of proximity identification at the user's computer & activating the reader / card system when in sleep mode. This arrangement is particularly interesting for applications such as network access and time & attendance.

The reader / ID card system may operate in passive and/or active mode.

Power Optimization & Charging

When the user leaves their work place, the reader does not (ceases to) detect any Zigbee / Bluetooth / Wibree signal from the token (plugged into the user's computer) and hence may go into "sleep mode" (to preserve battery power).

The reader of the reader / ID card system can be switched on from sleep mode when the reader / ID card system is presented to another reader such as a wall reader at the entrance of a building. Basically, the energy radiated from the wall reader switches on the reader carried by

the employee. Alternatively, the user can switch on the reader manually.

The reader can be charged inductively, from a power source or from a computer when connected via a USB cable.

An Embodiment Of Portable Identity Card / Reader System For Physical And Logical Access

FIGs. 1 and **2** illustrate a portable card reader 100, according to an embodiment of the invention. The card reader 100 comprises a generally rectangular body 102, having a length dimension "x1", a height dimension "y1" and a thickness dimension "z1". The body 102 has a generally planar, generally rectangular front surface 104, measuring "x1" by "y1". Electronics (or circuitry, see FIG. 4) for the reader are contained within the body portion 102.

The body 102 has a slot 106 for hooking (attaching) the reader to a lanyard (not shown) which may be worn around a user's neck.

A contactless ID card 110 may be disposed in a recess (receptacle) 108 on the front surface 104 of the reader body 102. Grooves or barbs may be provided to hold the ID card 110 in place. Alternatively, the user can clip their ID card also to the lanyard, so as to be in close proximity to the reader body 102. The reader 100 and the card 110 are used in combination. The contactless ID card 110 may conform to ISO 7810 standard, and may be generally retangular.

Exemplary dimensions for the body 102 are:

length x1 = 100.00mm

height y1 = 75mm

thickness z1 = 2.00mm

Exemplary dimensions for the contactless ID card 110 are:

length x2 = 85.60mm

height y2 = 53.98mm

thickness z2 = 0.76mm

FIG. 1 illustrates how a user can insert two contactless fobs 120 and 130 into the reader 100 for applications such as identification, payment, loyalty, ticketing, couponing etc. In addition,

an SD memory stick 140 can be inserted into the reader 100 for the purpose of storing data. The data can be transferred to the memory stick in wireless mode from the host computer or the reader can be connected directly to a USB port of the host computer using a cable. Not shown is a mini USB socket in the reader.

FIG. 2 illustrates how the contactless fobs 120 and 130 can communicate in contactless mode with the reader 100. Two antenna coils 122 and 132 are positioned in the reader body 102 to communicate with the two contactless fobs 120 and 130, respectively, in a contactless mode. In addition, there is an antenna 112 positioned around the perimeter of the reader body 102 which can act as a compensating antenna or to communicate with the ID card 110. No antenna is needed for the SD card 140, since it uses a contact interface. An additional antenna (not shown) may be included as a as a stripe of metal on the motherboard of the reader, for communicating via wireless such as with a wireless token (see 372, below) plugged into a user's computer (see 370, below).

FIG. 3 illustrates an overall portable identity card / reader system for physical and logical access, according to an embodiment of the invention.

A portable reader apparatus 300 (compare 100), with a plurality of contactless cards 310 (compare 110) and 330 (compare 120 and/or 130) inserted therein, and extended memory 340 (compare 130) inserted therein, constitute what may be called a "reader/card system" 350.

For physical access, a user presents his reader/card system 350 near a wall reader 360 which is connected to a facility computer 362, and access to the facility may be provided and logged in. This is in contactless (close proximity) mode, as indicated by the two-headed arrow 366.

For logical access, a user is in proximity with his computer 370, and a wireless link is provided between the reader/card system 350 and a token 372 plugged into the computer 370. This is in wireless (vicinity) mode. The user can then use the computer, including accessing other networked computers 374, as indicated by the arrow 376.

Ensure Technologies has developed a product called Xyloc which detects a user when close to their PC in order to prevent security breaches from within a company. The product determines a user's location and automatically locks the user's computer when the user is not

physically present. Basically, the company network is not compromised when an employee leaves his or her computer unattended. The wireless technology is based on 300, 800 or 900 MHz radio signals, depending on the country of installation. (Source: www.ensuretech.com)

Unlike the present invention, the solution provided by Ensure does not combine contactless (RFID reader / ID card system) with token technology for the dual purpose of physical and logical access.

Research In Motion (RIM) is a designer, manufacturer and marketer of wireless solutions for the mobile communications market and has developed the wireless handheld product BlackBerry®. Recent developments include the BlackBerry Smart Card Reader™ which is a lightweight, wearable smart card reader that enables controlled access to BlackBerry devices using Bluetooth® technology and advanced AES-256 encryption. The identification card which is inserted into a mechanical reader is an ISO 7816 compliant smart card.
Source: www.rim.com & http://www.blackberry.com/products/accessories/smartcard.shtml

Unlike the present invention, the solution provided by RIM does not combine contactless (RFID reader / ID card system) with wireless technology for the dual purpose of physical and logical access.

There has thus been described herein a portable RFID reader / card system (combination of reader and card) in the form of a card body structure with a slot to accommodate the attachment of a lanyard and grooves on each side of the housing to allow the bearer to slide in their proximity card for physical access control. The reader / card system communicates with the proximity card at close range (such as within only up to a few millimeters) in contactless mode at either 125 KHz or 13.56 MHz and communicates with an external reader over a longer range (such as up to 10 meters) at a specific frequency and with specific protocol modes. For example, when entering a building, a facility or a secure area, the user presents the reader / card system to an RFID reader usually mounted on a wall (mullion reader). The reader / card system communicates with the proximity card at the appropriate frequency and then communicates this information to the access control reader at the entrance to the building. This means that the proximity card does not necessarily need to communicate in the same manner as the reader / card system with the access control reader.

For logical access the portable reader / card system communicates in wireless mode with a Zigbee / Bluetooth / Wibree USB token inserted into (associated with) a USB port of the user's work station / personal computer.

When the user is in the vicinity of their computer (such as within 1-2 meters), a communication event is opened up between the Zigbee / Bluetooth / Wibree token and the reader / card system, allowing the user to access the network after checking the credentials on the proximity card via the reader / card system. As soon as the user moves away from their computer, the communication signal between the reader / card system and the Zigbee / Bluetooth / Wibree token deteriorates. The signal strength from the Zigbee / Bluetooth / Wibree token determines the maximum distance in which the user can move away from their computer, before it logs-off from the network or goes into password protected security mode. Once the reader / card system carried by the user is out of range of the Zigbee / Bluetooth / Wibree signal, the computer logs off automatically.

When the user leaves their work place, the reader / card system does not detect any Zigbee / Bluetooth / Wibree signal from the USB token and hence goes into sleep mode.

For physical access, the portable reader can be switched on from sleep mode when the reader / card system is presented to another reader such as a wall reader at the entrance of a building. Basically, the energy radiated from the wall reader switches on the reader / card system carried by the employee. Alternatively, the user can switch on the reader manually.

A battery in the portable reader can be charged inductively, from a power source or from a computer when connected via a USB cable.

The user can download files from the host computer to the memory of the portable reader / card system or to an extended memory card (such as SD) inserted into a slot in the unit.

The reader / card system can have slots to accommodate a payment fob, a customer loyalty fob or a coupon fob in applications as described in 10/990,296 filed 11/16/2004 ("C4"). To increase the read / write range as described above, compensating antennae can be assembled at each contactless fob slot as well as around the perimeter of the reader / card system.

This engaged arrangement of a reader / card system in the format of a card body operating in conjunction with an identity card or badge in close proximity and a Zigbee / Bluetooth / Wibree USB token connected to a host computer, enables multiple applications to be achieved using legacy technology.

FIG. 4 is a diagram of major functional blocks of an RFID reader apparatus, according to the invention.

FIG. 4 corresponds generally to FIG. 2A of the C16 provisional, and illustrates major functional blocks of an embodiment of an RFID reader apparatus 400, which may include (but are not limited to):

- memory 404
- contact interfaces 406, such as (but not limited to) USB (or smart card ISO 7816)
- a microprocessor 410 for controlling the operation of the other functional blocks
- contactless interfaces 412, such as (but not limited to) ISO 14443, ISO 15693 and NFC (and any similar interface)
- storage 416, such as (but not limited to) a hard drive (HDD)
- wireless interfaces 418, such as (but not limited to) IEEE 802.11, Bluetooth, Zigbee, Wibree, etc
- card slots 424 (which are contact interfaces) for inserting SD cards, and the like

Storage 416 may be an internal flash drive or an HDD augmented by external memory such as a removable SD memory stick. (Memory 404 may be standard RAM for the microprocessor 410.)

Such an RFID reader apparatus 400 with multiple interfaces (mechanical, contactless, wireless and optical), extended memory (flash and/or hard disk drive) and a slot to insert a transponder device or contactless smart card fob, as discussed hereinbelow, can be used in a plethora of applications such as logical and physical access, secure identification, ticketing, payment and e-commerce.

The RFID reader apparatus 400 may be configured for transferring messages & data from the contactless interface 412 to the wireless interface 418 in active mode and to run contactless to wireless applications.

The RFID reader apparatus 400 may be configured for interfacing with the Internet (via TCP/IP interface 430) and emulating a smart card. In real world applications, the apparatus is a "mobile wallet" used as prepaid electronic cash, tickets, ID, access to buildings and corporate networks, membership cards for clubs and loyalty programs, etc.

The RFID reader apparatus 100 may include a standard-compliant contactless interface and a wireless client interface; wherein the contactless interface 412 complies to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 & ISO 15693 and NFC; and wherein the wireless client interface 418 comprises at least one of the interfaces selected from the group consisting of Zigbee, Bluetooth, Wibree, WLAN 802.11, UWB, USB wireless and any similar interface.

Multiple ISO Standard Protocols (Mifare, ISO 14443, ISO 15693, etc) can be stored or masked to memory 404, making the apparatus RFID agnostic (any standard communication interface) for use in a combination of applications such as physical & logical access as well as payment.

The RFID reader apparatus 400 may operate in conjunction with the inserted contactless smart card fob (116, FIG. 1B) and communicates with;

- an Internet connected PC via it's mechanical (contact) interface such as USB,
- an external RFID terminal via it's contactless interface,
- an external dongle or token plugged into a PC via it's Zigbee/Bluetooth/Wibree interface (PAN),
- a mobile device via it's NFC/Bluetooth interface, and with a WiFi network (WAN) via it's wireless interface.

The communication protocol between the RFID reader apparatus 400 / Contactless smart card fob 116 and an external (see FIG. 3) RFID reader, terminal, handheld or kiosk can include transponder information or electronic value residing in the memory of the contactless chip and /or an authorization signal with encrypted keys (generated by matching a stored biometric template with a live fingerprint or thumbprint scan).

A downside to existing authentication devices such as "One-Time-Password" tokens is that they do not replace facility access badges, and cannot be issued or administrated directly from the physical access control system console.

The portable identity card / reader system disclosed herein allows employees, contractors, customers and business partners to securely access corporate facilities and IT resources. Via the wireless interface, the apparatus can be used by network administrators to manage user privileges and access to services; register, activate, and revoke certificates of authentication as required; and ensure that all digital certificates are valid and enforced.

The portable identity card / reader system disclosed herein can generate a new pass code every sixty seconds based on the HOTP algorithm endorsed by the Initiative for Open Authentication (OATH).

Via the wireless interface, the portable identity card / reader system disclosed herein can receive time- and event- based messages.

Using the wireless interface, data and applications can be added, removed, or changed after the portable Identity Card / Reader system has been issued, eliminating the time and cost of reissuing new devices. Applications can range from cafeteria payments to enterprise network sign-on. In a single process, employee access to areas such as gated entrances, buildings, or networks can be updated or revoked.

Users can securely login to a remote server using the Identity Card / Reader system and be protected against password snooping, man-in-the-middle, keyboard logging, spoofing, phishing, pharming and Trojan attacks

In telephone banking, callers flagged as high risk can be challenged with authentication in the form of one-time passwords, biometric voiceprint samples, or additional content match questions. The portable Identity Card / Reader system 400 can be provided with a speaker microphone interface 440 and speech recognition facility 442. This can provide a level of personalization, such as for sending a password via a wireless network.

Access to the in-built timer in synchronization with an Internet Atomic clock or server clock allows applications such as temporary web-coupons or the use of time based PINs.

For long range communication such as in garage access, the standard IEEE 802.15.4 in-vehicle gate access solution (400 MHz) can be applied.

Form Factor

The portable identity card / reader system may have the form factor of a card body, but other form factors such as watch, wrist band, key fob or belt clip design are also possible.

Energy Harvesting

In a building, the portable identity card / reader system can draw energy from the environment, such as picking up the electrical energy (50/60 Hertz) and using it to charge up its internal battery. Alternatively, the energy can be drawn from the office lights (using a photovoltaic cell, such as is common in card-size calculators).

The invention has been illustrated and described in a manner that should be considered as exemplary rather than restrictive in character - it being understood that only preferred embodiments have been shown and described, and that all changes and modifications that come within the spirit of the invention are desired to be protected. Undoubtedly, many other "variations" on the techniques set forth hereinabove will occur to one having ordinary skill in the art to which the present invention most nearly pertains, and such variations are intended to be within the scope of the invention, as disclosed herein.

CLAIMS

What is claimed is:

1. A portable RFID reader / card system comprising:
a generally rectangular body;
circuitry disposed within the body portion; and
a contactless ID card disposed in close proximity to the body portion.

2. The portable RFID reader / card system of claim 1, wherein:
the circuitry is arranged to communicate with the contactless ID card in a contactless mode and with an external reader in a wireless mode.

3. The portable RFID reader / card system of claim 2, wherein:
the contactless ID card is disposed in a recess in a surface of the body portion.

4. The portable RFID reader / card system of claim 2, wherein:
the contactless ID card is clipped to a lanyard which is attached to the body portion.

5. A method of using a contactless ID card for physical entry comprising:
disposing the ID card in close proximity to a portable reader system; and
presenting the combination of card and reader apparatus to a mullion reader.

6. A method of using a contactless ID card for logical access comprising:
disposing the ID card in close proximity to a portable reader system; and
presenting the combination of card and reader apparatus to a wireless token associated with a personal computer.

7. The method of claim 6, wherein:
when the user is in the vicinity of their computer, a communication event is opened up between the wireless token and combination of reader and ID card, thereby allowing the user to access a network after checking the credentials on the proximity (ID) card via the reader / card system.

8. The method of claim 7, further comprising:

when the user moves away from their computer, the communication signal between the reader / card system and the wireless token deteriorates, and the computer automatically logs-off from the network or goes into password protected security mode. Once the reader / card system carried by the user is out of range of the Zigbee / Bluetooth

9. The method of claim 7, wherein the token uses a standard selected from the group consisting of Zigbee, Bluetooth, and Wibree.

ABSTRACT

A portable RFID reader apparatus having a contactless interface and slots or recesses for for insertion of contactless smart card fobs, including ID card, and having a wireless interface for communicating with a token plugged into a computer, provides physical and logical access.

FIG. 1

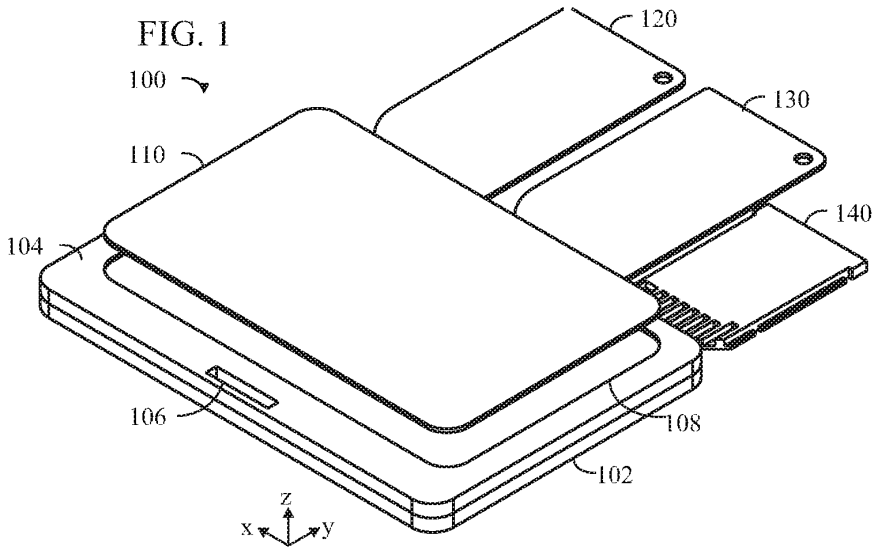


FIG. 2

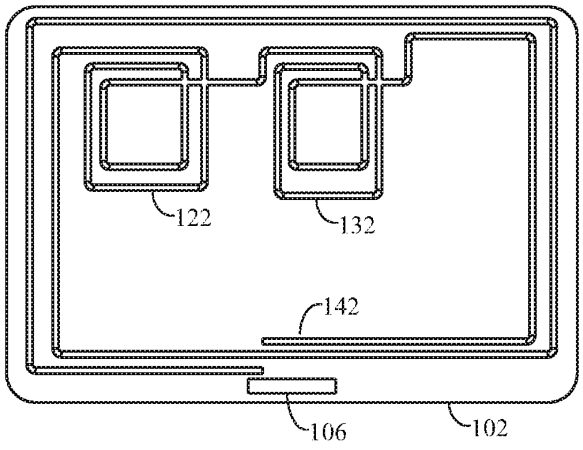


FIG. 3

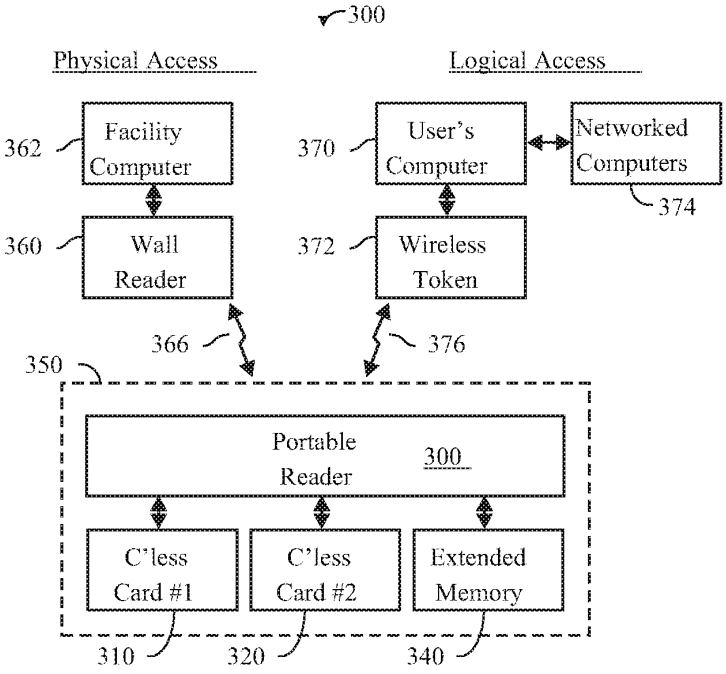
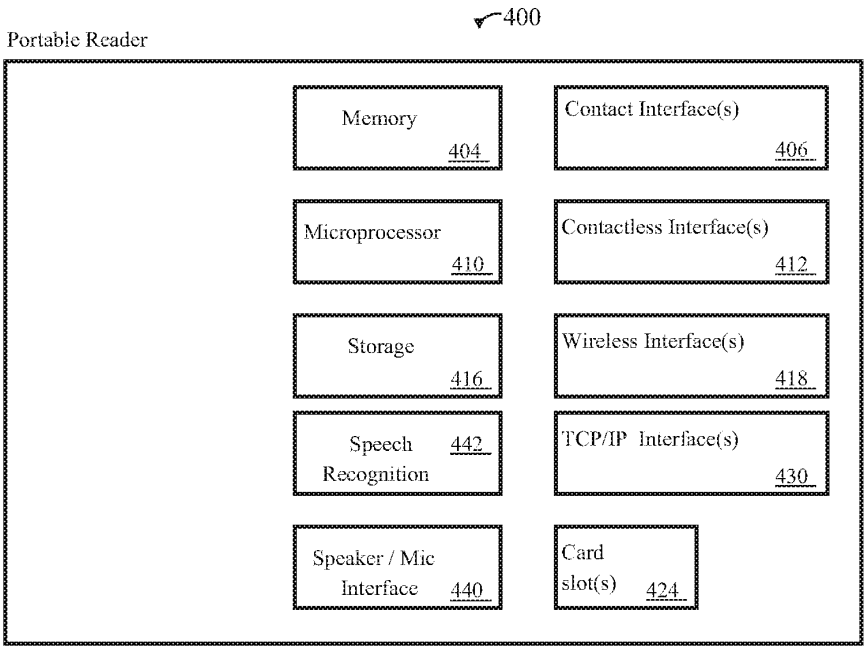

300
Physical Access
Logical Access
362
Facility Computer
370
User's Computer
Networked Computers
374
360
Wall Reader
372
Wireless Token
366
376
350
Portable Reader
300
C'less Card #1
C'less Card #2
Extended Memory
310
320
340

FIG. 4


400
Portable Reader
Memory
404
Contact Interface(s)
406
Microprocessor
410
Contactless Interface(s)
412
Storage
416
Wireless Interface(s)
418
Speech Recognition
442
TCP/IP Interface(s)
430
Speaker / Mic Interface
440
Card slot(s)
424

Attorney Docket: FINN-C18

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

COMBINED DECLARATION FOR PATENT APPLICATION
AND POWER OF ATTORNEY

Title: PORTABLE IDENTITY CARD / READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS
Inventor: FINN, David
Serial Number: 11/___,____
Filing Date: (approximately July 20, 2007)

As a below inventor, I hereby declare that; My residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am the original, SOLE inventor of the subject matter which is claimed and for which a patent is sought on the above-referenced invention.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above; that the above-identified specification contains a complete and accurate description of the subject matter which is claimed and for which a patent is sought.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, CFR §1.56(a).

I hereby claim benefit under Title 35, United States Code, §120 of any United States applications that are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in those prior applications in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations §1.56(a) which occurred between the filing date of the prior applications and the filing date of this application. I further claim benefit under Title 35 United States Code, §119 of any international patent applications listed below:

11/420,747 filed 27 May 2006 by Finn ("C16")
60/832,799 filed 24 July 2006 by Finn ("C18").
11/355,264 filed 15 Feb 2006 by Finn ("C11")
10/990,296 filed 16 Nov 2004 by Ryan et al. ("C4")

Title: PORTABLE IDENTITY CARD / READER SYSTEM FOR PHYSICAL AND LOGICAL ACCESS
Inventor: FINN, David
Serial Number: 11/___,___
Filing Date: (approximately July 20, 2007)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following agent(s) / attorney(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

GERALD E. LINDEN, Registration No. 30,282
DWIGHT A. STAUFFER, Registration No. 47,963

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 are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

David Finn 07/20/07 Ireland

David Finn Date Citizenship
Lower Churchfield, Tourmakeady, County Mayo, Ireland
Residence and Post Office Address

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Portable Identity Card Reader System For Physical And Logical Access
First Named Inventor/Applicant Name:	David Finn
Filer:	Gerald Linden
Attorney Docket Number:	
Filed as Small Entity	

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	250	250
Utility Examination Fee	2311	1	100	100
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**425**

Electronic Acknowledgement Receipt	
EFS ID:	1982714
Application Number:	11779299
International Application Number:	
Confirmation Number:	1938
Title of Invention:	Portable Identity Card Reader System For Physical And Logical Access
First Named Inventor/Applicant Name:	David Finn
Customer Number:	63397
Filer:	Gerald Linden
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	18-JUL-2007
Filing Date:	
Time Stamp:	08:35:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$425
RAM confirmation Number	5617
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)

1	Application Data Sheet	efs_ADS.pdf	1099078 3f3cb2c127fcec337cea566b6b09bf4f8459b189	no	4
Warnings:					
Information:					
2		efs_c18_application.pdf	151739 0317ca09def78949476c9a8c2257ba4b38177482	yes	32

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	29
	Claims	30	31
	Abstract	32	32

Warnings:					
Information:					
3	Drawings	efs_c18_fig1.pdf	14649 028aea7626af5ac7d6ce7fa60df48e4ff5992198	no	1
Warnings:					
Information:					
4	Drawings	efs_c18_fig3.pdf	12881 e6f9403461110fb8bc7acf9dc51e8d2c0b9cd8cc	no	1
Warnings:					
Information:					
5	Oath or Declaration filed	efs_C18_Declaration.pdf	327664 9eeeadec7ce16b62d84474b170b9812ffcf78775	no	2
Warnings:					
Information:					
6	Fee Worksheet (PTO-06)	fee-info.pdf	8354 546cbc988390cc81552a54d2571f8d96a4e3e413	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1614365		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (12-04)

F/D 7/18/2007

Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

PATENT APPLICATION FEE DETERMINATION RECORD
Substitute for Form PTO-875

Application or Docket Number
11/779,299

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	75		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	250		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	100		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	9	*	X 25=		OR	X 50=	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	*	X 100=			X 200=	
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))			N/A			N/A	
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	425		TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	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.