Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
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.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	
First Named Inventor	Siva G. Narendra
Title	MOBILE PHONE WITH MAGNETIC CARD EMULATION
Art Unit	
Examiner Name	
Attorney Docket Number	115.001US9.10

SIGNATURE of Applicant or Patent Practitioner

Signature	/Dana B. LeMoine/	Date (Optional)	2020-09-15
Name	Dana B. LeMoine	Registration Number	40062
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 35781

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Tyfone, Inc.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	/Siva G. Narendra/	Date (Optional)	March 11, 2014
Name	Siva G. Narendra		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/AIA/82C (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
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

POWER OF ATTORNEY BY APPLICANT

No more than ten (10) patent practitioners total may be appointed as set forth below by name and registration number. This page need not be submitted if appointing the Patent Practitioner(s) associated with a Customer Number (see form PTO/AIA/82B):

Name	Registration Number

Privacy Act Statement

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

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

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Siva G. Narendra
Art Unit	
Examiner Name	
Attorney Docket Number	115.001US9.10

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	4701601	A	1987-10-20	Francini et al.	Entire Document
	2	4786791	A	1988-11-22	Hodama	
	3	4791283	A	1988-12-13	Burkhardt	Entire Document
	4	4864109	A	1989-09-05	Minematsu et al.	
	5	5212478	A	1993-05-18	Moseley	
	6	5378887	A	1995-01-03	Kobayashi	
	7	5386106	A	1995-01-31	Kumar	Entire Document
	8	5537584	A	1996-07-16	Miyai et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	9	5574273	A	1996-11-12	Nakagawa et al.	Entire Document
	10	5585787	A	1996-12-17	Wallerstein	
	11	5629981	A	1997-05-13	Nerlikar	
	12	5700037	A	1997-12-23	Keller	
	13	5710421	A	1998-01-20	Kokubu	
	14	5834756	A	1998-11-10	Gutman et al.	
	15	5909491	A	1999-06-01	Luo	
	16	5940510	A	1999-08-17	Curry et al.	
	17	5949880	A	1999-09-07	Curry et al.	
	18	5952641	A	1999-09-14	Korshun	
	19	5955961	A	1999-09-21	Wallerstein	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	20	6016476	A	2000-01-18	Maes Stephane et al.	
	21	6021944	A	2000-02-08	Arakaki	
	22	6039260	A	2000-03-21	Eisele	
	23	6045043	A	2000-04-04	Bashan et al.	
	24	6068184	A	2000-05-30	Barnett	
	25	6105013	A	2000-08-15	Curry et al.	
	26	6182891	B1	2001-02-06	Furuhashi et al.	
	27	6189786	B1	2001-02-20	Itou et al.	
	28	6206293	B1	2001-03-27	Gutman et al.	
	29	6219439	B1	2001-04-17	Burger	
	30	6223954	B1	2001-05-01	Carow	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	31	6223984	B1	2001-05-01	Renner G et al.	
	32	6237095	B1	2001-05-22	Curry et al.	
	33	6250557	B1	2001-06-26	Forslund et al.	
	34	6315195	B1	2001-11-13	Ramachandran	
	35	6402029	B1	2002-06-11	Gangi	
	36	6450407	B1	2002-09-17	Freeman et al.	Entire Document
	37	6481623	B1	2002-11-19	Grant et al.	Entire Document
	38	6568600	B1	2003-05-27	Carpier et al.	Entire Document
	39	6588660	B1	2003-07-08	Buescher et al.	Entire Document
	40	6592044	B1	2003-07-15	Wong et al.	
	41	6594759	B1	2003-07-15	Wang	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	42	6598031	B1	2003-07-22	Ice	
	43	6607127	B2	2003-08-19	Wong	
	44	6609654	B1	2003-08-26	Anderson et al.	
	45	6631849	B2	2003-10-14	Blossom	
	46	6636833	B1	2003-10-21	Flitcroft et al.	
	47	6669487	B1	2003-12-30	Nishizawa et al.	
	48	6705520	B1	2004-03-16	Pitroda et al.	Entire Document
	49	6712277	B2	2004-03-30	Spencer	
	50	6715679	B1	2004-04-06	Infosino	
	51	6721196	B1	2004-04-13	Grassl	
	52	6747547	B2	2004-06-08	Benson	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	53	6764005	B2	2004-07-20	Cooper J	
	54	6769607	B1	2004-08-03	Pitroda et al.	
	55	6805288	B2	2004-10-19	Routhenstein et al.	
	56	6811082	B2	2004-11-02	Wong	Entire Document
	57	6836843	B2	2004-12-28	Seroussi et al.	
	58	6857566	B2	2005-02-22	Wankmueller	
	59	6882900	B1	2005-04-19	Terranova	
	60	6883718	B1	2005-04-26	Le et al.	
	61	6905072	B2	2005-06-14	Ramachandran	
	62	6907123	B1	2005-06-14	Schier	
	63	6908030	B2	2005-06-21	Rajasekaran et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	64	6925568	B1	2005-08-02	Heinonen	
	65	6937526	B2	2005-08-30	Furukawa	
	66	6952788	B2	2005-10-04	Rommelmann et al.	
	67	6995651	B2	2006-02-07	Amtmann et al.	
	68	7059520	B1	2006-06-13	Shtesl	
	69	7088246	B2	2006-08-08	Fukuoka	
	70	7185146	B2	2007-02-27	Masuyama et al.	
	71	7213766	B2	2007-05-08	Ryan et al.	Entire Document
	72	7221473	B2	2007-05-22	Jeran et al.	
	73	7281101	B2	2007-10-09	Mizushima et al.	
	74	7295790	B2	2007-11-13	Morimoto et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	75	7333062	B2	2008-02-19	Leizerovich et al.	Entire Document
	76	7350717	B2	2008-04-01	Conner et al.	
	77	7353993	B2	2008-04-08	Fujimoto	
	78	7410102	B2	2008-08-12	Winkler	
	79	7493484	B2	2009-02-17	Lee	
	80	7558107	B2	2009-07-07	Sakurai et al.	
	81	7558110	B2	2009-07-07	Mizushima et al.	
	82	7581678	B2	2009-09-01	Narendra et al.	
	83	7607580	B2	2009-10-27	Takita et al.	
	84	7673080	B1	2010-03-02	Yu et al.	
	85	7716082	B1	2010-05-11	Blalock	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	86	7789303	B2	2010-09-07	Fukasawa	
	87	7792516	B2	2010-09-07	Soderstrom	
	88	7828214	B2	2010-11-09	Narendra et al.	
	89	7898994	B2	2011-03-01	Zhao et al.	Entire Document
	90	7933571	B2	2011-04-26	Black et al.	
	91	7941197	B2	2011-05-10	Jain et al.	
	92	7948356	B2	2011-05-24	Kawamura et al.	
	93	7954715	B2	2011-06-07	Narendra et al.	
	94	7954716	B2	2011-06-07	Narendra et al.	
	95	7954717	B2	2011-06-07	Narendra et al.	
	96	7961101	B2	2011-06-14	Narendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	97	7991158	B2	2011-08-02	Narendra et al.	
	98	8072331	B2	2011-12-06	Narendra et al.	
	99	8082575	B2	2011-12-20	Doughty et al.	Entire Document
	100	8083145	B2	2011-12-27	Narendra et al.	
	101	8091786	B2	2012-01-10	Narendra et al.	
	102	8103881	B2	2012-01-24	Doughty et al.	Entire Document
	103	9092708	B1	2015-07-28	Narendra et al.	Entire Document
	104	9202156	B2	2015-12-01	Narendra et al.	Entire Document
	105	9715649	B2	2017-07-25	Narendra et al.	Entire Document
	106	RE41352	E	2010-05-25	Wood Jr	
	107	RE41471	E	2010-08-03	Wood Jr	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	108	RE42254	E	2011-03-29	Wood Jr	

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	20010002035	A1	2001-05-31	Kayanakis	
	2	20010006902	A	2001-07-05	Ito	Entire Document
	3	20010013551	A1	2001-08-16	Ramachandran	
	4	20010034246	A1	2001-10-25	Hutchison et al.	Entire Document
	5	20020007434	A1	2002-01-17	Campardo	
	6	20020025796	A1	2002-02-28	Taylor William et al.	Entire Document
	7	20020043566	A1	2002-04-18	Goodman et al.	
	8	20020044043	A1	2002-04-18	Chaco et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	9	20020095588	A1	2002-07-18	Shigematsu et al.	
	10	20020096570	A1	2002-07-25	Wong et al.	
	11	20020099665	A1	2002-07-25	Burger et al.	
	12	20020130187	A1	2002-09-19	Berg et al.	
	13	20020138422	A1	2002-09-26	Natsuno	
	14	20020138735	A1	2002-09-26	Felt et al.	
	15	20020139849	A1	2002-10-03	Gangi	
	16	20020148892	A1	2002-10-17	Bardwell	
	17	20020153424	A1	2002-10-24	Li	
	18	20020158747	A1	2002-10-31	Mcgregor et al.	
	19	20020178124	A1	2002-11-28	Lewis Shawn	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	20	20020180584	A1	2002-12-05	Mcgregor et al.	
	21	20020186845	A1	2002-12-12	Dutta et al.	
	22	20030218066	A1	2003-11-27	Fernandes et al.	Entire Document
	23	20030025939	A1	2003-02-06	Jeran et al.	
	24	20030028481	A1	2003-02-06	Flitcroft et al.	
	25	20030038177	A1	2003-02-27	Morrow	Entire Document
	26	20030052168	A1	2003-03-20	Wong	
	27	20030057278	A1	2003-03-27	Wong	
	28	20030061168	A1	2003-03-27	Routhenstein	
	29	20030079096	A1	2003-04-24	Murakami	
	30	20030080183	A1	2003-05-01	Rajasekaran et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	31	20030084220	A1	2003-05-01	Jones Larry et al.	Entire Document
	32	20030085288	A1	2003-05-08	Luu	
	33	20030115126	A1	2003-06-19	Pitroda	
	34	20030128124	A1	2003-07-10	Amtmann et al.	
	35	20030159050	A1	2003-08-21	Gantman et al.	
	36	20030200180	A1	2003-10-23	Phelan et al.	
	37	20030209604	A	2003-11-13	Harrison	Entire Document
	38	20030220876	A1	2003-11-27	Burger et al.	
	39	20030231550	A1	2003-12-18	Macfarlane	
	40	20040006654	A1	2004-01-08	Bando	
	41	20040027881	A1	2004-02-12	Furukawa	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	42	20040030660	A1	2004-02-12	Shatford	
	43	20040035942	A1	2004-02-26	Silverman	
	44	20040050930	A1	2004-03-18	Rowe	
	45	20040058705	A1	2004-03-25	Morgan et al.	
	46	20040064612	A1	2004-04-01	Pinto et al.	
	47	20040065733	A1	2004-04-08	Fukuoka	
	48	20040077372	A1	2004-04-22	Halpern	
	49	20040087339	A1	2004-05-06	Goldthwaite et al.	
	50	20040094624	A1	2004-05-20	Fernandes et al.	
	51	20040122685	A	2004-06-24	Bunce	Entire Document
	52	20040133787	A1	2004-07-08	Doughty et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	53	20040162932	A	2004-08-19	Mizushima et al.	Entire Document
	54	20040177045	A1	2004-09-09	Brown Kerry	
	55	20040188519	A1	2004-09-30	Cassone	
	56	20040199469	A1	2004-10-07	Barillova et al.	
	57	20040227859	A1	2004-11-18	Liang	
	58	20040243785	A1	2004-12-02	Shanmugasundaram et al.	
	59	20040243806	A1	2004-12-02	Mckinley et al.	
	60	20040251303	A1	2004-12-16	Cooper J	
	61	20040255145	A1	2004-12-16	Chow	
	62	20050224589	A1	2005-10-13	Park et al.	Entire Document
	63	20050240778	A1	2005-10-27	Saito	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	64	20050006462	A1	2005-01-13	Rouille et al.	
	65	20050017068	A1	2005-01-27	Zalewski et al.	
	66	20050022002	A	2005-01-27	Poisner	Entire Document
	67	20050029349	A1	2005-02-10	Mcgregor et al.	
	68	20050038736	A1	2005-02-17	Saunders	
	69	20050039027	A1	2005-02-17	Shapiro	
	70	20050044044	A1	2005-02-24	Burger et al.	
	71	20050050367	A1	2005-03-03	Burger et al.	
	72	20050052924	A1	2005-03-10	Nishizawa et al.	
	73	20050060586	A1	2005-03-17	Burger et al.	
	74	20050071282	A1	2005-03-31	Lu Hongqian et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	75	20050077349	A1	2005-04-14	Bonalle et al.	
	76	20050092830	A1	2005-05-05	Blossom	
	77	20050108096	A1	2005-05-19	Burger et al.	
	78	20050109838	A1	2005-05-26	Linlor	
	79	20050116026	A1	2005-06-02	Burger et al.	
	80	20050121512	A1	2005-06-09	Wankmueller	
	81	20050122209	A1	2005-06-09	Black	
	82	20050127164	A1	2005-06-16	Wankmueller	
	83	20050127166	A1	2005-06-16	Minemura	
	84	20050133606	A1	2005-06-23	Brown	
	85	20050136964	A1	2005-06-23	Le Saint et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	86	20050168339	A1	2005-08-04	Arai et al.	
	87	20050177724	A1	2005-08-11	Ali et al.	
	88	20050197859	A1	2005-09-08	Wilson et al.	
	89	20050204077	A1	2005-09-15	Kou	
	90	20050204092	A1	2005-09-15	Masuyama et al.	
	91	20050212657	A1	2005-09-29	Simon	
	92	20050223143	A1	2005-10-06	Kang et al.	
	93	20050246546	A	2005-11-03	Takagi et al.	Entire Document
	94	20050253687	A1	2005-11-17	Martinez et al.	
	95	20050258245	A1	2005-11-24	Bates et al.	
	96	20050268058	A	2005-12-01	Drasnin et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	97	20050268330	A1	2005-12-01	Di Rienzo	
	98	20060124755	A1	2006-06-15	Ito	Entire Document
	99	20060219776	A1	2006-10-05	Finn	Entire Document
	100	20060011731	A1	2006-01-19	Anders et al.	Entire Document
	101	20060027655	A1	2006-02-09	Smets et al.	
	102	20060045555	A1	2006-03-02	Morimoto et al.	
	103	20060077039	A1	2006-04-13	Ibi et al.	
	104	20060097851	A1	2006-05-11	Amtmann et al.	
	105	20060169778	A1	2006-08-03	Chung	Entire Document
	106	20060172606	A1	2006-08-03	Irisawa	
	107	20060186209	A1	2006-08-24	Narendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	108	20060226217	A1	2006-10-12	Narendra et al.	
	109	20060268764	A1	2006-11-30	Harris	
	110	20060279413	A1	2006-12-14	Yeager	
	111	20070033334	A1	2007-02-08	Katayama et al.	
	112	20070076877	A1	2007-04-05	Camp et al.	
	113	20070108280	A1	2007-05-17	Li et al.	
	114	20070110404	A1	2007-05-17	Ching et al.	
	115	20070145135	A1	2007-06-28	Jogand-Coulomb et al.	
	116	20070145152	A1	2007-06-28	Jogand-Coulomb et al.	
	117	20070195458	A1	2007-08-23	Sawai et al.	
	118	20070205864	A1	2007-09-06	Mutti et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	119	20070257797	A1	2007-11-08	Rancien et al.	
	120	20070293202	A1	2007-12-20	Moshir et al.	
	121	20080046649	A1	2008-02-21	Ito	
	122	20080065830	A1	2008-03-13	Aoki et al.	
	123	20080068173	A1	2008-03-20	Alexis et al.	
	124	20080073436	A1	2008-03-27	Nishizawa et al.	
	125	20080136619	A1	2008-06-12	Moran	
	126	20080147950	A1	2008-06-19	Chen	
	127	20080148077	A1	2008-06-19	Lee et al.	
	128	20080153416	A1	2008-06-26	Washiro	
	129	20080186174	A1	2008-08-07	Alexis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	130	20080214111	A1	2008-09-04	Moshir et al.	
	131	20080244208	A1	2008-10-02	Narendra et al.	
	132	20080279381	A1	2008-11-13	Narendra et al.	
	133	20080311849	A1	2008-12-18	Washiro	
	134	20080318535	A1	2008-12-25	Black et al.	
	135	20090070272	A1	2009-03-12	Jain	Entire Document
	136	20090108063	A1	2009-04-30	Jain et al.	Entire Document
	137	20090065571	A1	2009-03-12	Jain	
	138	20090065572	A1	2009-03-12	Jain	
	139	20090069049	A1	2009-03-12	Jain	
	140	20090069050	A1	2009-03-12	Jain et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	141	20090069051	A1	2009-03-12	Jain et al.	
	142	20090069052	A1	2009-03-12	Jain et al.	
	143	20090070691	A1	2009-03-12	Jain	
	144	20090070861	A	2009-03-12	Jain	Entire Document
	145	20090150610	A1	2009-06-11	Hsu et al.	
	146	20090152361	A1	2009-06-18	Narendra et al.	
	147	20090199283	A1	2009-08-06	Jain	
	148	20090250521	A1	2009-10-08	Fujita et al.	
	149	20090265552	A1	2009-10-22	Moshir et al.	
	150	20090270127	A1	2009-10-29	Kakimoto	
	151	20090290582	A1	2009-11-26	Suenaga et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	152	20090298540	A1	2009-12-03	Narendra et al.	
	153	20090315667	A1	2009-12-24	Kawamura et al.	
	154	20100033307	A	2010-02-11	Narendra et al.	Entire Document
	155	20100033310	A	2010-02-11	Narendra et al.	Entire Document
	156	20100049878	A1	2010-02-25	Yu et al.	
	157	20100213265	A1	2010-08-26	Narendra et al.	
	158	20110000960	A	2011-01-06	Harris	Entire Document
	159	20110053644	A1	2011-03-03	Narendra et al.	
	160	20110073663	A1	2011-03-31	Narendra et al.	
	161	20110073665	A1	2011-03-31	Narendra et al.	
	162	20110077052	A1	2011-03-31	Narendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	163	20110110404	A1	2011-05-12	Washiro	
	164	20110171996	A1	2011-07-14	Narendra et al.	
	165	20110180610	A1	2011-07-28	Narendra et al.	
	166	20110220726	A1	2011-09-15	Narendra et al.	
	167	20110223972	A1	2011-09-15	Narendra et al.	
	168	20110240748	A1	2011-10-06	Doughty et al.	Entire Document
	169	20110269438	A1	2011-11-03	Narendra et al.	
	170	20110271044	A1	2011-11-03	Narendra et al.	
	171	20110272468	A1	2011-11-10	Narendra et al.	
	172	20110272469	A1	2011-11-10	Narendra et al.	

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

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

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	10054890	DE	A1	2002-04-25	Schneider		
	2	3632294	DE	A1	1988-04-07	Limmer		
	3	0818757	EP	A2	1998-01-14	Hazra et al.		
	4	1014290	EP	A2	2000-06-28	Kettunene et al.		
	5	1117068	EP	A1	2001-07-18	Nagaoka et al.		
	6	1178450	EP	A2	2002-02-06	Vazvan		
	7	1189465	EP	A1	2002-03-20	Christensen Per et al.		
	8	1291748	EP	A2	2003-03-12	Stevens et al.		
	9	1308874	EP	A2	2003-05-07	Luu	Entire Document	
	10	161060	EP	A1	1985-11-13	Pullukat Thomas et al.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	11	2316908	GB	A	1998-03-11	Cowling		
	12	2000010668	JP	A	2000-01-14	Funatsu		
	13	2005018671	JP	A	2005-01-20	Okawa et al.		
	14	2007199847	JP	A	2007-08-09	Nakao et al.		
	15	2007328689	JP	A	2007-12-20	Yamada		
	16	4102112	JP	A	1992-04-03	Fukushima et al.		
	17	200905471	TW	A	2009-02-01	Narendra et al.		
	18	201020934	TW	B	2010-06-01	Narendra et al.	Entire Document	
	19	201023662	TW	A	2010-06-16	Narendra et al.		
	20	201126422	TW	A	2011-08-01	Narendra et al.	English Abstract	
	21	I336449	TW		2011-01-21	Narendra et al.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	22	0014678	WO	A1	2000-03-16	Combaluzier Pierre		
	23	0188659	WO	A2	2001-11-22	Wong et al.		
	24	03029942	WO	A2	2003-04-10	Burger et al.		
	25	03077473	WO	A1	2003-09-18	Andersson et al.		
	26	03081519	WO	A2	2003-10-02	Thomas et al.		
	27	2004012352	WO	A1	2004-02-05	Goldthwaite et al.		
	28	2004095169	WO	A2	2004-11-04	Osterweil et al.		
	29	2005027030	WO	A1	2005-03-24	Kurokawa et al.		
	30	2005119607	WO	A2	2005-12-15	Spitzer et al.		☒
	31	2005119608	WO	A1	2005-12-15	Spitzer et al.		☐
	32	2006091709	WO	A2	2006-08-31	Narendra et al.		☒

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	33	2006108184	WO	A1	2006-10-12	Narendra et al.		☐
	34	2007011937	WO	A2	2007-01-25	Narendra et al.		☐
	35	2008121566	WO	A1	2008-10-09	Narendra et al.		☐
	36	2009147548	WO	A2	2009-12-10	Corda		☐
	37	2010099093	WO	A1	2010-09-02	Narendra et al.		☐
	38	9626500	WO	A1	1996-08-29	Peek		☐
	39	9812674	WO	A2	1998-03-26	Field John		☐

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	International Search Report PCT Application No. PCT/US2005/019988, December 16, 2005, 5 pages.	
	2	International Search Report PCT Application No. PCT/US2005/022993, October 21, 2005, 3 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	3	International Search Report PCT Application No. PCT/US2006/013603, January 9, 2006, 3 pages.
	4	International Search Report PCT Application No. PCT/US2006/027847, March 29, 2007, 5 pages.
	5	International Search Report PCT Application No. PCT/US2008/057588, August 7, 2008, 1 pages.
	6	International Written Opinion PCT Application No. PCT/US2005/019988 , Dec. 4, 2006, 9 Pages.
	7	International Written Opinion PCT Application No. PCT/US2005/019988, Jan. 11, 2006, 8 pages.
	8	International Written Opinion PCT Application No. PCT/US2005/022993, December 4, 2006, 6 pages.
	9	International Written Opinion PCT Application No. PCT/US2006/006361, August 28, 2007, 8 pages.
	10	International Written Opinion PCT Application No. PCT/US2006/006361, September 22, 2006, 13 pages.
	11	International Written Opinion PCT Application No. PCT/US2006/013603, October 9, 2007, 7 pages.
	12	International Written Opinion PCT Application No. PCT/US2006/027847, January 22, 2008, 10 pages.
	13	International Written Opinion PCT Application No. PCT/US2008/057588, Aug. 7, 2008, 5 pages.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	14	International Written Opinion PCT Application No. PCT/US2008/057588, October 6, 2009, 6 pages.
	15	International Written Opinion PCT Application No. PCT/US2010/025014, April 15, 2010, 9 pages.
	16	International Written Opinion PCT Application No. PCT/US2010/025014, September 09, 2011, 6 pages.
	17	Lee, Youbok; "Antenna Circuit Design for RFID Applications", Microchip, AN710, 2003 Microchip Technology Inc., (2003), 50 pages.
	18	Official Letter from Taiwan Patent Office 115.001TW1, Application 95105997, and Search Report dated on Oct 20, 2010, 6 pages.
	19	US Patent Application 13/592,323 Office Action dated September 30, 2014, 6 pages
	20	US Patent Application 14/680,684 Office Action dated May 22, 2015, 5 pages.
	21	US Patent Application 14/747,770 Office Action dated September 25, 2015, 7 pages
	22	US Patent Application 14/833,113 Office Action dated September 24, 2015, 9 pages
	23	US Patent Application 14/866,998 Office Action dated November 5, 2015, 7 pages
	24	US Patent Application 14/929,297 Office Action dated September 16, 2016, 8 pages

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

	25	US Patent Application 14/948,325 Office Action dated September 20, 2016, 7 pages	
	26	US Patent Application 15/658,208 Office Action dated April 19, 2018, 7 pages	
	27	US Patent Application 16/218,733 Office Action dated November 29, 2019, 6 pages.	

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[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	
	Filing Date	
	First Named Inventor	Siva G. Narendra
	Art Unit	
	Examiner Name	
	Attorney Docket Number	115.001US9.10

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Dana B. LeMoine/	Date (YYYY-MM-DD)	2020-09-15
Name/Print	Dana B. LeMoine	Registration Number	40062

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.

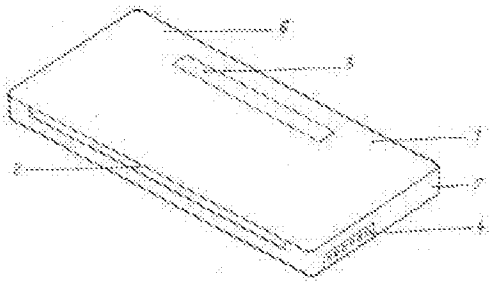
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Mobile universal data terminal with insertion and head parts has at least one card reading unit in one or more insertion slots with different arrangements for reading different chip card types

Publication number: DE10054890 (A1)
Publication date: 2002-04-25
Inventor(s): SCHNEIDER BERND [DE] +
Applicant(s): SCHNEIDER BERND [DE] +
Classification:
- international: ***G06K7/00;*** **G06K7/00;** (IPC1-7): G06F3/08; G06K7/06; G06K7/08; H04L29/12
- European: G06K7/00E; G06K7/00K
Application number: DE20001054890 20001106
Priority number(s): DE20001054890 20001106; DE20001051596 20001018

Abstract of **DE 10054890 (A1)**

The device has one or more card reading units (1), an arrangement both for reading, storing and transmitting data to or from a central computer and an insertion slot for chip cards. At least one card reading unit is arranged in one or more insertion slots with different arrangement s for reading different types of chip card, including cards with contacts and cards without contacts.



Data supplied from the ***espacenet*** database — Worldwide

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 54 890 A 1**

(51) Int. Cl.[7]:
G 06 F 3/08
G 06 K 7/06
G 06 K 7/08
H 04 L 29/12

(21) Aktenzeichen: 100 54 890.3
(22) Anmeldetag: 6. 11. 2000
(43) Offenlegungstag: 25. 4. 2002

DE 100 54 890 A 1

(66) Innere Priorität:
100 51 596. 7 18. 10. 2000

(71) Anmelder:
Schneider, Bernd, 01462 Gompitz, DE

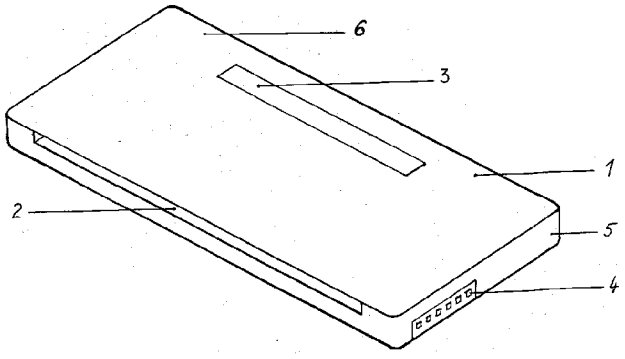
(74) Vertreter:
Patentanwälte Ilberg und Weißfloh, 01328 Dresden

(72) Erfinder:
gleich Anmelder

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Mobiles universelles Datenterminal mit Einschub und Kopfteil

(57) Die Erfindung betrifft ein mobiles universelles Datenterminal mit Einschub und Kartenleseeinheit zum Lesen, Schreiben und Speichern von Daten von Chipkarten. Es kann eine Übertragung von Daten (Verarbeiten von Daten) zu bzw. von einem zentralen Rechner erfolgen, mit dem Chipkarten gelesen oder beschrieben werden können.
Der Erfindung liegt die Aufgabe zugrunde, ein mobiles universelles Datenterminal zu schaffen, daß in der Lage ist, mehrere verschiedene Arten von Chipkarten je nach Bedarf automatisch zu erkennen, zu lesen und/oder zu beschreiben.
Erfindungsgemäß sind in einem mobilen universellen Datenterminal, das mindestens einen Einschub besitzt, eine oder mehrere Kartenleseeinheiten 1 angeordnet. Diese Kartenleseeinheiten 1 sind mit Mitteln sowohl zum Lesen und/oder Beschreiben als auch zum Speichern von Daten ausgerüstet. Diese Daten werden dann an das Datenterminal übergeben, das für ein Verarbeiten von Daten und auch zur Übertragung von Daten geeignet ist. Diese Daten werden weiterhin zu bzw. von einem zentralen Rechner übertragen. Dabei ist ein Kommunizieren des Datenterminals mit der oder den Kartenleseeinheiten 1 unter Einbeziehung des zentralen Rechners möglich. Das mobile Datenterminal besitzt mindestens einen Einschubschlitz für Chipkarten am Einschub. Im Einschub selbst sind mindestens eine oder mehrere Kartenleseeinheiten 1 in Slots (Einschubschacht für Kartenleseeinheit) angeordnet. Diese Kartenleseeinheiten 1 mit einem Einschubschlitz 2 besitzen ...



DE 100 54 890 A 1

IPR2025-00645 Page 00041

Beschreibung

[0001] Die Erfindung betrifft ein mobiles universelles Datenterminal mit Einschub und Kopfteil und Kartenleseeinheit zum Lesen, Schreiben und Speichern von Daten von Chipkarten. Es kann eine Übertragung von Daten (Verarbeiten von Daten) zu bzw. von einem zentralen Rechner erfolgen, mit dem Chipkarten gelesen und oder beschrieben werden können.

[0002] Es sind mobile Datenterminale (sogenannte Handheldcomputer) bekannt die mit einem Einschub ausgestattet sind. In diesem Einschub ist dabei ein Slot angeordnet mit dem eine Magnetkarten gelesen werden kann.

[0003] Aus der DE 41 33 148 ist ein Kommunikationsendgerät bekannt das mit einem Kartenlesegerät und Mitteln zum wahlweisen Übertragen von Daten oder Sprachsignalen zu bzw. von einem Gegengerät, das entsprechende Sprachübertragungs- bzw. Datenterminalfunktion aufweist. Das Kartenlesegerät kann dabei mehrere gleichartige Karten, hier Geldkarten, lesen und ist mit einem Speicher zum lesen der Karte ausgestattet. Dabei wird in zwei Schritten eine Gruppenkennungsinformation ausgewertet und freigegeben um eine kostenpflichtige Dienstleistung vorzubereiten und auszuführen.

[0004] Aus der DE 44 06 704 C1 sind Chipkarten bekannt auf denen mehrere Mikrokontroller angeordnet sind, die je nach Art des verwendeten Lesegerätes in Aktion treten und die. Chipkarte damit durch unterschiedliche Lesegeräte gelesen und die Daten ausgetauscht werden können. Eine ähnliche Lösung ist in der DE 44 65 583 C1 beschrieben wo Anschlüsse einer Chipkarte sowohl zur seriellen als auch zur parallele Übertragung von Daten geeignet sind und ebenfalls mehrere unterschiedliche Chips angeordnet sind, die in Abhängigkeit von der Art des Lesegerätes sich in Eingriff befinden können.

[0005] Neben einer Vielzahl von kontaktbehafteten Chipkarten sind auch kontaktlose Chipkarten bekannt. So ist z. B. in der DE 196 08 515 C1 eine kontaktlose Chipkarte beschrieben, die mittels einer piezoelektrischen Membran über Schall an ein Lesegerät angekoppelt ist und kommuniziert.

[0006] Aus der DE 197 70 521 A1 sind Chipkarten bekannt, die neben statischen auch dynamische Daten enthalten und die damit intelligente Lesegeräte, mit denen sowohl gelesen als auch geschrieben werden kann, voraussetzen.

[0007] Die DE 196 33 924 beschreibt einen Chipkartenleser wo als Lesegerät eine ebene Kunststoffplatte fungiert. Sie besitzt dabei genau die Größe einer Chipkarte und muß von Hand positioniert werden. Dies ist mit einer Hand nur sehr schwer möglich. Außerdem ist ein Positionieren, Halten und gleichzeitiges Bedienen einzelner Tasten von Hand nur sehr schwer möglich. Im gleichen Schutzrecht sind Koppelspulen beschrieben die ebenfalls eine kontaktlose Ankopplung und ein kontaktloses Kommunizieren zwischen einer Chipkarte und einem Lesegerät ermöglichen.

[0008] Alle bekannten im Stand der Technik beschriebenen Lesegeräte beschreiben jeweils nur die Möglichkeit eine ganz bestimmte Kartenart lesen zu können.

[0009] Der Erfindung liegt die Aufgabe zugrunde ein mobiles universelles Datenterminal zu schaffen, daß in der Lage ist mehrere verschiedene Arten von Chipkarten je nach Bedarf automatisch zu erkennen, zu lesen und/oder zu beschreiben.

[0010] Die Aufgabe wird erfindungsgemäß mit den technischen Merkmalen des 1. Anspruches gelöst. Dabei sind in einem mobilen universellen Datenterminal, das mindestens einen Einschub besitzt, eine oder mehrere Kartenleseeinheiten **1** angeordnet. Diese Kartenleseeinheiten **1** sind mit Mitteln sowohl zum Lesen und/oder Beschreiben als auch zum Speichern von Daten ausgerüstet. Diese Daten werden dann an das Datenterminal übergeben, das für ein Verarbeiten von Daten und auch zur Übertragung von Daten geeignet ist. Diese Daten werden weiterhin zu bzw. von einem zentralen Rechner übertragen. Dabei ist ein Kommunizieren des Datenterminals mit der oder den Kartenleseeinheiten **1** unter Einbeziehung des zentralen Rechners möglich. Das mobile Datenterminal besitzt mindestens einen Einschubschlitz für Chipkarten am Einschub. Im Einschub selbst sind mindestens eine oder mehrere Kartenleseeinheiten **1** in Slots (Einschubschacht für Kartenleseeinheit **1**) angeordnet. Diese Kartenleseeinheiten **1** besitzen verschiedene Mittel, die zum Lesen von unterschiedlichen Arten von Chipkarten so ausgebildet sind, daß sowohl eine in den Einschubschlitz **2** der Kartenleseeinheit **1** eingesteckte kontaktbehaftete als auch eine kontaktlose Chipkarte gelesen werden kann.

[0011] In einer vorteilhaften Ausgestaltung ist das mobile universelle Datenterminal so ausgebildet, daß eine erste Kartenleseeinheit **1** mit einem Einschubschlitz **2** für Chipkarten in einem Slot (Einschubschacht für Kartenleseeinheit **1**) angeordnet ist. Dabei ist die zu lesende und/oder zu beschreibende kontaktbehaftete oder kontaktlose Chipkarte durch den Einschubschlitz des Einschubes bis in diese erste Kartenleseeinheit **1** einzustecken. Sie wird dann im eingeschobenen Zustand gelesen und/oder beschrieben. Im Datenterminal ist des weiteren eine zweite Kartenleseeinheit parallel zur ersten in einem zweiten Slot angeordnet. Vorteilhafterweise ist dabei die in der ersten Kartenleseeinheit **1** eingesteckte Chipkarte eine kontaktlose Chipkarte, die mittels eines elektrischen Feldes, insbesondere mittels eines Transponder-Schaltkreises gelesen und/oder beschrieben werden kann.

[0012] In einer anderen Ausführungsform kann mindestens eine Kartenleseeinheit **1** mit einem Einschubschlitz **2** für kontaktbehaftete oder kontaktlose Chipkarten in einem Slot so angeordnet und ausgebildet sein, daß auch eine nur teilweise durch den Einschubschlitz des Einschubes eingesteckte, kontaktbehaftete oder kontaktlose Chipkarte gelesen und/oder beschrieben werden kann. Da z. B. bei einer kontaktbehafteten Chipkarte bereits ein Kontaktieren über die Kontakte für einen Datenaustausch ausreichend ist, reicht die Fixierung auch bei einer nur halb oder noch weniger eingeschobenen Chipkarte aus solange die Kontaktierung sicher gewährleistet ist. Bei einer kontaktlosen Chipkarte ist bereits eine Datenübertragung möglich wenn sich der Transponder-Schaltkreis bzw. dessen Antenne in dem Bereich auf dem eine Antenne, oder ein Teil der Antenne auf der Chipkarte angeordnet ist, befindet.

[0013] Weiterhin kann das mobile universelle Datenterminal in einer vorteilhaften Ausführungsform mit einer oder mehreren Kartenleseeinheiten ausgestattet sein, die so im mobilen universellen Datenterminal angeordnet, gesteckt oder montiert sind und mit speziellen technischen Mitteln so ausgestattet sind, das eine kontaktlose Chipkarte gelesen und/oder beschrieben wird ohne daß sie sich im Einschubschlitz des mobilen Datenterminals befindet. Dabei ist auf der Gehäuseoberfläche des mobilen universellen Datenterminals eine Auflagefläche angeordnet und/oder gekennzeichnet, wo die Chipkarte aufzulegen ist. Während des Kommunikationsvorganges muß die Chipkarte dann z. B. von Hand fixiert werden um ein fehlerfreies Lesen und/oder Schreiben zu gewährleisten.

[0014] Vorteilhafterweise ist die Auflagefläche auf der Oberfläche des Gehäuses des mobilen universellen Datenterminals als eine Vertiefung in den Abmessungen einer Chipkarte an geeigneter Stelle ausgebildet. Beim Lesen und/oder Schreiben ist damit eine genaue Fixierung der entspre-

chenden Chipkarte ohne Probleme möglich. Um das Fixieren der zu lesenden und/oder zu beschreibenden Chipkarte von Hand auf der Oberfläche des mobilen universellen Datenterminal zu vermeiden ist es von Vorteil, wenn zusätzlich auf der Oberfläche des Gehäuses an geeigneter Stelle des Datenterminals ein Befestigungs- und/oder Arretierelement für eine Chipkarte angeordnet ist. Dabei ist das Befestigungs- und/oder Arretierelement auf der Oberfläche des Gehäuses an einer Stelle klappbar oder drehbar angeordnet. Es befindet sich direkt neben der Vertiefung die als Auflagefläche für die Chipkarte dient. Befindet es sich in Eingriff sichert es gleichzeitig die Chipkarte gegen Verrutschen bzw. gegen ein herausfallen aus der Vertiefung. Zum Lesen und/oder Schreiben von kontaktlosen Chipkarten ist auf der Leiterplatte mindestens eines Kartenlesers bzw. auf der Leiterplatte des Kartenlesers der an der Oberfläche des mobilen universellen Datenterminals angeordnet ist, bzw. direkt unter der Vertiefung des Gehäuses parallel zur Gehäusewandung sich befindet mindestens ein Schaltkreis als Transponder-Schaltkreis ausgebildet. Dieser Transponder-Schaltkreis ist mit den anderen Bauelementen der entsprechenden Leiterplatte und/oder den anderen Bauelementen des mobilen universellen Datenterminals verschalten.

[0015] Bei einer vorteilhaften Bestückung einer Leiterplatte für ein erfindungsgemäßen mobiles universelles Datenterminal ist auf der Leiterplatte in der Kartenleseeinheit **1** mindestens ein Kommunikationskontroller-Schaltkreis verschalten, der über die Schaltkreise des mobilen Datenterminals mittels Identifikationsnummern (ID-Nummern) steuerbar ist. Auf der Leiterplatte in der Kartenleseeinheit **1** ist ein verschaltetes Bord angeordnet, auf dem ein oder mehrere Mikrokontroller kontaktiert sind, die mit dem Kommunikationskontroller-Schaltkreis verbunden sind und untereinander Daten austauschen. Auf dieser Leiterplatte sind des weiteren ein oder mehrere Flash-Module, die insbesondere Speichermodule sind angeordnet, die mit allen anderen Bauelementen verschalten sind und kommunizieren. Somit können beliebige Informationen von und zu den betreffenden Chipkarten gespeichert werden.

[0016] In einer besonderen Ausgestaltung der Erfindung sind anstelle des Einschubes Kontakte für ein aufsteckbares Kopfteil im bzw. am mobilen universellen Datenterminal angeordnet. Das Kopfteil besteht aus mindestens zwei steckbaren, arretierbaren Einzelteilen. Der steckbare kontaktierte Kopf bildet das Bussystem zum mobilen universellen Datenterminal. Am Kopf ist des weiteren ein kontaktiertes Anbauteil anordenbar, welches vorzugsweise haubenförmig ausgebildet ist. Es enthält ein oder mehrere Slots für z. B. Kartenleseeinheiten (**1**) oder Speichermodule oder Funkmodule. Diese Kartenleseeinheiten (**1**) sind mit verschiedenen Mitteln zum Lesen und/oder Schreiben unterschiedlichen Arten von Chipkarten ausgebildet. Das Anbauteil besitzt einen oder mehrere Einschubschlitze und es sind sowohl in den Einschubschlitz eingesteckte kontaktbehaftete als auch kontaktlose Chipkarte lesbar und/oder beschreibbar. Des weiteren sind zum kodierten Datenaustausch ein oder mehrere Kommunikationskontroller-Schaltkreis angeordnet.

[0017] Im Anbauteil sind vorzugsweise ein oder mehrere Leiterplatten kaskadenartig übereinander anordenbar, wobei jede Leiterplatte jeweils spezielle Kontakte für die Verbindung zur nächsten Leiterplatte besitzt und auf jeder Leiterplatte oder den gesteckten Modulen ist ein Komunikationskontroller-Schaltkreis angeordnet, der die Daten verschlüsselt für das Bussystem bereitstellt.

[0018] In einer Außenseite des Anbauteils ist ein Mikrofon und/oder ein Erkennungssystem zur Personenidentifikation, wie z. B. ein Iriserkennungssystem, ein Fingeridentifikationssystem und/oder ein Tastaturfeld angeordnet.

[0019] Die Erfindung soll nachstehend an mehreren Ausführungsbeispielen und an Hand der Zeichnung näher erläutert werden.

[0020] Dabei besteht ein erfindungsgemäßer kontaktbehafteter Kartenleser **1** aus einem Gehäuse **5** mit Deckel **6**, einer innen angeordneten Leiterplatte, die aus einem Leiterplattengrundkörper und den darauf kontaktierten und untereinander verschalteten Bauelementen (In Zeichnungen nicht dargestellt) besteht. Im Deckel **6** ist ein Sichtfenster **3** ausgestanzt, so daß man kontrollieren kann, ob die zu lesende und/oder zu beschreibende Chipkarte voll eingeschoben ist. Gleichzeitig wird durch das Einschieben ein Kontakt (der als Endschalter ausgebildet ist) geschlossen, so daß die Datenkommunikation mit der Chipkarte begonnen werden kann. Seitlich am Leiterplattengrundkörper und im Gehäuse **5** sind deckungsgleich sechs Öffnungen **4** angeordnet, durch die die Kontaktstifte in eine auf dem Leiterplattengrundkörper an entsprechender Stelle befestigte Steckerleiste eingreifen. Diese Öffnungen **4** können sich an der verschiedenen Stellen im Gehäuse **5** befinden. Im Gehäuse **5** ist auf einer seiner Längsseite ein schmaler Einschubschlitz **2** vorgesehen, in den die zu lesende Chipkarte einzustecken ist. Dieser Kartenleser ist in einen Slot (Einschubschacht für Kartenleseeinheit **1**) eingeschoben. Dabei sind seine Innenabmessungen auf die Außenabmessungen so abgestimmt, daß sich der Kartenleser zum einen leicht einschieben läßt und zum anderen eine Führung hinreichend genau gewährleistet ist, so daß die Steckerleiste genau über die Steckerstifte geschoben wird und eine zuverlässige Kontaktierung erfolgt. Durch eine seitliche Öffnung (Einschubschlitz) im Slot, der sich deckungsgleich an der Stelle befindet in dem der schmale Einschubschlitz **2** in der Kartenleseeinheit **1** angeordnet ist, kann die Chipkarte in den Kartenleseeinheit **1** eingeschoben und gelesen werden.

[0021] Dabei sind im mobilen universellen Datenterminal, das einen Einschub besitzt, zwei Slots angeordnet. Der Einschub selbst enthält des weiteren Batterieschächte zum einen für die interne Stromversorgung des Datenterminals selbst und zum anderen für die Stromversorgung der Kartenleseeinheiten. Im Einschub sind an entsprechender Stelle zwei schmale Schlitze zum einschieben von zwei Chipkarten ausgebildet. Die beiden im Slot einsteckbaren Kartenleseeinheiten **1** sind mit Mitteln (unterschiedlichen Bauelementen) sowohl zum Lesen und/oder Beschreiben als auch zum statischen und dynamischen Speichern von Daten ausgerüstet. Diese Daten werden in Verbindung mit den Daten der eingesteckten Chipkarten während dem Verarbeitungsprozess an das Datenterminal übergeben, das für ein weiteres gesteuertes bzw. nach speziellen eingespeicherten Programm- und Prüfroutinen ablaufendes Verarbeiten von Daten und auch zur Übertragung von Daten geeignet ist. Diese Daten werden weiterhin zu bzw. von einem zentralen Rechner übertragen. Dabei ist ein Kommunizieren des Datenterminals mit der oder den Kartenleseeinheiten **1** unter Einbeziehung eines zentralen Rechners (Hostrechners) möglich. Das mobile Datenterminal besitzt in der Ausführung mit zwei Slots (Einschubschacht für Kartenleseeinheit **1**) und zwei Einschubschlitzen zwei Kartenleseeinheiten **1**, wobei eine mit Mitteln zum Lesen und/oder Beschreiben von kontaktbehafteten Chipkarten und eine mit Mitteln zum Lesen und/oder Beschreiben von kontaktlosen Chipkarten ausgestattet ist. Im Datenterminal sind die beiden Kartenleseeinheiten **1** parallel zu einander in zwei parallelen Slots angeordnet. Diese Kartenleseeinheiten **1** können bei Bedarf schnell ausgetauscht werden, so daß andere Kartenleseeinheiten **1** mit denen sich spezielle Chipkarten lesen und/oder beschreiben lassen in Eingriff gebracht werden können. Die

entsprechende Software wird dabei über den zentralen Rechner zur Verfügung gestellt. Mit dem erfindungsgemäßen mobilen universellen Datenterminal wird der Nutzer in die Lage versetzt mit einem Grundgerät alle zur Zeit bekannten, verschiedenen Arten von Chipkarten an jedem beliebigen Ort verarbeiten zu können.

[0022] Vorteilhafterweise ist dabei die Kartenleseeinheit **1**, in die eine kontaktlose Chipkarte einzustecken ist, mit einem Transponder-Schaltkreis ausgestattet. Auf der kontaktlosen Chipkarte ist eine Antenne so angeordnet, daß sie die Daten mittels eines elektrischen Feldes austauschen kann und damit mittels eines Transponder-Schaltkreises gelesen und/oder beschrieben werden kann.

[0023] In einer weiteren Ausbildung des mobilen universellen Datenterminals ist auf der Rückseite, d. h. der der Tastaturseite des mobilen universellen Datenterminals gegenüberliegenden Gehäuseseite, die Auflagefläche für eine kontaktlose Chipkarte auf der Oberfläche des Gehäuses des mobilen universellen Datenterminals als eine Vertiefung in den Abmessungen einer Chipkarte an geeigneter Stelle ausgebildet. Beim Lesen und/oder Schreiben wird die Chipkarte in die Vertiefung gelegt. Damit erfolgt eine genaue Fixierung der entsprechenden zu verarbeitenden Chipkarte. Um das Fixieren der zu lesenden und/oder zu beschreibenden Chipkarte von Hand auf der Oberfläche des mobilen universellen Datenterminal zu vermeiden ist zusätzlich in der Rückseite des Gehäuses ein ausklappbarer Hebel angeordnet. Dieser Hebel wird aufgeklappt und über die Chipkarte hinweg geklappt. Er rastet, wenn er aufliegt ein und sichert die Chipkarte gegen verrutschen bzw. gegen herunterfallen. Der Hebel kann gleichzeitig mit einem Kontakt verbunden sein, so daß ein Verarbeitungsvorgang erst beginnen kann, wenn der Hebel die Chipkarte fixiert und er eingerastet ist.

[0024] Zum Lesen und/oder Schreiben von kontaktlosen Chipkarten ist unter der Vertiefung des Gehäuses des mobilen universellen Datenterminals eine speziell bestückte Leiterplatte eines Kartenlesers parallel zur Gehäusewandung angeordnet. Auf dieser Leiterplatte ist ein Kommunikationskontroller-Schaltkreis so verschalten, daß er über die Schaltkreise des mobilen Datenterminals mittels Identifikationsnummern (ID-Nummern) steuerbar ist.

[0025] Des weiteren ist auf der Leiterplatte ein verschaltetes Bord angeordnet auf dem mehrere verschaltete Mikrokontroller kontaktiert sind, die ihrerseits mit dem Kommunikationkontroller-Schaltkreis verbunden sind. Auf dieser Leiterplatte sind ebenfalls mehrere Flash-Module und ein Transponder-Schaltkreis angeordnet und untereinander verbunden.

Patentansprüche

1. Mobiles universelles Datenterminal mit Einschub und Kopfteil, in dem eine oder mehrere Kartenleseeinheiten angeordnet sind und Mitteln sowohl zum Lesen und Speichern als auch zur Übertragung von Daten (Verarbeiten von Daten) zu bzw. von einem zentralen Rechner und einem Einschubschlitz für Chipkarten am Einschub, **dadurch gekennzeichnet**,
daß im Einschub mindestens eine oder mehrere Kartenleseeinheiten (**1**) in Slots angeordnet sind,
diese Kartenleseeinheiten (**1**) mit verschiedenen Mitteln zum Lesen und/oder von unterschiedlichen Arten von Chipkarten so ausgebildet sind
daß sowohl eine in den Einschubschlitz eingesteckte kontaktbehaftete als auch eine kontaktlose Chipkarte gelesen und/oder beschrieben werden kann.

2. Mobiles universelles Datenterminal nach Anspruch 1, dadurch gekennzeichnet,
daß eine erste Kartenleseeinheit (**1**) mit einem Einschubschlitz (**2**) für Chipkarten in einem Slot so angeordnet ist,
daß eine durch den Einschubschlitz des Einschubes einsteckbare, kontaktbehaftete oder kontaktlose Chipkarte bis in diese erste Kartenleseeinheit (**1**) gesteckt und im eingeschobenen Zustand die kontaktbehaftete oder kontaktlose Chipkarte gelesen und/oder beschrieben werden kann
und eine zweite Kartenleseeinheit parallel dazu in einem zweiten Slot so angeordnet ist,
daß die in der ersten Kartenleseeinheit eingesteckte kontaktlose Chipkarte mittels eines elektrischen Feldes, insbesondere mittels eines Transponder-Schaltkreises gelesen und/oder beschrieben werden kann.

3. Mobiles universelles Datenterminal nach Anspruch 1, dadurch gekennzeichnet, daß mindestens eine Kartenleseeinheit (**1**) mit einem Einschubschlitz (**2**) für kontaktbehaftete oder kontaktlose Chipkarten in einem Slot so angeordnet ist, daß auch eine nur teilweise durch den Einschubschlitz des Einschubes eingesteckte, kontaktbehaftete oder kontaktlose Chipkarte gelesen und/oder beschrieben werden kann.

4. Mobiles universelles Datenterminal nach Anspruch 1, dadurch gekennzeichnet, daß eine oder mehrere Kartenleseeinheiten (**1**) in einem mobilen Datenterminal gesteckt oder montiert sind und mit technischen Mitteln so ausgestattet sind, das eine kontaktlose Chipkarte gelesen und/oder beschrieben wird, ohne daß sie sich im Einschubschlitz des mobilen Datenterminals befindet wobei auf der Gehäuseoberfläche des mobilen Datenterminals eine Auflagefläche angeordnet und/oder gekennzeichnet ist.

5. Mobiles universelles Datenterminal nach Anspruch 4, dadurch gekennzeichnet, daß auf der Oberfläche des Gehäuses des mobilen universellen Datenterminals die Auflagefläche als eine Vertiefung in den Abmessungen einer Chipkarte an geeigneter Stelle des mobilen Datenterminals ausgebildet ist.

6. Mobiles universelles Datenterminal nach Anspruch 4, dadurch gekennzeichnet, daß auf der Oberfläche des Gehäuses an geeigneter Stelle des mobilen Datenterminals ein Befestigungs- und/oder Arretierelement für eine kontaktlose Chipkarte angeordnet ist.

7. Mobiles universelles Datenterminal nach Anspruch 4, dadurch gekennzeichnet, daß das Befestigungs- und/oder Arretierelement auf der Oberfläche des Gehäuses an geeigneter Stelle des mobilen Datenterminals für eine kontaktlose Chipkarte klappbar oder drehbar angeordnet ist.

8. Mobiles universelles Datenterminal nach Anspruch 1 bis 7, dadurch gekennzeichnet, daß auf der Leiterplatte des Kartenleseeinheit (**1**) mindestens ein Schaltkreis als Transponder-Schaltkreis ausgebildet ist und mit anderen Bauelementen verschalten ist.

9. Mobiles universelles Datenterminal nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
daß auf der Leiterplatte in der Kartenleseeinheit (**1**) mindestens ein Kommunikationskontroller-Schaltkreis verschalten ist, der über die Schaltkreise des mobilen Datenterminals mittels Identifikationsnummern (ID-Nummern) steuerbar ist,
auf der Leiterplatte ein verschaltetes Bord angeordnet ist, auf dem ein oder mehrere Mikrokontroller kontaktiert sind, die mit dem Kommunikationskontroller-Schaltkreis verbunden sind,
und auf der Leiterplatte ein oder mehrere Flash-Module angeordnet sind, die mit allen anderen Bauele-

menten verschalten sind.

10. Mobiles universelles Datenterminal nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß auf der Leiterplatte in der Kartenleseeinheit (**1**) alle erforderlichen Bauelemente einschließlich Kommunikationskontroller-Schaltkreis und Transponder-Schaltkreis angeordnet und verschalten sind und mit dieser Kartenleseeinheit (**1**) sowohl kontaktlose als auch kontaktbehaftete Chipkarten mit dieser Kartenleseeinheit lesbar sind.

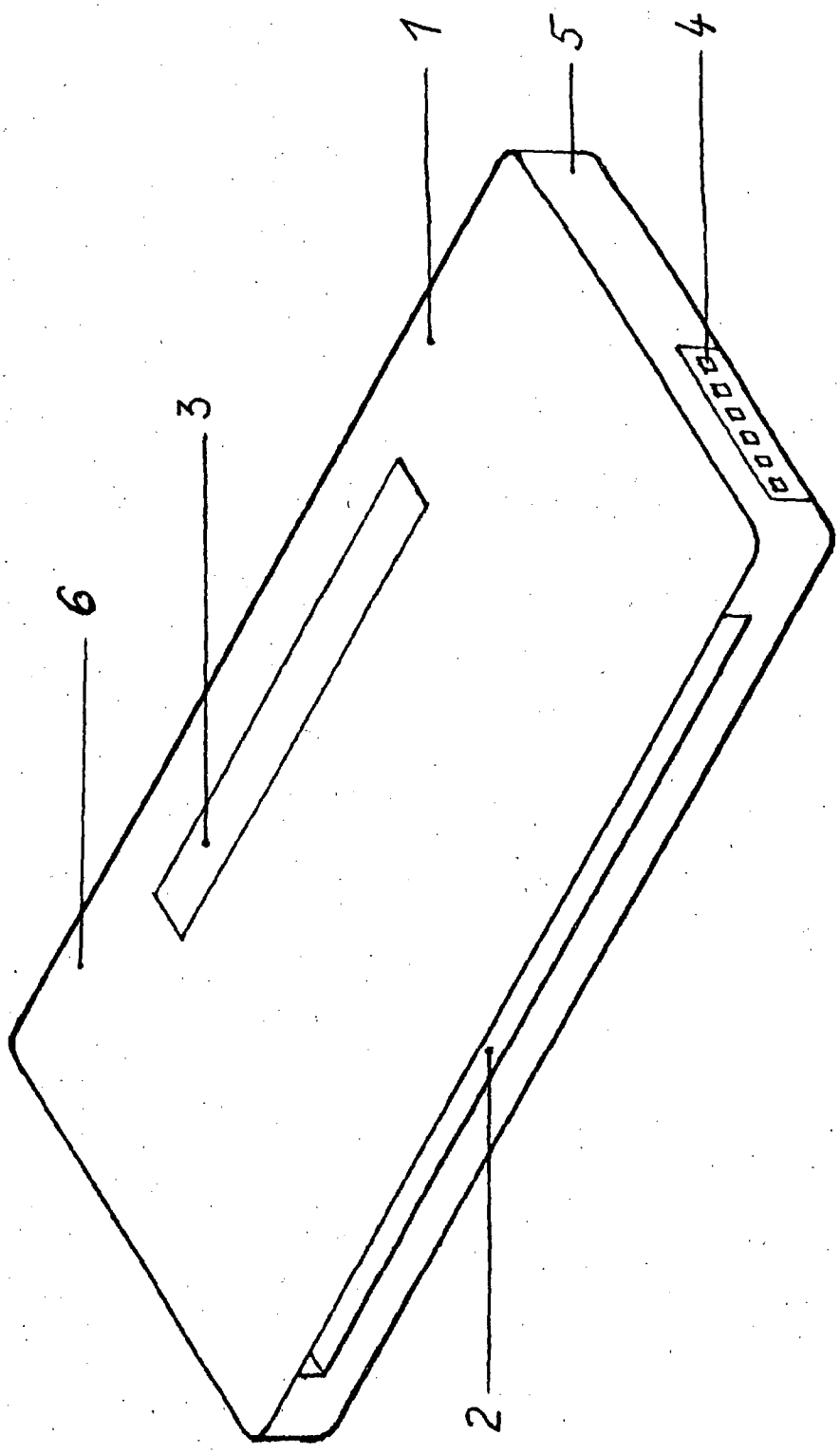
11. Mobiles universelles Datenterminal nach Anspruch 1, dadurch gekennzeichnet,
daß anstelle des Einschubes mindestens eine oder mehrere Kartenleseeinheiten (**1**) in einem steckbaren kontaktierten Kopf angeordnet sind, der seinerseits am mobilen universellen Datenterminal aufsteckbar angeordnet ist,
wobei dieser Kopf, der das Bussystem zum Datenterminal bildet, aus mindestens zwei zusammensteckbaren und arretierbaren Einzelteilen besteht und das kleinere Teil als kontaktiertes Anbauteil so ausgebildet ist, daß in ihm ein oder mehrere Kartenleseeinheiten (**1**) mit verschiedenen Mitteln zum Lesen und/oder Schreiben und/oder von unterschiedlichen Arten von Chipkarten ausgebildet sind und das Anbauteil einen oder mehrere Einschubschlitze besitzt und eine in den Einschubschlitz eingesteckte kontaktbehaftete als auch eine kontaktlose Chipkarte gelesen und/oder beschrieben werden kann und ein oder mehrere Kommunikationskontroller-Schaltkreise angeordnet sind.

12. Mobiles universelles Datenterminal nach Anspruch 11, dadurch gekennzeichnet, daß im Anbauteil ein oder mehrere Leiterplatten kaskadenartig übereinander anordenbar sind, wobei jede Leiterplatte jeweils spezielle Kontakte für die Verbindung zur nächsten Leiterplatte besitzt und auf jeder Leiterplatte und/oder auf der Platine steckbare Module, ein Komunikationskontroller-Schaltkreis angeordnet ist, der die Daten verschlüsselt für das Bussystem bereitstellt.

13. Mobiles universelles Datenterminal nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß in einer Außenseite des Anbauteils ein Mikrofon und/oder Lautsprecher und/oder auf der Außenseite ein Erkennungssystem zur Personenidentifikation und/oder ein Tastaturfeld angeordnet ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 100 54 890 A1
Int. Cl.[7]: G 06 F 3/08
Offenlegungstag: 25. April 2002



IPR2025-00645 Page 00046

Operating unit for smart cards (chip cards)

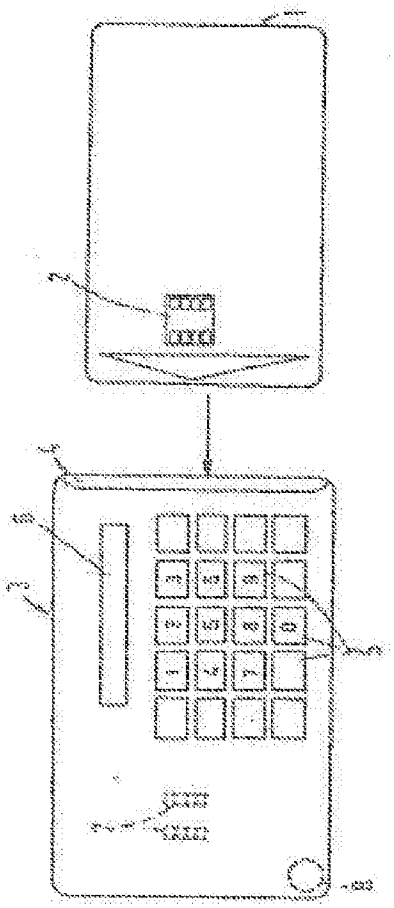
Publication number: DE3632294 (A1)
Publication date: 1988-04-07
Inventor(s): LIMMER HANS [DE] +
Applicant(s): SIEMENS AG [DE] +
Classification:
- international: ***G06K19/077; G06K7/00; G07F7/10;*** **G06K19/077; G06K7/00; G07F7/10;** (IPC1-7): G06K19/00; G07F7/08; G11C17/00; G11C7/00
- European: G06K19/077; G06K7/00K2; G07F7/10D
Application number: DE19863632294 19860923
Priority number(s): DE19863632294 19860923

Cited documents:

DE3222288 (A1)
US4563575 (A)

Abstract of **DE 3632294 (A1)**

To test the access rights to a system by comparing a personal identification number, the so-called PIN, which is entered by the user, with a PIN which is stored or calculated in the chip, an operating unit which is independent of the smart card (chip card) reader is provided. This operating unit (3) is in the form of an independent, portable plug-in pocket, which has a keyboard (5) and a display field (6) on its covering surface. The dimensions of the plug-in pocket are chosen to be only slightly greater than those of the smart card (1). Also, a flat battery (8) or a solar cell is provided as the power (voltage) source.



Data supplied from the ***espacenet*** database — Worldwide

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3632294 A1**

(51) Int. Cl. 4:
G 06 K 19/00
G 07 F 7/08
G 11 C 17/00
// G11C 7/00

(21) Aktenzeichen: P 36 32 294.6
(22) Anmeldetag: 23. 9. 86
(43) Offenlegungstag: 7. 4. 88

Behördeneigentum

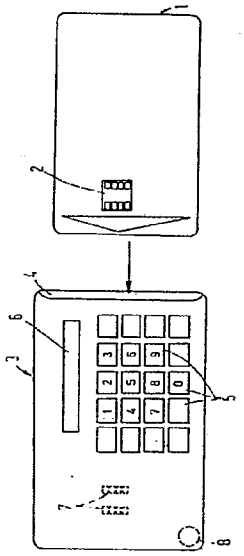
DE 3632294 A1

(71) Anmelder:
Siemens AG, 1000 Berlin und 8000 München, DE

(72) Erfinder:
Limmer, Hans, 8025 Unterhaching, DE

(54) Bedieneinheit für Chipkarten

Zur Prüfung der Zugangsberechtigung zu einem System durch Vergleich einer vom Benutzer eingegebenen persönlichen Identifikationsnummer, der sogenannten PIN, mit einer im Chip gespeicherten oder errechneten PIN ist eine vom Chipkartenleser unabhängige Bedieneinheit vorgesehen. Diese Bedieneinheit (3) ist als selbständige tragbare Einstecktasche ausgebildet, die auf ihrer Deckfläche eine Tastatur (5) und ein Anzeigefeld (6) aufweist. Die Abmessungen der Einstecktasche sind dabei nur geringfügig größer gewählt als die Abmessungen der Chipkarte (1). Ferner ist als Spannungsquelle eine Flachbatterie (8) oder eine Solarzelle vorgesehen.



DE 3632294 A1

IPR2025-00645 Page 00048

Patentanspruch

Bedieneinheit für Chipkarten mit einer schlitzartigen Einsteköffnung für die Chipkarte und einer im Innenraum vorgesehenen Kontaktiervorrichtung oder kontaktlosen Verbindung zum Anschluß des Chips sowohl an eine Spannungsquelle als auch an eine Tastatur, zur Verwendung in einem Datenaustauschsystem, bei dem die Zugangsberechtigung zum System durch einen Vergleich einer mittels der Tastatur eingegebenen Geheimnummer mit der im Chip gespeicherten oder errechneten Geheimnummer geprüft wird, **gekennzeichnet durch** die Kombination folgender Merkmale:

a) die Bedieneinheit (3) ist als selbständige, tragbare Einstecktasche ausgebildet,
b) die Einstecktasche weist an ihrer Deckfläche eine Tastatur (5) und ein Anzeigefeld (6) auf,
c) die Abmessungen der Einstecktasche sind geringfügig größer gewählt als die Abmessungen der Chipkarte (1),
d) als Spannungsquelle ist eine Flachbatterie (8) oder eine Solarzelle vorgesehen.

Beschreibung

Die Erfindung bezieht sich auf eine Bedieneinheit für Chipkarten nach dem Oberbegriff des Anspruchs 1.

Für bestehende und zukünftige Anwendungen auf allen Gebieten der Informationsverarbeitung gewinnt die Chipkarte auf Grund des Speichervermögens, der Sicherheit und der Dezentralisierung von Funktionen zunehmend an Bedeutung. Um die vielfältigen Möglichkeiten eines Chipkartensystems nutzen zu können, muß einerseits jeder Benutzer eine dem jeweiligen System angepaßte Chipkarte haben und andererseits müssen die an das System angeschlossenen Terminals mit einem Chipkartenleser versehen sein, der die elektrische und mechanische Verbindung zwischen dem Terminal und der Chipkarte herstellt. Um einen möglichen Mißbrauch von vornherein auszuschließen, sind verschiedene Sicherheitskonzepte entwickelt worden, zu denen beispielsweise die persönliche Identifikationsnummer, die sogenannte PIN gehört. Der Inhaber einer Chipkarte erhält dabei nur dann Zugang zum System, wenn er durch Angabe seiner PIN nachweist, daß die von ihm in den Chipkartenleser eingeführte Chipkarte tatsächlich ihm gehört. Dies geschieht in der Weise, daß die über eine am Chipkartenleser vorhandene Tastatur eingegebene PIN mit der im Chip der Chipkarte gespeicherten oder errechneten PIN verglichen und erst bei geprüfter Übereinstimmung eine entsprechende Freigabe für den nachfolgenden Datenaustausch erteilt wird. Diese PIN-Prüfung macht es erforderlich, daß der Chipkartenleser zum Betrieb der Tastatur und gegebenenfalls eines Anzeigefeldes eine Stromversorgung enthält.

Mit der Eingabe der PIN entsteht nun aber ein neues Problem insofern, als sich die Terminals üblicherweise in öffentlich zugänglichen Räumen und Standorten befinden, weshalb nicht ganz ausgeschlossen werden kann, daß der jeweilige Benutzer beim Eintasten seiner PIN beobachtet wird. Aus diesem Grund ist bereits eine sogenannte Super-Chipkarte im Gespräch, bei der die Tastatur und das Anzeigefeld auf der Karte selbst vorgesehen sind. Dies hätte den Vorteil, daß der Karteninhaber die Eingabe seiner PIN und gegebenenfalls weiterer

Daten abseits des Terminals direkt auf der Karte durchführen könnte, ohne Gefahr zu laufen, dabei beobachtet zu werden. Bei Verwendung einer derart "vorbereiteten" Chipkarte könnte dann alles weitere mit einem relativ einfachen Terminal realisiert werden. Der Gebrauch der Super-Chipkarte setzt allerdings voraus, daß in der Chipkarte zusätzlich eine Spannungsquelle integriert sein muß, was wegen der zu großen Bauhöhe verfügbarer Batterien derzeit noch auf erhebliche Probleme stößt.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Chipkartenkonzept zu entwickeln, das die Vorteile der Super-Chipkarte voll nutzen kann, ohne die Schwierigkeiten mit der Stromversorgung in Kauf nehmen zu müssen.

Diese Aufgabe wird ausgehend von einer Bedieneinheit für Chipkarten der eingangs genannten Art durch die Merkmale des Anspruchs 1 gelöst. Der Vorteil einer derartigen Bedieneinheit besteht darin, daß die Super-Chipkarte praktisch in zwei Einheiten unterteilt wird, nämlich zum einen in eine normale Chipkarte und zum anderen in einen Adapter in Form der Einstecktasche, in dem die Tastatur, das Anzeigefeld und die Batterie zur Stromversorgung untergebracht sind.

Im folgenden wird ein Ausführungsbeispiel der Neuerung anhand der Zeichnung näher erläutert.

Die Figur zeigt im rechten Teil eine übliche Chipkarte **1** mit einem integrierten Chip **2**. Diese Chipkarte **1** ist in Pfeilrichtung in eine Bedieneinheit **3** einsteckbar, die als Einstecktasche mit seitlichem Einsteckschlitz **4** ausgebildet ist. Auf der Deckfläche der Bedieneinheit **3** befindet sich eine Tastatur **5** und eine Anzeigeeinheit **6**. Außerdem enthält die Bedieneinheit **3** eine im Innenraum angeordnete Kontaktiereinrichtung **7** für den Chip **2** sowie eine Flachbatterie **8**. Anstelle einer Flachbatterie kann auch eine Solarzelle auf der Deckfläche vorgesehen werden. Mit einer derart ausgebildeten Bedieneinheit, die nur geringfügig größere Abmessungen aufweist als die Chipkarte und deshalb zusammen mit dieser leicht transportiert und aufbewahrt werden kann, ist eine vorgezogene PIN-Überprüfung unabhängig und abseits vom eigentlichen Chipkartenleser möglich mit dem Vorteil, daß die Eintastung der PIN unbemerkt von Dritten durchführbar ist. Anschließend wird die Chipkarte **1** aus der Bedieneinheit **3** gezogen und in den eigentlichen Chipkartenleser am Terminal eingesteckt. Für den Fall, daß der unmittelbare Zugang zum Chipkartenleser nicht möglich sein sollte, ist zur Sicherheit zusätzlich vorgesehen, daß der durch den PIN-Vergleich frei gewordene Zugang zum Chip nach einer vorgegebenen Zeitspanne wieder gesperrt wird. Zu diesem Zweck ist in der Chipkarte eine Sperre vorgesehen, die beispielsweise durch ein Zeitglied gesteuert wird und nach Ablauf einer vorgegebenen Zeit eine Zugangssperre zu den Speicherbereichen des Chips bewirkt.

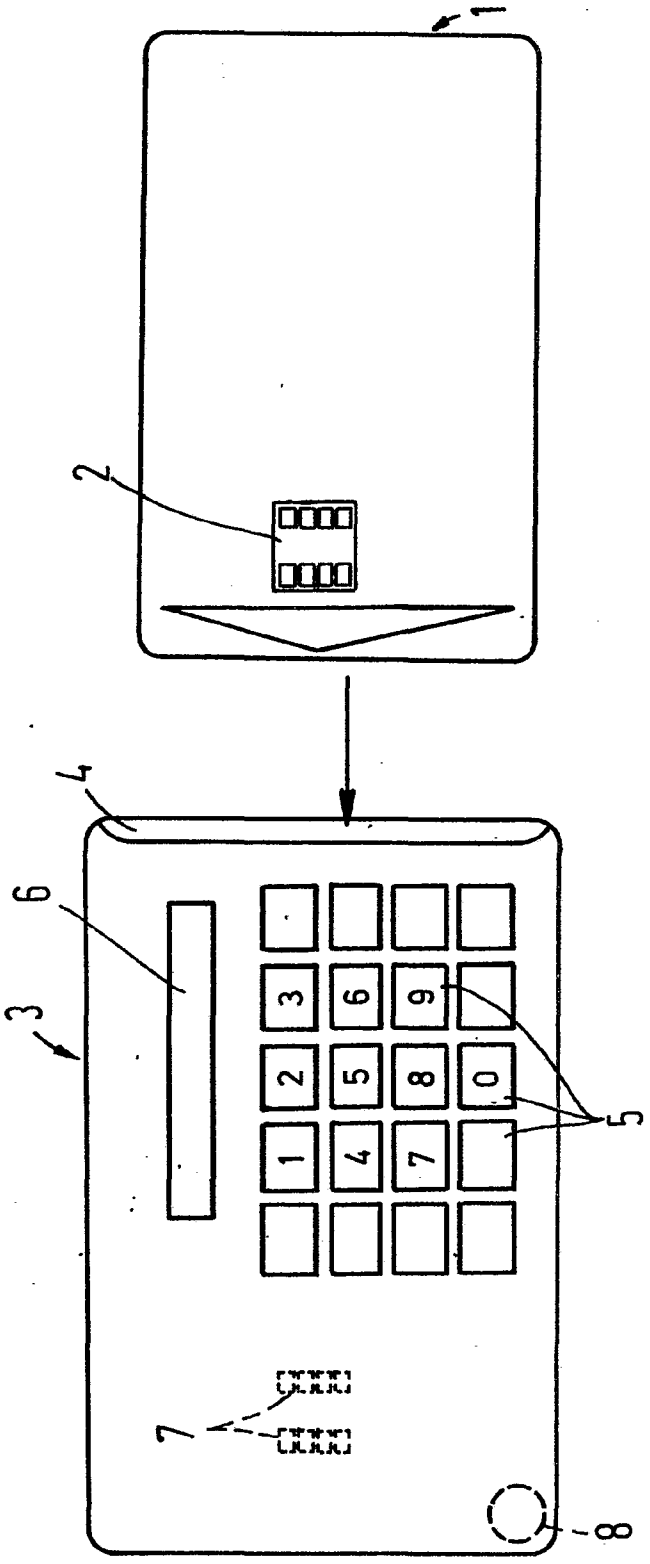
ORIGINAL INSPECTED

– Leerseite –

Nummer: 36 32 294
Int. Cl.4: G 06 K 19/00
Anmeldetag: 23. September 1986
Offenlegungstag: 7. April 1988

86 P 1637 DE

3632294



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 818 757 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
14.01.1998 Bulletin 1998/03

(21) Application number: **97111858.3**

(22) Date of filing: **11.07.1997**

(51) Int. Cl.[6]: **G07C 9/00**, G07F 7/10, G07F 19/00, H04L 9/32, H04M 3/38

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **12.07.1996 US 678908**

(71) Applicant: **AT&T Corp.**
New York, NY 10013-2412 (US)

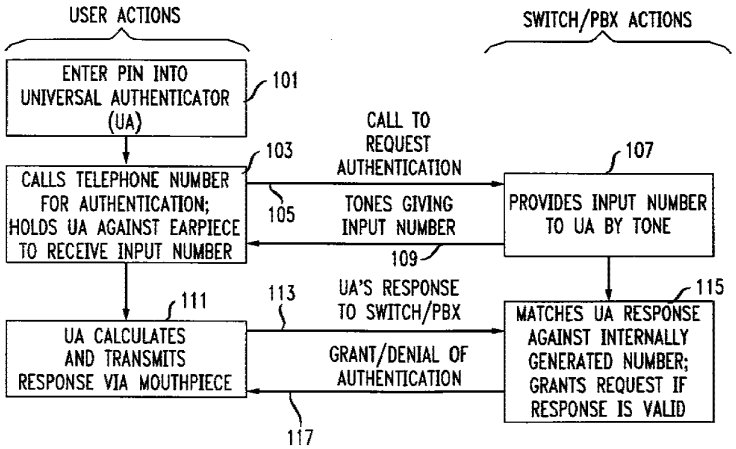
(72) Inventors:
- **Hazra, Amitava**
  Holmdel, New Jersey 07733 (US)
- **Wilkes, Joseph E.**
  Red Bank, New Jersey 07701 (US)

(74) Representative:
KUHNEN, WACKER & PARTNER
Alois-Steinecker-Strasse 22
85354 Freising (DE)

(54) Universal Authentication device for use over telephone lines

(57) A method is provided for securely transmitting information from a telephone to a calling party over a telephone network. In accordance with the method, encrypted audio signals are received from the telephone over a communication path to an authentication mechanism that may be located in the telephone network. The communication path is then disabled by placing the telephone is a hold state. The encrypted audio signals are decrypted to yield decrypted audio signals. The decrypted audio signals are transmitted to the calling party while the communication path is disabled. Finally, a communication path is enabled from the telephone to the calling party subsequent to transmitting the decrypted audio signals. This method provides a high degree of security since the communication path between the user and the authentication mechanism is disabled when the decrypted message is transmitted to the called party. Accordingly, if a party were to intercept the communication path between the user and the authentication mechanism (such as a listener using a receiver to intercept a wireless telephone transmission), the party could not intercept the decrypted message.

FIG. 1



EP 0 818 757 A2

Description

Technical Field

This invention relates to authentication arrangements for telecommunications systems users.

Background of the Invention

Telephone calling card fraud and fraudulent use of corporate PBXs currently costs consumers over a billion dollars a year. In a typical arrangement, callers to the PBX use an 800 number to get access to the PBX. Their authenticity is verified by asking them to dial a multi-digit digit access code, which, if authentic, gives these people access via the PBX to a second dial tone. The caller can then place any outgoing call not denied to normal users within the PBX. Clearly, anyone who can obtain the 800 number and the access code can then place calls that are charged to the PBX. More generally, the present calling card arrangements are also subject to extensive fraud through the use of stolen cards or through the interception by audio taps or visual observation of a calling card number. Computer "hackers" are particularly active in using their computers to access corporate PBXs and determine valid access codes by trial and error. They then sell these codes along with the PBX telephone numbers to "resellers" who resell these to numerous fraudulent users. This vastly magnifies the scope of the fraud. Similar problems arise when a caller transmits private information such as a credit card or social security number. Private information can be readily intercepted in the same manner in which access codes are fraudulently obtained.

U.S. Patent No. 5,406,619 relates to a universal authentication (UA) device that can be used over any phone line to authenticate the use of calling cards, private corporate PBXs etc. The authentication device provides unique signals that authenticate its user. The authentication device is used in lieu of a calling card and is equipped with hardware to allow a query-response type of authentication scheme to be used or to provide the data of a query and the response to that data. In any case, the authentication message (response) sent by the device will be different for successive authentication requests. The UA includes an audio interface (tone generation and reception) which allows the device to communicate directly with the telephone using tone signals and frees the user from manual keying in of codes. However, since the authentication message sent by the UA device is in an encrypted format, the technique disclosed in this patent cannot be used to transmit private information to a called party, unless, of course, the called party can decrypt the message. Thus, a problem exists in that there is no inexpensive and convenient arrangement for permitting users of ordinary telephone lines or wireless systems to transmit private information with a relatively high degree of security and which does not require decryption by the called party.

Summary of the Invention

The present invention provides a method for securely transmitting information from a telephone to a calling party over a telephone network. In accordance with the method, encrypted audio signals are received from the telephone over a communication path to an authentication mechanism that may be located in the telephone network. The communication path is then disabled by placing the telephone is a hold state. The encrypted audio signals are decrypted to yield decrypted audio signals. The decrypted audio signals are transmitted to the calling party while the communication path is disabled. Finally, a communication path is enabled from the telephone to the calling party subsequent to transmitting the decrypted audio signals. This method provides a high degree of security since the communication path between the user and the authentication mechanism is disabled when the decrypted message is transmitted to the called party. Accordingly, if a party were to intercept the communication path between the user and the authentication mechanism (such as a listener using a receiver to intercept a wireless telephone transmission), the party could not intercept the decrypted message.

Brief Description of the Drawings

FIG. 1 is a block diagram of one scenario for authentication in accordance with the present invention.

FIG. 2 shows one embodiment of the UA constructed in accordance with the present invention that can be easily mounted to and removed from a cellular telephone.

FIG. 3 shows a perspective view of an exemplary portable cellular telephone to which the UA shown in FIG. 2 may be mounted.

FIG. 4 shows the UA and telephone positioned inside a sleeve.

FIG. 5 shows the external appearance of one embodiment of the UA.

FIG. 6 is an overall block diagram of the operation of the universal authenticator.

FIG. 7 shows the internals of the UA.

Detailed Description

A Universal Authenticator (UA) is a card-sized device that is equipped with computational hardware to implement a action mapping queries into responses, a keypad to enter input, an LCD display and an audio interface which can receive input and provide output in the form of tones transmittable via a telephone handset over a customer line to a switching system. The object of implementing a function mapping queries (a first number) into responses (part of a second number) is to

IPR2025-00645 Page 00053

create time varying responses, based on time varying queries, so that an interception of one query-response couple will not be useful at a later time. It also has the magnetic bar information currently on calling cards so that it can also be used at the special stations already provided for calling cards as well as from any other phone. Two different devices provided to two different users picked at random, will almost certainly use different functions to generate responses. It should be noted that the device is significantly different from the AT&T SMART CARD Registered TM and other smart cards which can only be used from special stations. (This is discussed in detail later). Time varying authentication messages may be produced by three different methods. The first method is to use a challenge-response scheme-that is, to let the system at the far end provide a random number to the authentication device, which then computes an appropriate response and transmits it back to the system. The other method is to use the Time of Day as input to a function, and transmit the output of the function as well as the Time of Day used, to the system at the far end. The third method is to use a monotonically increasing or decreasing function, such as a count which is incremented with each use. The first method is described in detail in the following paragraphs. The second and third methods are briefly described later.

USE OF UNIVERSAL AUTHENTICATOR

A procedure for using this device for corporate PBX authentication is as follows. Each legitimate user is assigned a Personal Identification Number (PIN) which is also associated with the particular UA provided to him or her. Before seeking authentication the user enters his/her PIN into the UA to activate it. The UA will only be activated and ready for use if the PIN is correct. Next, the user dials a phone number (printed on the UA if desirable) to seek authentication (as done currently with corporate PBXs). A voiced response directs the user to place the activated UA close to the earpiece of the calling telephone station and enable it to receive incoming tones from the earpiece. The authentication system then sends a set of tones representing a random number which is received by the audio interface of the UA. This is the query number. The UA then produces an output number as an appropriate response to the query number and flashes a message to the user to place the UA on the mouthpiece and hit the key to start transmission. The UA sends the set of tones representing the output that it has produced. The system matches the response against an output that it generates internally, and authenticates the request if there is a match. The overall scenario of operation is shown in FIG. 1.

The user has the option, the only option available in some presently available authentication devices, of manually keying in the number to the UA and dialing the response back to the system manually. In this case a voiced response from the system provides the user with a random number to enter into the UA. Once this is keyed into the UA by the user, the UA produces a corresponding output number on its display. This is entered by the user (using a telephone dual tone multi-frequency (DTMF) keyboard if provided or using voice if a speech-recognizing system is supported) to seek authentication. Alternatively, and preferably, the user may request the UA to transmit the tones representing the output number.

APPEARANCE AND INTERNALS

FIG. 5 shows the external appearance of the UA. The external appearance of the device is similar to a smart card except that it has an audio interface to allow it to communicate using an ordinary telephone station. The keypad allows entry of the PIN or manual entry of the input random number (if the user so chooses). The LCD displays the number entered. After computation of the response, the response number is also displayed. The LED flashes to indicate that computation is complete. The key in the notch on the edge is for enabling the audio reception/transmission and is convenient when the user has to hold the UA flat against the earpiece or mouthpiece.

A magnetic bar code on the device allows it to be used from a calling card reader station as well. In this case, only the encoded identification is transmitted, so that authentication is much less secure.

FIG. 2 shows one embodiment of the UA that can be easily mounted to and removed from a cellular telephone so that the caller does not need to physically handle the device during initiation of a call. This feature may be advantageously employed in cellular telephones located in automobiles, for example, where the caller may have particular difficulty in placing the UA against the earpiece and where for security reasons it is desirable to remove the UA from the cellular telephone when not in use. FIG. 3 shows a perspective view of an exemplary portable cellular telephone to which the UA shown in FIG. 2 may be mounted. The telephone has a front operational face with a push button area 11 and display screen 12 disposed between an earpiece 13 and mouthpiece 14. The telephone has a smooth back face (not shown), an upper end wall 23 from which a collapsible antenna 15 extends, a pair of opposed side walls 24 and 25 with a bank of connector holes 16 formed in one such wall, and a bottom end wall containing a jack recess (not shown).

In accordance with the embodiment of the present invention shown in FIG. 2, a pair of speakers is disposed lateral to the plane of the UA so that when the UA is placed adjacent to the back face of the cellular telephone, the speakers will be situated along the side walls 24 and 25 of the telephone in proximity to the earpiece 13. The UA may be conveniently coupled to the telephone with a sleeve fabricated from elastic material.

IPR2025-00645 Page 00054

The UA, with its speakers, are positioned inside the sleeve and the telephone is then inserted through the sleeve, as shown in FIG. 4. The sleeve 27 may have one or more cut-outs to expose the display 12, push button area 11, earpiece 13 and mouthpiece 14. The elastic material forming the sleeve is sufficiently flexible to fit around a wide variety of cellular telephone configurations. The sleeve is configured so that it does not interfere with either the antenna 15 or the recharging process. The position of the sleeve along the length of the telephone may be varied to properly accommodate the features of any particular telephone design.

The design of the UA shown in FIG. 2 may be modified as appropriate to accommodate the requirements of cellular telephones. For example, the UA may be provided with a sliding, spring-loaded activation switch instead of a push-button switch to minimize the likelihood of accidental activation. In operation, the UA may advantageously employ a simple authentication procedure such as by employing a monotonically increasing or decreasing function. For example, in one simple authentication procedure, which is discussed below, the UA counts the total number of previous authentications and the authentication system only accepts the authentication if the count transmitted by the UA exceeds the last authenticated count. The use of this authentication procedure eliminates the need to enter numbers into the UA and hence no keyboard is needed. The internals of the device are shown in FIG. 7. Entry from the keypad is done either when entering the PIN or if manual mode of entering the input number is chosen. Depending on the operation, the entry from the keypad is gated to either a PIN entry register or a MUX The content of the PIN entry register is compared with the content of a stored PIN register and in case of a match, the compute/table lookup unit of the microprocessor (for generating the response) is enabled for subsequent operation. When the user enables the tone detection (by using the key in the notch) the received tones (from the receiver) are converted into bits which are sent to the MUX. The MUX allows the choice of automatic mode (through the audio interface) or manual mode (through the keypad) of input entry. The entry selected by the MUX is entered into the input shift register and subsequently provided to the compute/table lookup unit. On completion of response computation, the response is provided to both the output display register and the output shift register. The output display register allows the response output to be displayed in the LCD The content of the output shift register is provided to the tone generator when the user enables it (by clicking the key in the edge notch a second time) and the tone generator converts the output to tones which are transmitted by the transmitter.

FIG. 1 is a block diagram of the scenario for authentication. The user enters a PIN into a universal authenticator (action block 101). This primes the universal authenticator for later use. The user then calls a telephone number for the authentication service and holds the UA against the earpiece of the telephone instrument to receive an input number, generally a random number generated by the authentication system. The call is set up (arrow 105) to the authentication system and the authentication system which is generally either a switching system (switch) or a PBX provides a random number to the UA by means of tone signals. These tone signals are transmitted to the UA (arrow 109) and are received via the earpiece of the handset of the telephone instrument The UA then calculates the response and transmits a response via the mouthpiece of the subscriber handset. This response is transmitted to the authentication system (arrow 113) which matches the UA response against an internally generated number and grants the request if the response is valid (action block 115). The authentication system then transmits back to the user a grant or denial of the authentication (arrow 117) after which the user can make a telephone call or otherwise take advantage of the positive authentication. With the universal authenticator described herein, it is also possible to use keyboard entry into the UA instead of listening to tones and to inform the user of the random number through a voiced response from the authentication system. Similarly, it is also possible for the user to transmit a response to the authentication system by keying in the response using a dual tone multifrequency (DTMF) keypad of the user's telephone instrument. Further, in an alternative configuration, the UA itself supplies the input number. With this configuration, block 107 and arrow 109 are not used and the UA instead of receiving the input number generates the input number internally within block 103. The response in this case must include the input number to permit the authentication system to authenticate the "response" number from the same input number that was used by the UA.

FIG. 5 is a physical diagram of the universal authenticator 301. It includes an audio interface 303 comprising a microphone for receiving signals from a telephone connection and a speaker for transmitting signals to a telephone connection. The computing hardware 305 inside the UA is shown by a dashed line since it cannot be seen from the outside of the UA. The UA also has a keyboard 307 which has the 12 DTMF keys and a reset bar 309 for resetting the UA. Also shown are an LCD display 311 of numbers received or generated by the UA and a key 313 in a notch on the edge of the UA. A magnetic code bar 315 is also attached to the outside of the UA so that the UA can be read by conventional credit readers. Additional details concerning the internals of the UA and its operation may be found in U.S. Patent No. 5,406,619.

FIG. 6 is an overall block diagram of the operation of the universal authenticator. The circled numbers represent successive steps and have been placed on the diagram to help the reader follow the progress of the process. The two main blocks in dashed lines are the universal authenticator 301 and the authentication sys-

IPR2025-00645 Page 00055

tem 501 which is likely to be a switching system or a PBX. The process starts when the user requests an authentication (action block 503) (It is assumed that the UA is already in the ready state because the user has previously entered a correct PIN.) The request for authentication is performed by dialing a number for a connection to authentication system 501. The completion of the action is represented by arrow 505. The authentication system generates an 8-digit input number (block 507) which number is then transmitted by tones to the UA (arrow 509). The UA receives these tones by being held against the earpiece of the handset from which the user requested the authentication (action block 511). The input number is then transmitted from the tone detector of the UA and is transmitted (arrow 513) to storage 515 for storing the digits representing the input number. (In an alternative arrangement, the input number can be keyed in by the user using keypad 307.) These 8 digits are then passed (arrow 517) to the compute hardware 519 which generates 8 digits of output. These 8 digits of output are combined with an 8-digit identification of the UA (in block 523) to form a 16-digit output consisting of the 8-digit output of the compute hardware and the 8-digit output of the sequence identification. These are stored in the 16 digits of block 525 and are transmitted (arrow 527) from the tone generator 423 via the speaker 439 over the telephone connection to the authentication system 501 They are received and stored in a 16-digit response register 531 which takes the 8-digit UA sequence identifier selected in block 533 and transmits (arrow 535) these digits to the compute hardware. The compute hardware then uses the input number and the UA sequence identifier to compute the 8 digits of output computed by compute hardware 519 of the UA. The computed output is transmitted (arrow 549) to an output register 545 where they are compared (arrow 543) with the 8 output digits received and stored in block 531. If there is a match then authentication is granted and if there is a mismatch authentication is denied. The grant/deny authentication signal 547 is transmitted back to the user and is used to allow the switching system or PBX to accept or reject further calls from that user.

SAFEGUARDS

It is well-known that the query-response method of authentication is superior to a single password or code. (See, for example, W. J. Caelli (ed.): Computer Security In The Age Of Information, pages 223-234, Elsevier Science Publishers, B.V., IFIP, 1989.) In the query-response mode the response (the output number) that is provided by the user is good only for the specific query (input number) presented by the system. An eavesdropper can gain nothing by illegal monitoring of the response because the query presented by the system will almost certainly be something different the next time and will require a completely different response. Typically, a complex function (or a large table, or a combination of function and table) to map queries to responses provides good protection against attempts to breach the security of the system.

The second safeguard is the use of the PIN (possibly 4 digits). This ensures that unless the PIN is known the UA is useless to a thief. Also, the user may preload the PIN in a secluded place (away from public phone booth for example). Finally, once the PIN is entered, the UA can only be used for a limited number of times (say 5) and for a limited amount of time. The PIN must be reentered after that to continue using the UA. This ensures that even if a UA loaded with the valid PIN is stolen, it can be used only a limited number of times. Also, if a user loads a PIN and forgets to use the UA subsequently, an automatic internal timer will erase the PIN after some time, making the UA useless for a thief. Of course, the user is expected to report loss of the UA immediately as with other credit cards, calling cards etc.

Finally, as with most authentication schemes, the authentication system will break the connection after a limited number of retries in case of errors. Thus if the system at the far end receives an incorrect response it will send a different input to allow the user to retry. After a limited number of retries the connection is broken. Reestablishing the connection will of course be delayed by the normal delay in the phone network.

IMPLEMENTATION

The implementation consists of two parts; the implementation of the query-response in software/hardware on the switch/PBX, and the implementation of the program on the UA to determine the output number given an input number. The part to be implemented on the switch, PBX or other telecommunications network element, consists of selection of the input random number, a DTMF output and/or voiced response system to relay the number to the user, reception of the response or digits keyed in by user, and matching of these against the system's own internally generated response. The generation of response can be packaged in a chip to avoid any probing. Within the UA there has to be a similar mechanism for generation of response. This mechanism can be an implementation of a computational algorithm or a table lookup process or a combination of both. The mechanism within the switch/PBX for generation of the matching response must also take into account the identity of the particular UA involved. Two different UAs will almost certainly use different functions for the query-response match. The UA reveals its identity by embedding digits specifying its id number within its output response. The switch/PBX will, with the help of this id, determine the appropriate function to use for checking the response given by the UA.

As indicated earlier the functions mapping queries to responses should be different for different UAs. This may be achieved easily within the UA by having a table

IPR2025-00645 Page 00056

mapping certain inputs to certain outputs. But, this has two serious drawbacks-first the set of inputs is limited thus somewhat compromising security, and secondly at the system end a very large amount of memory will be taken up storing the tables of the many UAs. A solution (from standard encipherment algorithms) is to use a common algorithm for the mapping, but modify the algorithm somewhat for each user by using a different key input for each user. Within the system the sequence id of the UA may be used as an entry into a table to find the key for that UA which can then be provided to the algorithm so that it is suitably modified for the particular UA and can calculate the proper response for the given input. Within the UA the details can be somewhat simpler. Only a specific version of the algorithm has to be implemented. This may be wholly or partially table-driven. FIG. 6 shows some details of the overall scheme involving the UA and of the query-response system on the switch or PBX (assuming the sizes of the initial query number and the UA sequence id to be both 8 digits long). (8 digits each for the query number and the sequence id will provide sufficient protection, and at the same time the total response size to be keyed in by user would be 16 digits. This is comparable to calling card codes currently being used (14 digits).

The UA is a sealed unit which will minimize damage due to moisture, etc. The batteries are sealed in. A low power indicator informs the user that the battery is about to die; the user then has the option of calling in for a replacement UA. Typically, the UA will be replaced every couple of years just like credit cards, calling cards etc. The battery power is adequate to last the anticipated life-time of the UA. A customer provided PIN will be "burnt" into a ROM in the UA before it is provided to the customer. The UA identity and key or other information necessary to control the generation of the response message are also "burnt" into the ROM of the UA. In one preferred implementation, the program is also "burnt" into the ROM, although, alternatively, it could be loaded into RAM after the battery is installed.

Different codes for different services can be used to set the UA to a specific mode of operation for authenticating the use of the desired service. The telephone number to request the authentication for using the specific service has to be called and the query-response process executed as earlier described. The implementation of the UA as well as the overall scheme is feasible with currently available technology.

The authentication service can be provided by telephone switches (such as AT&T's 5ESS Registered TM switch) as a feature. Corporate PBXs can be served by such a switch which will act as a gatekeeper. Once a caller's request to access a PBX is authenticated the caller will be granted access to the PBX by the gatekeeper switch and the PBX will service the caller's requests, so the PBX is not tied up performing repeated authentication for users requesting access. Also, once the system end of the authentication mechanism is available on the telephone network it will become easier to make the UA available for a variety of purposes. The telephone network owner (local telephone company or long distance provider) can then provide authentication as an end to end service-providing both UAs and the authentication service on the network. The UA is not a competitor of the smart card in this respect. While smart cards are usually more computationally powerful and versatile than the proposed UA, they are also more expensive and are restricted by their need for special stations to operate from.

The UA also may be used to transmit private information such as a credit card number. In operation, the user transmits the private information to the network switch/PBX serving as the gatekeeper. The private information is encrypted by the UA using any of the previously mentioned encryption techniques used to encrypt authentication messages. The network gatekeeper subsequently decrypts the private information and temporarily disables the communication path between the user and network by placing the user in a "hold" state in a well known manner. The decrypted information is then forwarded to the called party by the gatekeeper. Since the communication path between the user and the gatekeeper is disabled, a party that intercepts this communication path (such as a listener using a receiver to intercept a wireless telephone transmission) cannot intercept the decrypted message transmitted from the gatekeeper to the called party. That is, the transmission of information from the user to the called party is performed in two distinct steps that are isolated from one another so that both the encrypted and decrypted information cannot be intercepted by a single party receiving one step of the transmission. Once the decrypted information has been transmitted by the network, the communication path between the network and the user is re-established so that communication between the user and the called party can continue in the usual manner.

ALTERNATIVE IMPLEMENTATIONS

It is possible to have a somewhat more rugged and less expensive implementation by not using the standard tones used by DTMF, and instead encoding the audio signals using frequency shift keying with just two frequencies in the audio range (a "high" frequency and a "low" frequency). This is the scheme described, for example, in U.S. Patent 4,823,956, used for incoming caller line identification. In that case the DTMF Tone detector/generator (SSI20C90) will not be needed. Also, instead of a carbon microphone it is possible to use other techniques to pick up the incoming audio. A detector based on an inductor coil (similar to those used in hearing aids) can pick up the electrical signal directly from the phone line (near the earpiece) bypassing the need for a microphone. This will work well in noisy environments. Similarly, instead of an ordinary metal dia-

IPR2025-00645 Page 00057

phragm speaker, a piezo-electric sound generator can be used to generate the outgoing audio. Such piezo-electric devices are physically more rugged than metal diaphragms and are also more compact. They are also less expensive. Them is no need for high fidelity in the audio output because it is only necessary for the far end to determine whether the frequency is "high" or "low". So piezo-electric sound generators which are typically limited to a few frequencies may be quite acceptable. The authenticator device requires the user to execute two actions with the device in order to receive authentication. The user has to first click the receive/transmit key and hold the device against the earpiece to receive the incoming audio signal, and then click the key again and hold the device against the mouthpiece to transmit the outgoing audio signal. A modification to the scheme can reduce the number of user actions needed and make the device easier to use.

By adding a pseudo random signal generator (such as a Pseudo Noise sequence generator) and an internal clock, the device can be itself made to produce the input number. Then there is no need to receive incoming audio signals from the phone line. The user then, has to only hold the device against the mouthpiece and click the transmit key. The Time of Day available from the internal clock will be provided as the seed to the pseudo random signal generator, and the output of this generator will be the input number to the authenticator device. The device will transmit both its internal Time of Day (year, month, day, hour and minute) along with the output number from the computation/table look-up function.

The system at the far end receives the Time of Day from the device and first verifies that it is close (within a threshold) to its own internal Time of Day. If the device's Time of Day is not within the threshold, the far end system (PBX or switch) will ask that the device's clock be synchronized with the far end system's clock before authentication is requested. The check for the consistency of Time of Day is to be done to prevent an eavesdropper from recording a pair-Time of Day and output number-and reusing the pair to gain fraudulent authentication.

If the device's Time of Day is within the acceptable threshold the far end system uses the transmitted Time of Day to generate the input number for authentication, and subsequently the output number, and matches it against the output number received In case of a match, authentication will be granted.

Another alternative, somewhat less safe, is to store a count in the UA, and advance the count with each use. The authentication system also keeps track of the count. The UA transmits both the count and the transformation of the count to the authentication system. The authentication system will then verify the transformation but will only accept the authentication if the transmitted count exceeds the last authenticated count. Advantageously, this arrangement prevents someone who has intercepted a legitimate authentication from simply reusing it, but avoids the necessity for receiving a random number from the authentication system. The term "random" or "pseudo-random" as used herein means that the number is unpredictable, and not that it meets the tests of random numbers such as those found in a random number table. Unpredictability is the key attribute.

Claims

1. Authentication means, characterized by:

means for automatically transmitting audio signals over a voice telephone line, said line connected via a telephone network to an authentication system, said means for transmitting arranged for transmitting by having a user of said authentication means hold said means for transmitting against a microphone of a telephone station while leaving a speaker of said telephone station available for said user of said authentication means to listen;

means for generating a number, independent of any keyed personal identification number, coupled to said means for transmitting, wherein said number is derived from a time-varying quantity and a key unique for said authentication means, and said quantity globally and independently maintained internally in said authentication means and in said authentication system; said number for transmission by said means for transmitting to said authentication system for authenticating an identity of said user of said authentication means; and said number comprising data for identifying said authentication means and comprising no data based on any keyed personal identification data;

means for storing a personal identification number;

a keypad for entry of a personal identification number;

means for enabling said authentication means in response to a match of the stored and entered personal identification numbers, wherein said authentication means is planar and essentially the size of a credit card and said means for transmitting includes a pair of opposing speakers situated in a plane lateral to a plane of the authentication means; and

a sleeve formed from an elastic material in which said authentication means and said pair of speakers are insertable, said sleeve being configured to support said authentication means against a back face of a telephone when said sleeve is enclosed around said authentication means, said sleeve being fur-

IPR2025-00645 Page 00058

ther configured to allow operation of said telephone when enclosed around said authentication means.

2. A method for securely transmitting information from a telephone to a calling party over a telephone network, characterized by the steps of:

receiving encrypted audio signals from the telephone over a communication path to the telephone network;
disabling said communication path by placing said telephone is a hold state;
decrypting said encrypted audio signals into decrypted audio signals;
transmitting said decrypted audio signals to the calling party while said communication path is disabled; and
enabling a communication path from the telephone to the calling party subsequent to transmitting said decrypted audio signals.

3. The authentication means of claim 1 further characterized by a control key, for operation by said user in response to prompting signals received on said speaker of said telephone station, for changing a state of said authentication means.

4. The authentication means of claim 3 characterized in that said control key is used for initiating transmission of said number.

5. The authentication means of claim 1 further characterized by a key for disabling said authentication means.

6. The authentication means of claim 1 further characterized by

timing means for disabling said authentication device after a lapse of a predetermined interval following enablement or use of said authentication means.

7. The authentication means of claim 1 further characterized by clock means for maintaining date and time;

wherein said independently maintained quantity is date and time.

8. The authentication means of claim 1 further characterized by:

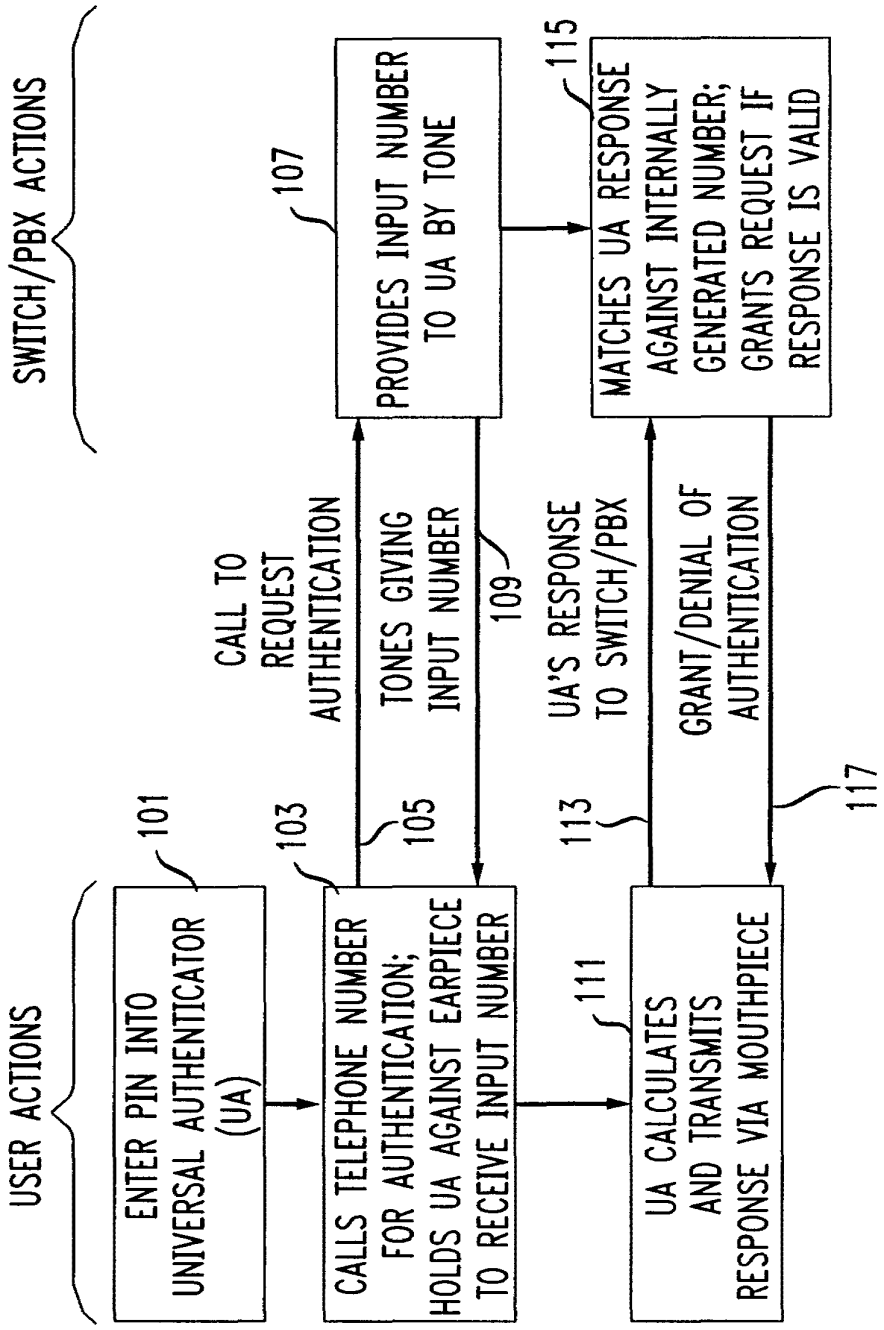
means for displaying said number;
wherein, in noisy surroundings, said user is enabled to key said number into said telephone station, using a keypad of said station.

9. The authentication means of claim 1 further characterized by:

means for storing additional personal identification numbers; and
means for storing additional data corresponding to said additional personal identification numbers;
wherein said means for enabling is also responsive to a match of one of said additional personal identification numbers for enabling said authentication means; and
wherein said means for generating is further responsive to said additional data if said user keys one of said additional personal identification numbers.

IPR2025-00645 Page 00059

FIG. 1



IPR2025-00645 Page 00060

FIG. 2

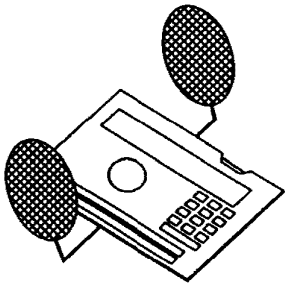
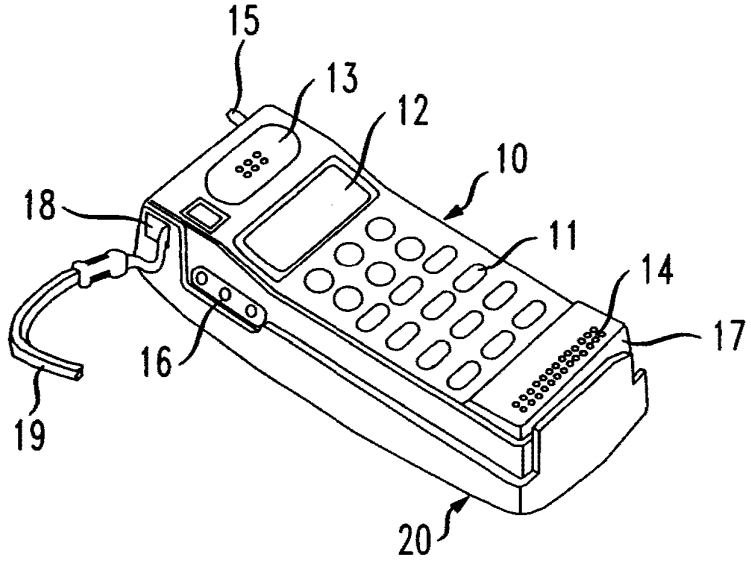


FIG. 3



IPR2025-00645 Page 00061

FIG. 4

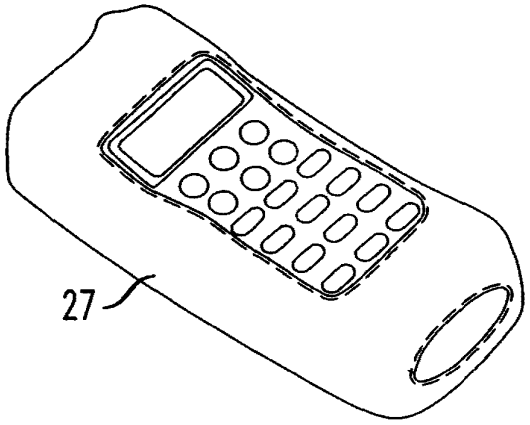
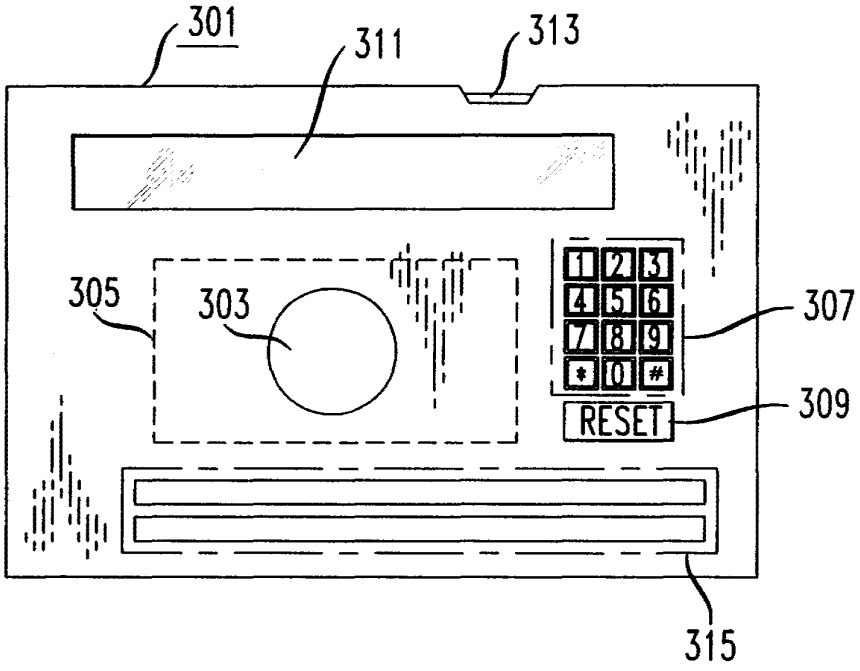
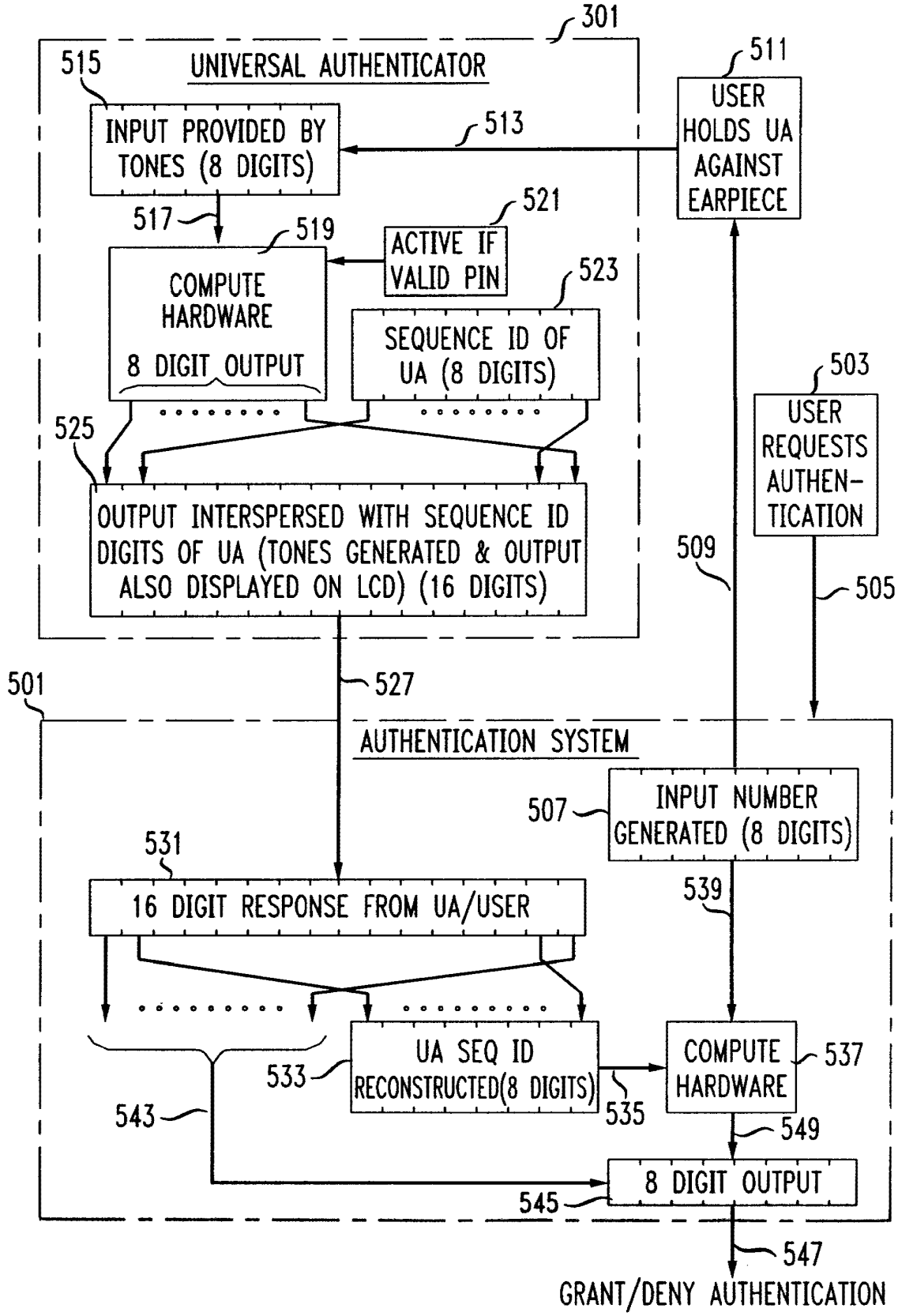


FIG. 5



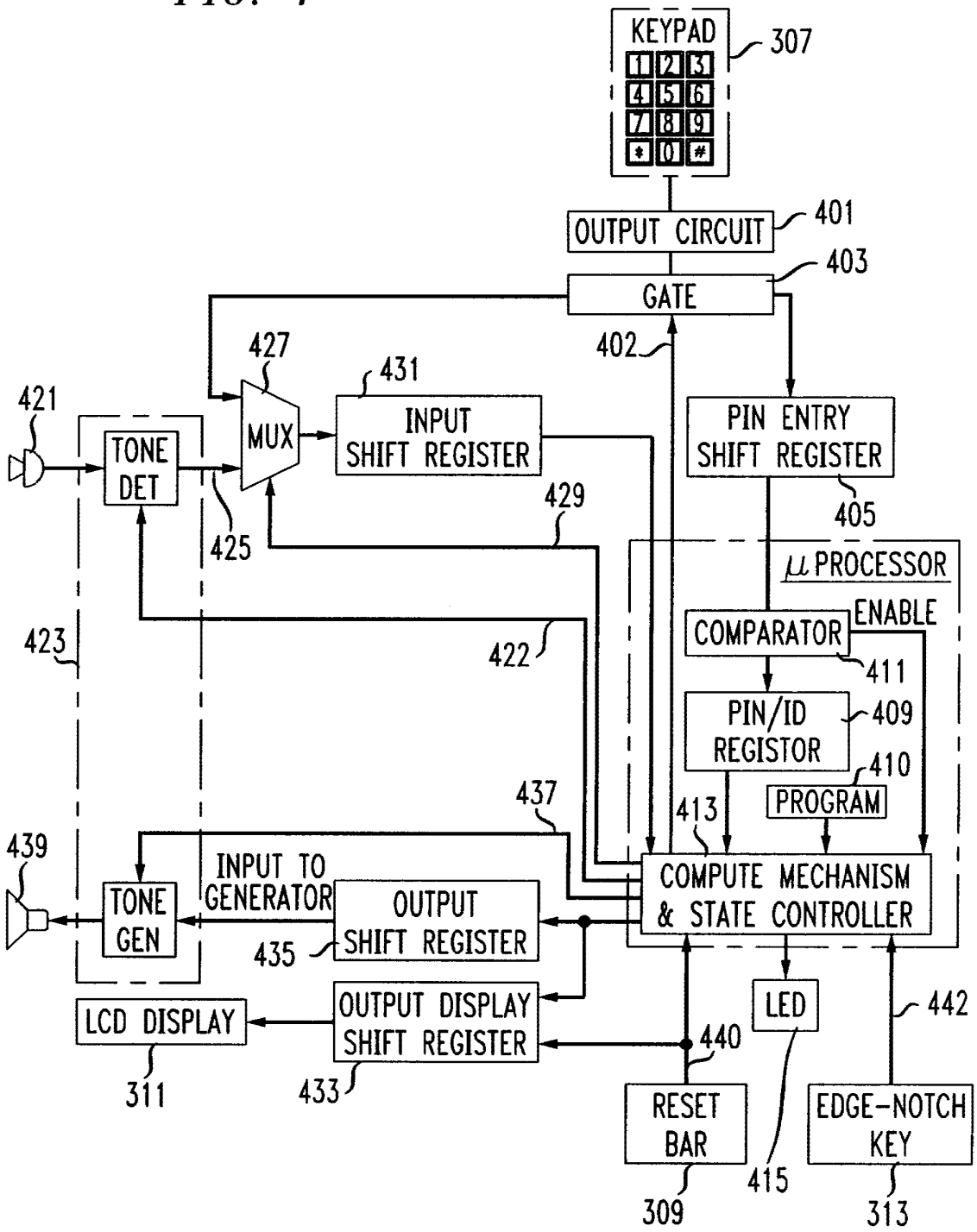
IPR2025-00645 Page 00062

FIG. 6



IPR2025-00645 Page 00063

FIG. 7



IPR2025-00645 Page 00064

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 014 290 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.06.2000 Bulletin 2000/26

(51) Int Cl.[7]: **G06K 7/00**

(21) Application number: **99309450.7**

(22) Date of filing: **26.11.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **26.11.1998 GB 9825937**
29.10.1999 GB 9925675

(71) Applicant: **NOKIA MOBILE PHONES LTD.**
02150 Espoo (FI)

(72) Inventors:
- **Kettunene, Mikko**
  89073 ULm (DE)
- **Buschmann, Ulrich**
  89275 Elchingen (DE)

(74) Representative: **Hibbert, Juliet Jane Grace**
Nokia IPR Department
Nokia (UK) Limited
Summit Avenue
Southwood
Farnborough Hampshire GU14 0NG (GB)

(54) Data card holder and reader therefor

(57) A holder and reader for two or more data cards for a radio communication device, the holder comprising a body having formations for releasably carrying said two or more data cards and being adapted to be removably installed in the data card reader of said device.

EP 1 014 290 A2

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to a holder for a data card and to a reader for reading/writing data from/to the data card. In particular, the present invention relates to a holder for a data card such as a subscriber identity module (SIM) which is designed to be used in conjunction with a reader of a radio communication device for wireless communication with a radio network.

[0002] Data cards take various forms and those used, for example, in cellular devices, may include passive memory cards (i.e. essentially a ROM), or an active processor card (i.e. capable of processing information internally within the card). An example of the latter is a smart card, which has a memory implemented as an integrated circuit in which information is stored. A smart card used extensively in GSM is the subscriber identity module (SIM). GSM specification 11.11 details the structure and functionality of SIM cards, but briefly a SIM card is a user removable module providing storage of subscriber related information. Notably, a SIM contains data fixed during the administration phase (e.g. the International Mobile Subscriber Identity (IMSI) which unambiguously identifies a subscriber, a personal identification number (PIN) to provide protection against unauthorised use), temporary network data (e.g. LAI location area information) and service related data (e.g. language preference, advice of charge). In the proposed Universal Mobile Telecommunications System (UMTS) standard, it is intended to have a User Service Identity Module (USIM) which is an application residing on the IC Card used for accessing UMTS services of a certain Service Provider and much like GSM SIMs shall contain sufficient information to identify the user and the Service Provider.

[0003] In GSM 11.11, two types of SIM cards are specified. The functionality of the SIM is the same for each, it is principally that the physical dimensions are different. One is a credit card size SIM, and the other is a plug in SIM about 15 mm by 20 mm. The rationale behind the different sizes is that the credit card size is perceived as a convenient size for the user from a practical standpoint. The plug-in SIM is intended to be semi-permanently installed in the cellular telephone. For example, in ordinary use, the SIM card could be located and used in a portable radio telephone handset; when the user is planning to travel in his car the SIM card can be removed from the handset and inserted into the radio telephone in the car.

[0004] Often cited problems with swapping the SIM card between different radio communication devices include the inconvenience and the length of time it takes to do so, and also the inherent 'fiddle-factor', i.e. awkwardness of having to manipulate the SIM so as to place it in the SIM reader. Such problems are compounded when a number of SIM cards are to be loaded/unloaded.

[0005] Against this background, an aspect of the present invention resides in a holder for two or more data cards for a radio communication device, the holder comprising a body having formations for releasably carrying said two or more data cards and being adapted to be removably installed in a data card reader of said device.

[0006] In accordance with this aspect of the invention, two or more data cards can be readily loaded in the holder and the holder easily installed in the data reader. This not only avoids the need for a large number of mechanical parts associated with the data reader, but loading/unloading of the data cards is remote from the data card reader and is thus less awkward.

[0007] In a first embodiment, said formations are provided such that the two or more data cards when loaded in the body are carried in an oppositely facing back to back arrangement. Thus providing for economy of space.

[0008] Preferably, said formations are provided in said body by longitudinally extending slots for receiving said two or more data cards, and the body accordingly may include respective apertures for exposing electrical contacts of said data cards when loaded in the body.

[0009] In a second aspect, the present invention provides a radio communication device including a data card reader, the device having a housing defining an aperture associated with the reader and dimensioned to receive a data card holder carrying two or more data cards, the arrangement being such that the data card holder is removable from the reader, and wherein the data card holder is provided with formations for releasably carrying two or more data cards.

[0010] In one arrangement, the data card holder carries said two or more data cards in an oppositely facing arrangement, and the data card reader comprises two or more electrical circuits correspondingly arranged in facing relationship for reading the two or more data cards. In another arrangement, the data card holder carries said two or more data cards in a similarly facing arrangement, and the data card reader comprises one electrical circuit for reading the two or more data cards.

[0011] Optionally, the radio communication device comprises a cover member adapted to be disposed against said housing such that when a data card holder is located in the card reader the cover obstructs retraction of at least one of the two or more data cards.

[0012] Accordingly, two or more data cards can be loaded in the data reader and the cover plate, in a first position, covers one of the cards in the data card reader (or for example two of the cards if the reader contains three data cards) whilst permitting withdrawal of the other data card(s). With the cover member in a second position the data card(s) which were shut off in the first position can be withdrawn from the reader. In terms of the reverse operation of loading the data reader, the cover member in the first position allows uninhibited insertion of one or more data cards into the reader, and in the second position allows insertion of further data cards into the reader into card spaces/areas which were

IPR2025-00645 Page 00066

previously blocked by the cover member.

[0013] In this way, data cards which are temporarily installed in the reader on a frequent basis can be quickly and easily loaded and unloaded from the reader, and data cards which are to be stored on a relatively more permanent basis (but still requiring loading/unloading albeit infrequently) in the reader can be taken out by simply releasing the cover member from the housing.

[0014] Suitably, the cover member is provided with an aperture which when the cover member is disposed in the first position is in alignment with said second data card, thereby allowing retraction thereof. The aperture may be slot in registration with a corresponding slot in the reader having loaded therein the data card.

[0015] Conveniently, the data card holder is provided with longitudinally extending slots for receiving said two or more data cards, and the cover member is provided with one or more slots which when the cover member is disposed against said housing are in alignment with one or more of the openings of the longitudinally extending slots of the data card holder.

[0016] Advantageously, the radio communication device comprises ejector means arranged to urge the installed data card holder such that on removal of the cover member at least a portion of the data card holder is urged to project through the aperture.

[0017] Alternatively, the data card holder and reader are provided with a latching mechanism therebetween that allows the data card holder to be pressed into the reader for connection and then pressed in again for disconnection. This consequently eliminates the need for a separate ejector button and associated componentry to release the holder from the reader. The latching releasably connecting together the holder and reader, the holder having a longitudinal axis indicative of a longitudinal direction and being adapted to be received in the reader, and the latching mechanism being engagable in a latched condition connecting together the holder and reader by pressing the holder in the longitudinal direction into the reader, and being disengagable from the latched condition to release the holder and reader by pressing the holder into the reader in the longitudinal direction, the latching mechanism comprising

a first element having a lateral deflecting surface and detent and being associated with one of the holder or the reader, the lateral deflecting surface being inclined to the longitudinal axis,

a second element associated with the other of the holder or reader, and resilient means operative on pressing the holder into the reader to urge the holder and reader longitudinally apart, and to effect relative bias in a transverse direction to the longitudinal direction between the first element and the second element,

such that on pressing the holder into the reader for connection, the first and second elements and the resilient means cooperate so as to engage the second element with the detent in the latched condition, and on pressing the holder into the reader for release, the first element disengages from the detent and the resilient means operates to urge at least a portion of the holder from the reader for removal thereof.

[0018] The present invention will now be described by way of example with reference to the following drawings in which:

Figure 1 shows an exploded perspective view of a radio communication device including a holder in accordance with one embodiment of the present invention;

Figure 2 shows a close-up of the holder of Figure 1;

Figure 3 shows the device of Figures 1 and 2 including ejector systems;

Figures 4a and 4b show a radio communication device of the first embodiment in which a cover member is in the first position allowing retraction of a data card;

Figure 5 shows a perspective view of a radio communication device in a holder in accordance with a second embodiment of the present invention;

Figure 6 shows the underside of a holder of Figure 5;

Figure 7 shows an element of the holder of the second embodiment;

Figure 8 and 9 show a data card reader of the second embodiment;

Figures 10a and 10b show schematic side and underneath views of the reader of Figures 8 and 9;

Figures 11a to 11j show a series of configurations of elements of the latch mechanism of the second embodiment.

[0019] Referring initially to Figure 1, there is shown a first embodiment of a holder and a radio communication device of the present invention. In this embodiment, the radio communication device is a unit 10 that is mountable for instance in a car or other motor vehicle, and provided in the unit is a data card reader 18.

[0020] As is apparent from Figure 1, the unit 10 is a generally rectangular box shape housing consisting of top and bottom cover plates 12, 14, connected, when assembled, by four rectangularly arranged side walls 16. The unit is provided with the data card reader generally denoted 18. The front wall of the unit has a rec-

IPR2025-00645 Page 00067

tangular aperture 20, which internally leads into the data reader 18. The data card reader 18 comprises two printed circuit boards 22, 24 for reading inserted data cards. The two printed circuit boards 22, 24 carrying the usual reading electrical circuitry including contacts are arranged substantially parallel in a mutually facing configuration.

[0021] Turning to the data card holder 26, which is shown in more detail in Figures 2 and 3, it is a generally rectangular cartridge 26 designed to carry two data cards. The cartridge 26 is dimensioned to be inserted into, and removed from, the data reader 18 through the aperture 20 in the unit. As can be seen from Figure 2, the cartridge 26 is provided with two slotted openings 28, 30 which extend longitudinally into the cartridge 26 thereby providing flat cavities for receiving respective data cards. As shown, the flat cavities are arranged in the cartridge 26 with the plane of their major faces one on top of the other and separated by a separation wall 32. The cartridge 26 is further provided with contact windows 34 in its major faces, each contact window opening into respective flat cavities for receiving respective data cards.

[0022] To insert a data card into the holder, it is introduced into one of the slotted openings 28, 30 and then slid further into the flat cavity. Care should be taken to ensure that the data card is inserted such that once in the cartridge, the electrical contact areas of the data card are exposed through the contact window 34. To facilitate this, guide grooves or such like are provided in the cartridge. When the cartridge is loaded with two data cards they are so arranged that their electrical contact areas face oppositely outwards through respective contact windows 34 of the cartridge 26.

[0023] Cartridge 26 carrying the two data cards can then be loaded into the data card reader 18 by introducing the cartridge to the aperture 20 in the front wall of the unit 10 and pressing the cartridge through the aperture 20 into the reader.

[0024] When the cartridge is inserted into the data reader 18 of the unit 10, the electrical contact areas of the data cards are brought into registration and electrical contact with the electrical contacts of the two facing reader printed circuits boards 22, 24.

[0025] Mechanical means for holding the holder in place in the reader may conveniently be provided.

[0026] Also shown in Figure 1 and in more detail in Figure 2, is a front cover panel 36 associated with the housing of the unit 10. The front panel 36 is adapted to be fixed to the front wall of the unit 10 presenting the data reader aperture 20 by any appropriate mechanical means such as screws or catches or a hinged connection. In the major face of the front panel 36 there is provided a slot 38 and this is positioned so that when a data card holder 26 is present in the data reader the slot 38 is in alignment with one of the slotted apertures 28 of the data holder. In this way, the data card holder 26 can be semi-permanently installed in the data reader and still there would be immediate access to a data card loaded in the reader, as shown in Figures 4a and 4b.

[0027] It may be that the data card holder is subject to an ejecting force when located in the data reader provided by a convenient ejector means 40 (see Figure 3). When the front panel is removed the ejector means 40 would push at least a portion of the length of the data card holder out from the aperture 20 of the unit.

[0028] The arrangement is such that in an embodiment without an ejector system being associated with the data card reader, the trailing end of the inserted data card projects out from the unit and the slotted aperture of the cover panel 36 so that the user can easily grasp it and pull it out. Alternatively with an ejector mechanism, activation of the mechanism (for instance by pressing a release button) would cause projection of the trailing end of the data card. Release of the cover panel 36 allows access to the other slotted aperture of the holder and data card therein previously blocked. Again either by means of ejector mechanism activation or spring biasing.

[0029] A second embodiment of the invention is shown in Figures 5 to 11, in which the data card holder is designated 100 and the part of the radio communication unit including the data card reader is designated 200.

[0030] Referring to Figures 5 and 6, in this embodiment, the data card holder 100 is a generally flat rectangularly shaped module being defined by an upper wall 102 extending rearwardly into a cantilever tail portion 104, two side walls 106, 108 depending from the two longitudinal sides of the upper wall 102, and a front wall 110 presenting a front face. For part of its base 111 the data card module 100 has a door 112 depending from and hinged at the rear end of the module so that it hinges open downwardly. A first data card 113, such as the user SIM, can be installed into the module from generally the forward end by inserting it into a sleeve 114 provided in the door 112. The user SIM is inserted so that electrical contacts thereon face downwardly and thus are exposed through a window 116 provided in the lower wall of the door. Extending upwardly from the two opposite side walls of the door 112 are a pair of resilient closure hooks 118 which are designed to cooperate with the complementary recesses 120 provided in the side walls 106, 108 of the module so as to keep the door 112 shut when it is closed. Release of the door 112 to access the user SIM can be effected simply by urging the closure hooks 118 slightly outwards so as to free them from respective recesses 120, thereby allowing the door 112 to be swung open.

[0031] As in the previously described first embodiment, the data card holder of the second embodiment is adapted to carry a second data card 122 such as a SMART Card which may be a further memory card. The second data card in this embodiment is inserted from the rear end of the module, and for receiving the second data card the rear end of the module is open, ie there is

IPR2025-00645 Page 00068

no wall to the module at this end the upper wall, side walls and the base of the module defining a slot 124 for receiving the second data card. Accordingly, the leading edge of the second data card 122 is inserted into the slot 124 in the rear end of the module and the card 122 is then continued to be slid further into the module. As the body of the second card 122 is being slid into the module the top surface of the card 122 abuts and brushes against a lip 125 which depends from the back end of the tail 104. Due to the top surface of the second card 122 pushing against the lip 125, the tail 104 of the module deflects upwardly slightly owing to its inherent flexibility because of the absence of any surrounding supporting walls. Once the second data card 122 has been fully inserted into the slot, the leading edge thereof being stopped by an internal wall of the module, the trailing edge of the second data card 122 locates against the lip 125 of the tail 104 which accordingly has deflected downwards so as to hold the trailing edge of the second data card 122 securely in position in the module, as shown by the discontinuous lines in Figure 6. Electrical contact points 123 of the second data card are provided on the exposed portion of the data card and face downwardly.

[0032] Disposed at the front end of the module is a compartment 126 defined by the front wall, the upper wall, the two side walls, an internal wall and the base. This compartment houses a sprung peg member 128 that protrudes through a slot 130 in the base. The sprung peg member 128 is illustrated in shadow lines in Figures 5 and 6 and more clearly in Figure 7.

[0033] Referring to Figure 7, the sprung peg member 128 consists of a pin head 132 projecting from and at right angles to the plane of a generally serpentine spring portion 134 that extends from a side wall 136 having connection elements 138 for attaching the side wall 136 with the sprung peg member 128 to the module. Resilience is afforded to the pin head 132 by the serpentine configuration of the spring portion 134. As already mentioned, the pin head 132 protrudes from the slot 130 in the base of the compartment 126, the slot extending transversely to the longitudinal axis of the module. In its normal position the pin head 132 is pressed against the end wall 138 of the slot 130, and is so biased by the spring portion 134 that movement away from the end wall 138 causes the pin head 132 to be urged towards the wall 138. The function of the sprung peg member 128 will become more apparent later.

[0034] Turning to the data card reader 200, in Figure 5 the data card reader is shown with an attached fascia plate 202, and in Figure 8 is shown with the fascia plate removed. The fascia plate 202 provides a slotted aperture 204 for receiving the data card module 100. Further, there is a small cut-out 206 from the bottom edge of the slot 204 for allowing entry of the pin head 132 of the sprung peg member 128 past the fascia 202.

[0035] Referring to Figure 8, the data card reader 200 comprises a frame 210 mounted on a PCB 212. The PCB carries two sets of electrical contacts for registering with respective electrical contacts of the two data cards in the module. The arrangement is such that when the module carrying two data cards is loaded into the reader the electrical contacts of the data cards both face downwardly and come into registration with the upwardly facing electrcial contacts on the PCB. Accordingly, only one PCB is required and the arrangement provides efficient use of space.

[0036] The frame 210 is constructed from wall members consisting of two opposite side walls, a cross bar, back wall and base, so that the frame defines a chamber for receiving the data card module 100. A slider 214 is mounted across the two side walls of the frame and is slidably mounted in relation to the frame on a pair of tracks 216 extending laterally outwards from the frame. These slidingly engage with corresponding channels 218 formed in the side walls of the slider 214. The slider 214 is biased towards the front of the data card reader by a spring 238 (Fig 9). More details of spring 238 are given below. The undersurface of the slider is provided with a pair of ramps terminating in small feet which are designed to catch the leading edge of the second data card when the data card module is entered into the data card reader. The ramps serve to gradually push down on the second data card so that its electrical contacts make a good contact with the corresponding contacts on the PCB.

[0037] Extending forwardly from the front of the frame are a pair of oppositely facing arms 220. Spanning the two arms 220 is a shaft 222 which is journalled in circular holes 224 provided in the lower portions of the arms 220. The journalling of the shaft 222 with respect to the circular holes 224 is such that the shaft can rotate about its axis, and furthermore can slide laterally in the holes 224 from side to side. Rigidly fixed to the shaft 222 and extending a major part of the length thereof is a flap 226 which is therefore also able to rotate with the shaft 222 about its axis and move laterally with it. To the right side of the front face of the flap 226 there is provided a relief pattern 228. The relief pattern 228 is a formation which projects outwards from the face of the flap 226, and the front face of the relief pattern 228 is in a plane substantially parallel to that of the front face of the flap 226.

[0038] The relief pattern 228 consists of an upper raised formation 230 in the form of a lug, and a lower raised formation 232 in the form of a substantially 'V' shaped wedge. Defined between the upper and lower raised formations is a guideway 234. The two sides of the lower raised formation taper decreasingly downwards, with the right side having a greater degree of inclination than the left side. Just at its bottom edge, the lower raised formation is bevelled inwardly 236. The function of the relief pattern will be described later.

[0039] In Figure 8 the flap 226 is shown as being disposed in the vertical plane and is resiliently biased about the shaft axis so that unless deflected it always takes up a vertical orientation. The flap 226 whilst being able

IPR2025-00645 Page 00069

to slide from side to side in holes 224 is also resiliently biased laterally towards the right side in Figure 8 such that the right vertical side wall of the flap abuts the right arm of the frame of the data card reader. The rotational resilient bias and the lateral resilient bias can be provided by one or more springs. However in the preferred form of this embodiment these two biases together with the forward bias on the side 214 are exerted by one and the same spring, that is spring 238.

[0040] Figures 10a and 10b show the spring 238 in side and underneath plan views respectively. The spring 238 is stretched between a fin 240 depending down from the right side wall of the slider 214 and a foot 242 extending out from the back of the left edge of the flap 226. The fin 240 extends through a slot in the PCB along which it can move. Accordingly, the spring is connected in an oblique fashion so that it urges the slider towards the front of the reader, so that it also urges the flap to the right hand side, and so that it also imparts a rotational bias torque to the flap to keep in normally in the vertical position. Thus it should be apparent that the spring exerts a plurality component forces, which obviates the need for a series of springs thus providing savings in component count.

[0041] The design of the data card module and the data card reader is such that in order to install the module in the reader the module is simply pressed into the slotted aperture of the reader and once inside the reader, the module automatically locks into position in the reader. For releasing the module it is simply pressed once again into the reader which automatically unlocks the module from the reader so as to allow the withdrawal of the module. The details of this operation are as follows.

[0042] Details of installing the module in the reader will be described first. With two data cards loaded into the data card holder module, the data card module is offered up to the slotted aperture 204 in the fascia plate 202 of the data card reader. It is offered up to the aperture 204 with the rear end of the tail portion 104 of the module as the leading edge. Accordingly, the tail portion 104 is inserted into the aperture 204 and the front face 110 is pressed inwards. As the tail 104 passes the opening of the slotted aperture 204 it comes into contact with the flap 226 near to its top edge midway along the length of the flap. This applies a turning force to the flap which as a result rotates about the shaft axis from its vertical configuration towards a horizontal configuration, and as the module is pushed in further the flap adopts a horizontal planar orientation against the rotational bias of the spring 238 which acts to hold the flap in a vertical plane.

[0043] The module is continued to be inserted inside the reader and once the tail 104 is past the slotted aperture, the side walls 106, 108 of the module slide against and effectively come to be guided first by the end walls of the slotted aperture 204, and on further insertion by the side walls and cross bar of the frame 210 of the data reader, which thus receives the module. This engagement between respective walls of the module and reader frame serves to constrain the module to be able to move with only one degree of freedom in relation to the reader, that is sliding in a longitudinal direction in and out of the slotted aperture 204.

[0044] As the module is further pressed into the reader the leading edge of the second data card catches the depending feet on the under surface of the slider 214, and as the module is pressed in further the second data card pushing on these feet moves the slider 214 backwards. Backwards displacement of the slider stretches the spring 238 which consequently imparts a forward acting force on the slider, which in turn pushes on the module via the feet and data card leading edge so as to tend to urge the module back out of the slotted aperture 204 against the direction of insertion.

[0045] Once approximately two thirds of the length of the module has been fed into the reader, the sprung peg member 128 approaches the slotted aperture 204 and pin head 128 passes through the cut-out 206 in the slotted aperture. On continued insertion past the slotted aperture the pin head 132 of peg member 128 comes into contact with the bottom right hand comer of the now horizontally orientated lower raised formation 232.

[0046] This is the start point of the pin head's journey around the contour of the relief pattern as illustrated in Figures 11a to 11j. In Figure 11a the start point is indicated at position A. It should be borne in mind that the pin head 132 is biased against the end wall 138 of the slot 130 in the base of the module by the spring portion 134, and can move against the bias of the spring 134 in the slot. Furthermore, the flap is resiliently biased by spring 238 so as to be urged laterally towards the right but can slide from side to side against the action of the lateral resilient bias so that the shaft slides in the holes of the extending arms of the frame.

[0047] From position A, as the data card module is pushed in into the reader, the pin head 132 moves inwards into the reader and pushes against the side of the inclined right hand surface of the lower raised formation. Because the pin head is hard against the end 138 of the slot it cannot move to the right and thus the action of moving the pin inwards translates to displacement to the left of the flap. In other words, the pin displaces the flap to the left by a wedging action on the inclined hand surface of the lower raised formation against the lateral spring bias. As the module is pushed further inwards into the reader, the pin which of course is also moving inwards continues to push against the right side of the lower raised formation and because of the extending inclination of the lower raised formation the pin carries on acting on the formation to move the formation and consequently the flap towards the left hand side.

[0048] During this inward movement of the module, the leading edge of the second data card which has engaged the depending feet of the slider pushes the slider further backwards thereby further stretching the spring

IPR2025-00645 Page 00070

which consequently exerts a forward pushing force on the slider and the module.

[0049] As the module is pressed in some more against the pushing force of the slider, the pin head continues to push on the inclined right side surface of the lower formation, pushing the flap to the left until the pin head reaches the position marked B in the Figure 11b which in relation to the formation is the upper right position. In this position, the flap has been displaced to the left by the amount indicated as delta in Figures 11a and 11b. Because the flap has moved to the left, the spring which is connected to the flap has been stretched to the left and so applies a bias to the flap to pull it back towards the right. From B, as the module is pushed further in, the pin head clears the crest of the right side surface of the formation. At this juncture, because of the lateral resilient bias of the spring pulling the flap towards the right, the spring snaps the flap towards the right so that the pin head abuts and stops against the upper raised formation in the position shown at C: it abuts against the right hand side of the upper raised formation and prevents the flap from total movement to the right. At this point the data card module is fully inserted inside the data card reader and the front face of the module is flush with the face of the fascia plate. Accordingly, insertion of the modules ceases. Consequently, the slider 214 which is resiliently biased to push the module back outwards pushes the module accordingly which moves the pin head down along the right side face of the upper raised formation to position D in Figure 11d. At this point, the pin head is moved along the inclined right side face of the upper raised formation by the action of the lateral resilient bias of the spring continuing to pull the flap across to the right. The pin head is also moved towards the trough of the V shaped notch in the lower raised formation by action of the slider pushing outwards on the module. As a result, the pin head is moved along guideway 234 and comes to stop in the catch member given by the right angle detent defined by the left side wall of the substantially V shaped notch in the upper surface of the lower raised formation at position E in Figure 11e. In this position, the pin head is latched with respect to the relief pattern and consequently the module is securely held in the reader.

[0050] This latching is provided by virtue in one direction of the pushing action of the slider on the module thus urging the pin against the base of the V shaped notch of the lower raised formation which is held firm in that direction by being part of the flap which is fixed in that direction by the arms of the frame of the reader. And in the other direction by virtue of the pin head being pushed by the left side wall (because of the lateral spring bias) against the end wall 138 of the slot 130 in the module. Accordingly, the module is installed in the reader.

[0051] To uninstall the module and release it from the reader, the operation is as follows.

[0052] The front face 110 of the module is once again pressed in towards the data card reader. This dislodges the pin head from the right angle detent of the V shaped notch to position F and onwards in guideway 234 such that it approaches the crest of the left wall. At this point, the flap which is still biased to some extent to the right now has the opportunity to move across to the right once more and accordingly the pin head clears the left side wall and proceeds to position G. In this configuration, the flap has moved back to the right so that its right side wall is hard against the right arm 220 of the frame of the reader.

[0053] With the pin head clear of the guideway 234, the slider which is urging the module outwards pushes on the module by means of the longitudinal bias of the spring. This pushes the module outwards to some extent. The effect of this on the pin head is that the pin head moves sideways towards the left along the left hand side of the lower raised formation. The pin head is able to move sideways towards the left because it can move to the left in the slot 130 in the module from which it projects against the bias of its spring portion 134. As the module is withdrawn from the reader it slides down the inclined left hand surface of the lower raised formation, itself moving to the left against spring bias 134 as it does so, and in Figure 11h. As it approaches the lower part of the left inclined wall (Figure 11 i) the resilience of the spring portion 134 pushes the pin head towards the right back over the bevel 236 towards its start position hard against the end wall 138 of the slot 130. The module is thus retracted from the reader.

[0054] Accordingly, it should be apparent that the pin head is made to follow the contour of the relief pattern because while the pin head reciprocates longitudinally, the flap moves transversely from side to side. Thus in a general sense the latching mechanism allows the data card module to be pressed into the reader for connection and then again for disconnection by the provision of resiliently biased interengaging formations.

[0055] It is envisaged that one of the data cards will be the user SIM card and the other data card could be a Smart card or a further SIM card having stored thereon the phone numbers of the Emergency Services in various countries. In this way, if the car is driven around in different countries, something that is very probable for example in central Europe, then the user does not have to commit to memory the different Emergency Services' telephone numbers. It should be mentioned that the user SIM need not be installed in the unit in order for the Emergency SIM card to be operational.

[0056] Accordingly, if the Emergency SIM requires replacement because say the Service Provider is changed, or needs testing, or the car has a new owner, it can be quickly and conveniently removed from the radio device unit and then drawing out the data card holder and finally removing the SIM. Since this operation can be performed by the user it does not require a specialist Serviceperson. Nor does it mean that the radio device has to be opened up, thus minimising the risk of damaging the radio device.

IPR2025-00645 Page 00071

[0057] The unit itself may be a telematic terminal operating in GSM with some Value Added Services for example security and traffic information services using the double SIM card concept (user SIM and back-up SIM). The telematic terminal is normally mounted (fixed) in the car. The set up is envisaged such that there are no limitations for the first SIM, the User SIM. The second SIM, so called back-up, should not be prepaid, fixed dial or twin-card. In this context, an easily removable User SIM would carry out the every day phone usage. The back-up SIM (also called as Fixed SIM), would be a secondary, limited usage SIM to carry out some Value Added Service functions.

[0058] The telematic unit uses GSM communications and GPS data to implement Value Added Services for different purposes. Some of them like traffic information are terminal independent and some of them are highly dependent on existing car interfaces like automatic emergency call (airbag signal triggered), theft protection service (theft alarm triggered) etc.

[0059] The basis of the double SIM concept is to back-up the User SIM in emergency situations since it is not always assured that the User SIM is inserted, can support the functionality, or is not blocked etc. It is envisaged to have two SIMs active at the same time (receiving, paging).

[0060] The present invention may be embodied in other specific forms without departing from its essential attributes. For example, the radio communication device could be a portable handheld radiotelephone. The particular design of the mechanical formations provided for holding the two data cards could take a number of different arrangements for example grooves, channels or flanged lips could be provided for receiving the data cards. Additionally, the elements of the latching mechanism of the second embodiment may be mechanically reversed.

[0061] Furthermore, each feature disclosed in this specification (which term includes the claims) and/or shown in the drawings may be incorporated in the invention independently of other disclosed and/or illustrated features. In this regard, the invention includes any novel feature or combination of features disclosed herein either explicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed.

[0062] Accordingly, reference should be made to the appended claims and other general statements herein rather than to the foregoing description as indicating the scope of invention.

[0063] The abstract as filed herewith is included herein by reference.

Claims

1. A holder for two or more data cards for a radio communication device, the holder comprising a body having formations for releasably carrying said two or more data cards and being adapted to be removably installed in a data card reader of said device.

2. A holder according to claim 1, wherein said formations are provided such that the two or more data cards when loaded in the body are carried in an oppositely facing back to back arrangement.

3. A holder according to claim 1 or claim 2, wherein said formations comprise longitudinally extending slots for receiving said two or more data cards.

4. A holder according to any of claims 1 to 3, wherein the body includes respective apertures for exposing electrical contacts of said data cards when loaded in the body.

5. A radio communication device including a data card reader, the device having a housing defining an aperture associated with the reader and dimensioned to receive a holder carrying two or more data cards, the arrangement being such that the data card holder is removable from the reader, and wherein the data card holder is provided with formations for releasably carrying two or more data cards.

6. A radio communication device according to claim 5, wherein the data card holder carries said two or more data cards in an oppositely facing arrangement, and the data card reader comprises two or more electrical circuits correspondingly arranged in facing relationship for reading the two or more data cards.

7. A radio communication device according to claim 5 or claim 6, comprising a cover member adapted to be disposed against said housing such that when a data card holder is located in the card reader the cover obstructs retraction of at least one of the two or more data cards.

8. A radio communication device according to any of claims 5 to 7, wherein the data card holder is provided with longitudinally extending slots for receiving said two or more data cards, and the cover member is provided with one or more slots which when the cover member is disposed against said housing are in alignment with one or more of the openings of the longitudinally extending slots of the data card holder.

9. A radio communication device according to any of claims 5 to 8, comprising ejector means urging the installed data card holder such that on removal of the cover member at least a portion of the data card holder is urged through the aperture.

IPR2025-00645 Page 00072

10. A radio communication device according to claim 5, wherein the data card reader and a data card holder have a latching mechanism therebetween for releasably connecting together the holder and the reader, the holder having a longitudinal axis indicating a longitudinal direction and being adapted to be received in the reader, and the latching mechanism being engagable in the latched condition to connect together the holder and reader by pressing the holder in the longitudinal direction into the reader, and being disengagable from the latched condition to release the holder and reader by pressing the holder into the reader in the longitudinal direction,

the latching mechanism comprising
a lateral deflecting surface and detent associated with one or other of the holder or reader, the lateral deflecting surface being inclined to the longitudinal direction,
a peg member associated with the other of the holder or reader, and
resilient means operative to apply bias in the longitudinal direction and in a transverse direction to the longitudinal direction,
in which the longitudinal bias of the resilient means acts so as to urge the holder and reader longitudinally apart,
and the transverse bias of the resilient means acts so as to urge one of said lateral deflecting surface and detent or said peg member transversely with respect to the other one of the lateral deflecting surface and detent or the peg member,
the arrangement being such that responsive to pressing the holder into the reader for connection, the lateral deflecting surface, peg member and resilient means cooperate so as to engage the peg member with the detent in the latched condition,
and responsive to pressing the holder into the reader for release, the peg member disengages from the detent and the resilient means operates to urge at least a portion of the holder from the reader for removal thereof.

11. A radio communication device according to claim 10, wherein the arrangement is that for connection of the holder and reader the holder is inserted into the reader causing the lateral deflecting surface to abut the peg member and whereby responsive to continued insertion the peg member and the lateral deflecting surface co-operate to cause transverse deflection of one of said lateral deflecting surface and detent or said peg member against the transverse bias of the resilient means,

and continued insertion causes the peg member and the lateral deflecting surface to clear one another so as thereby to allow the resilient means to bias and hold the peg member into engagement with the detent in the latched position by means of the longitudinal and transverse bias thereof,
and wherein for releasing the holder from the reader the holder is urged towards the reader in the longitudinal direction against the longitudinal bias of the resilient means so as to disengage the peg member from the detent thereby allowing the transverse bias of the resilient means to urge one of said lateral deflecting surface and catch member or said peg member in a transverse direction such that the peg member is clear of the catch member so that the first resilient means can urge the holder apart from the reader for removal of the holder from the reader.

12. A radio communication device according to claim 10 or 11, wherein the lateral deflecting surface and detent are incorporated in a relief formation associated with the reader, and the peg member is associated with the holder.

13. A radio communication device according to claim 12, wherein the transverse bias of the resilient means acts so as to urge the relief formation transversely with respect to the peg member.

14. A radio communication device according to claim 10, wherein the data card reader defines a chamber for receiving the holder and includes a slider adapted to be engaged with the holder so as to resiliently bias the holder out of the card reader.

15. A radio communication device according to claim 12, wherein the relief formation is provided on a flap.

16. A radio communication device according to claim 15, wherein a spring disposed between the slider and the flap provide the resilient means.

17. A radio communication device according to any of claims 10 to 16, wherein the data card holder has a backwardly extending cantilever tail portion.

18. A radio communication device according to claim 17, wherein said at least one data card is mounted from the rear of the holder.

19. A radio communication device according to any of claims 10 to 18, wherein disposed towards the front of the holder is a compartment carrying a sprung peg which depends from a slot in the base of the compartment wherein said peg is resiliently biased in said slot towards an end wall of the slot.

IPR2025-00645 Page 00073

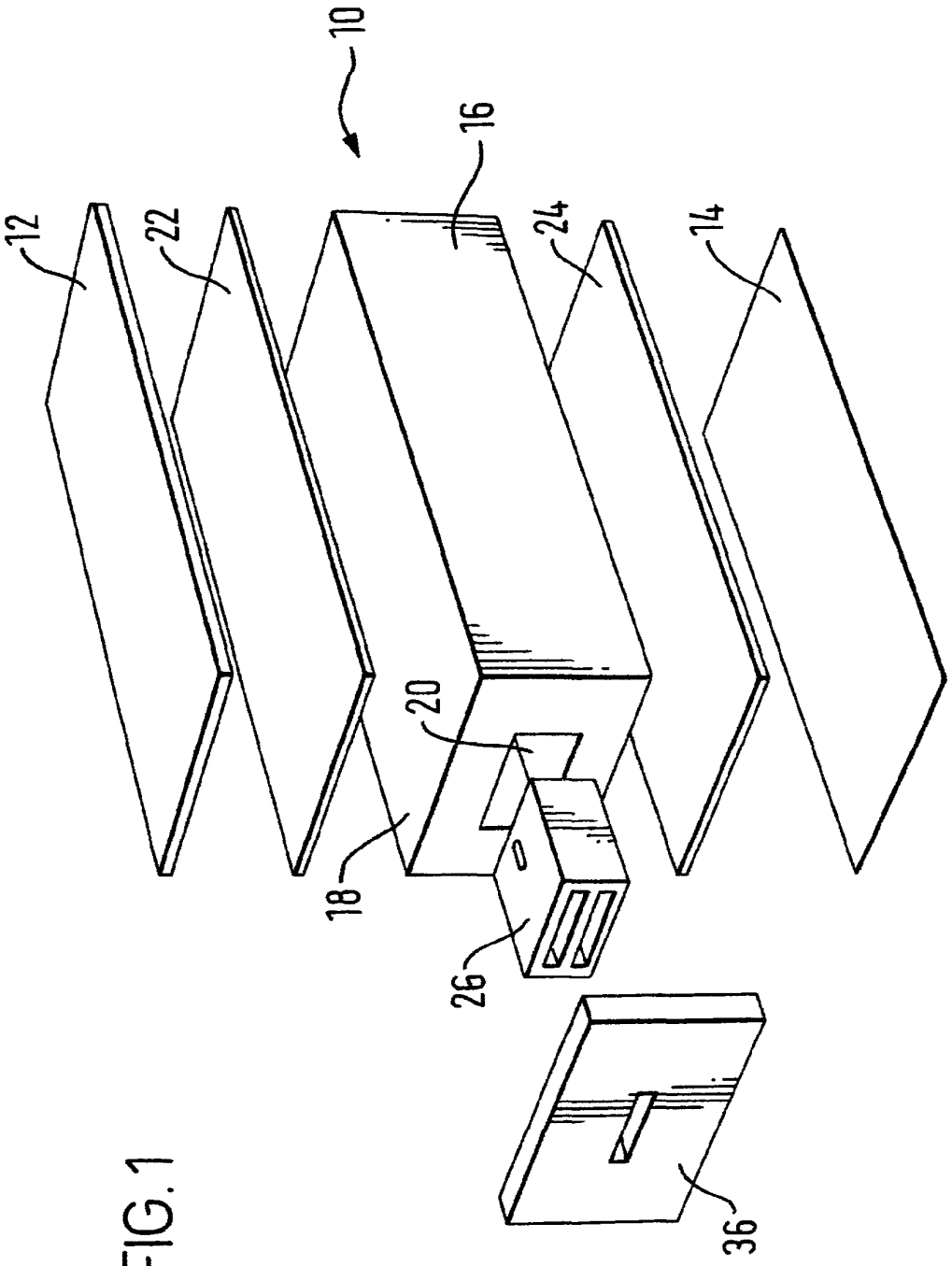


FIG. 1

IPR2025-00645 Page 00074

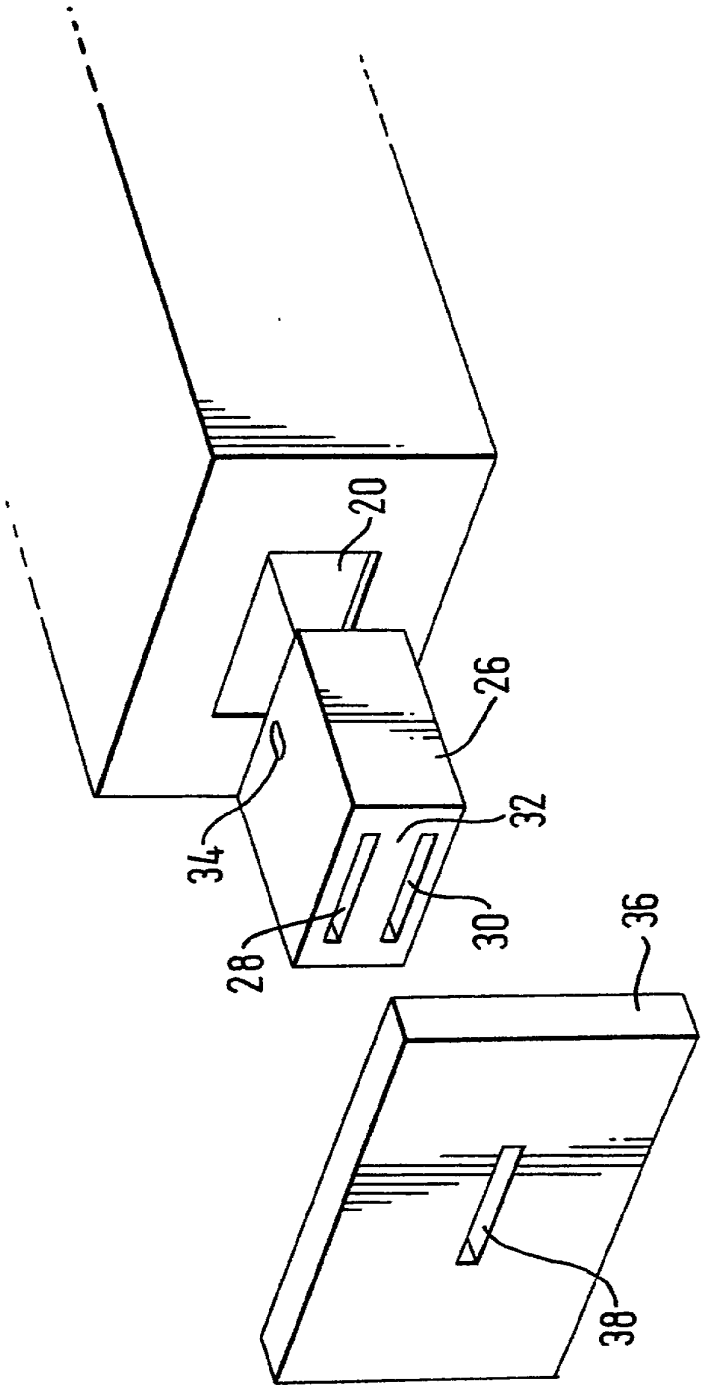


FIG. 2

IPR2025-00645 Page 00075

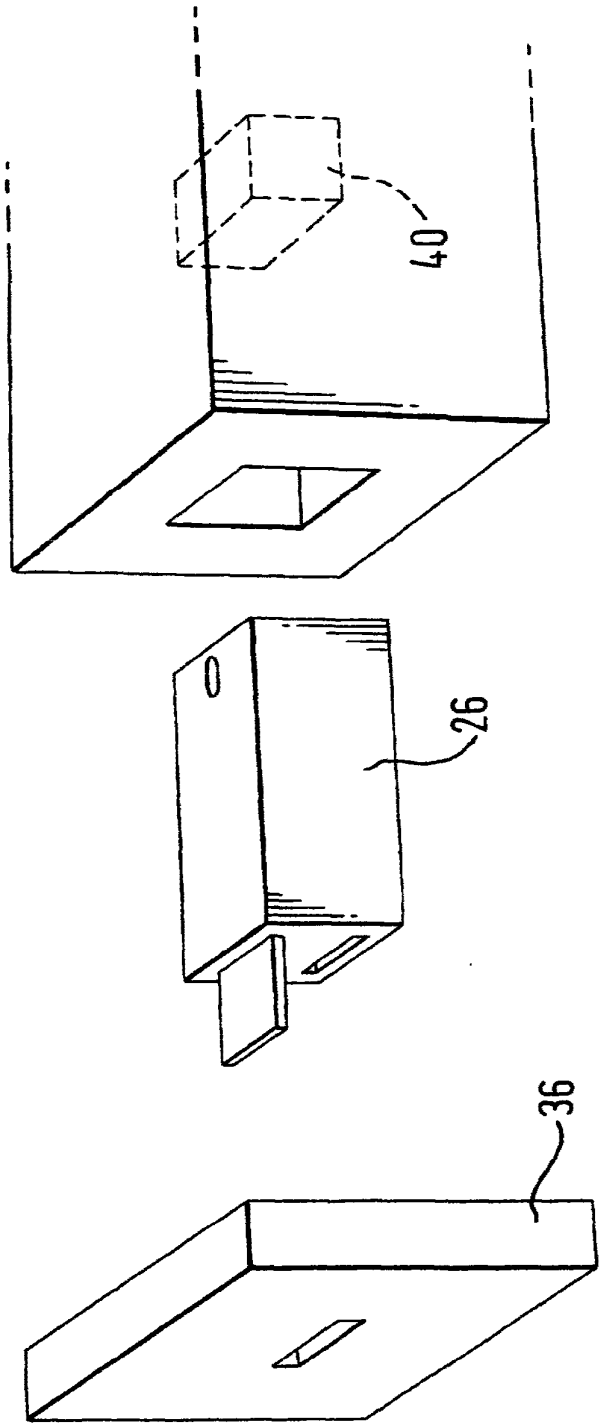


FIG.3

IPR2025-00645 Page 00076

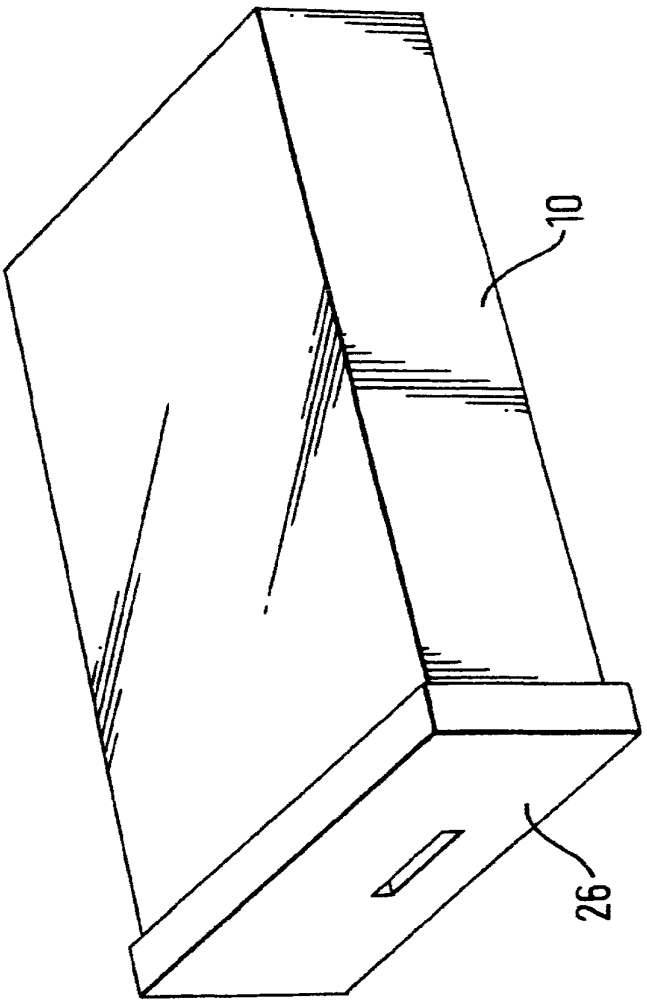


FIG. 4a

IPR2025-00645 Page 00077

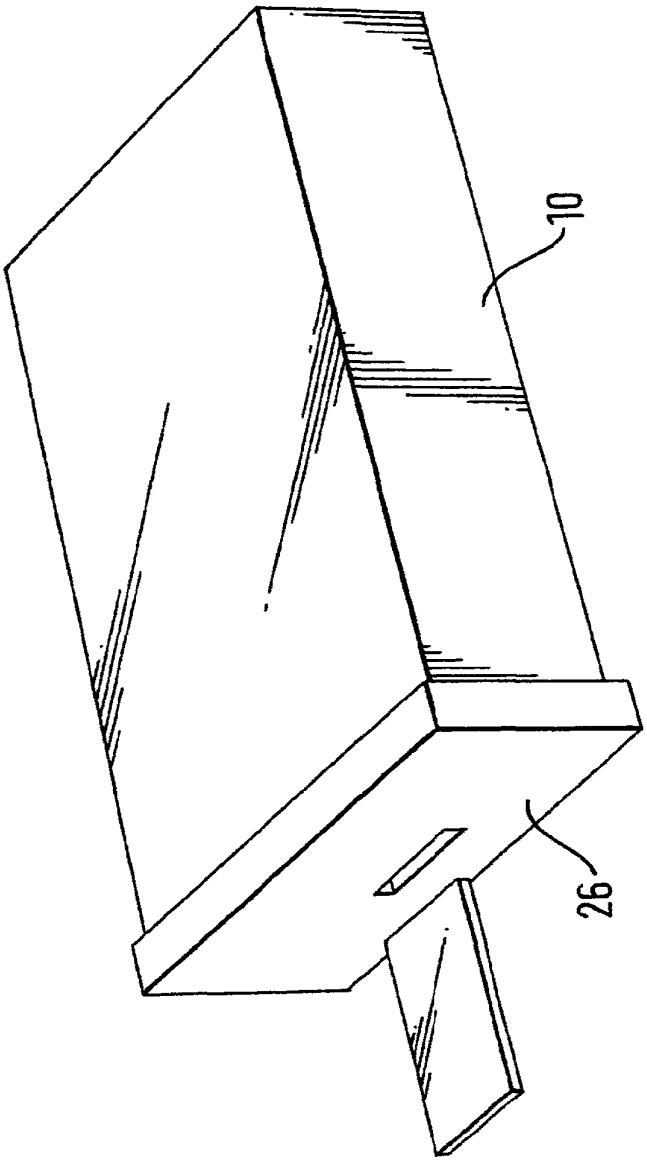


FIG. 4b

IPR2025-00645 Page 00078

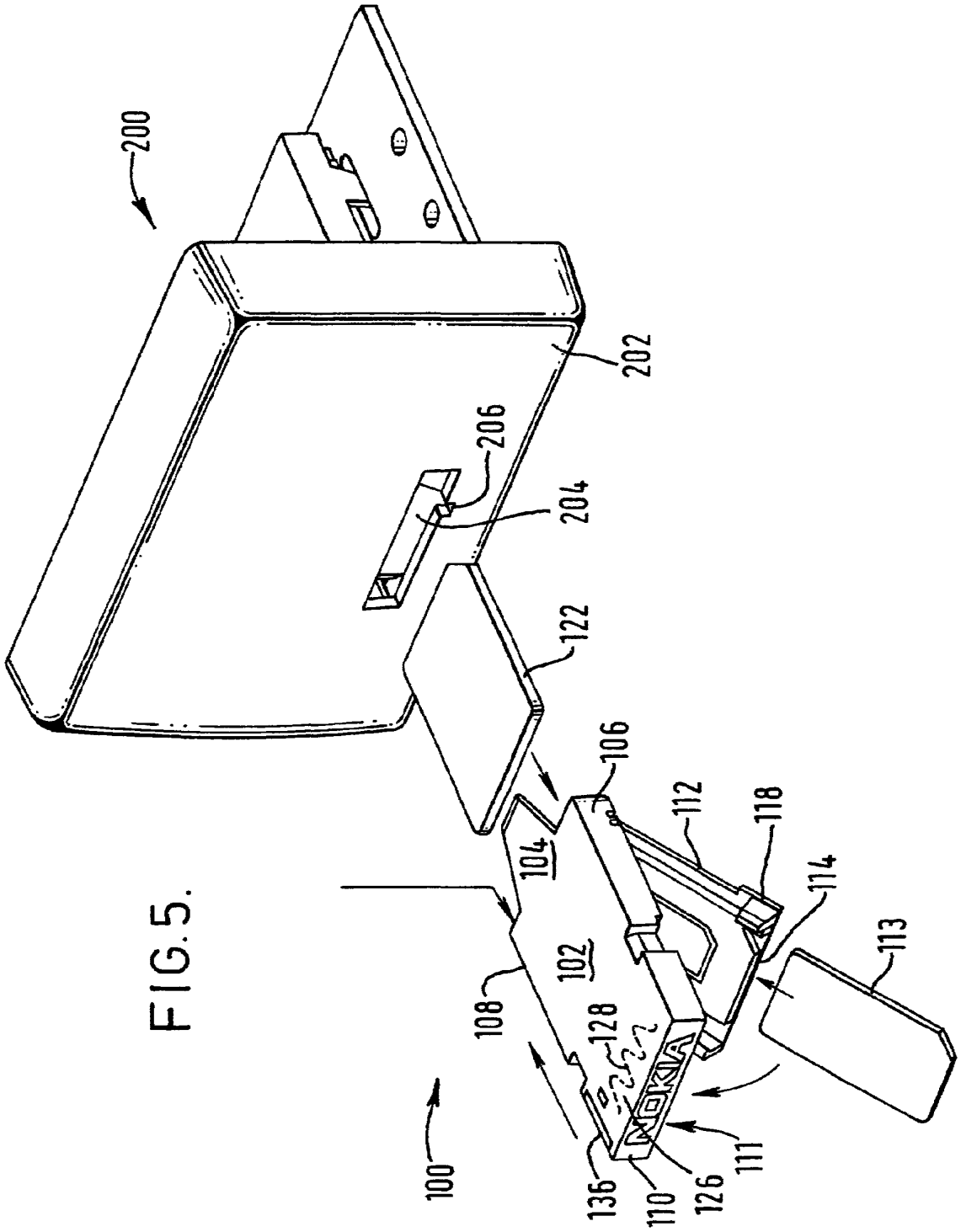


FIG.5.

IPR2025-00645 Page 00079

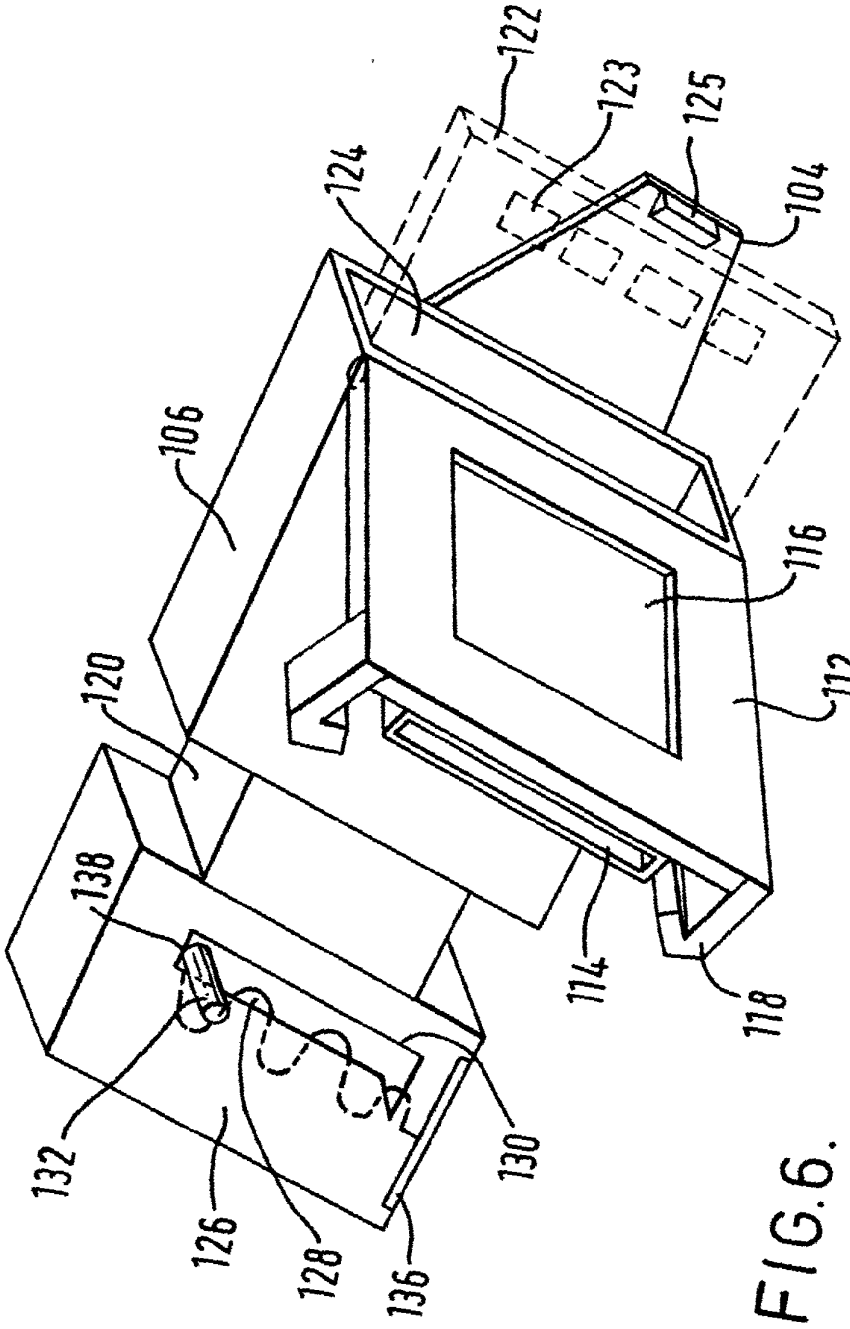
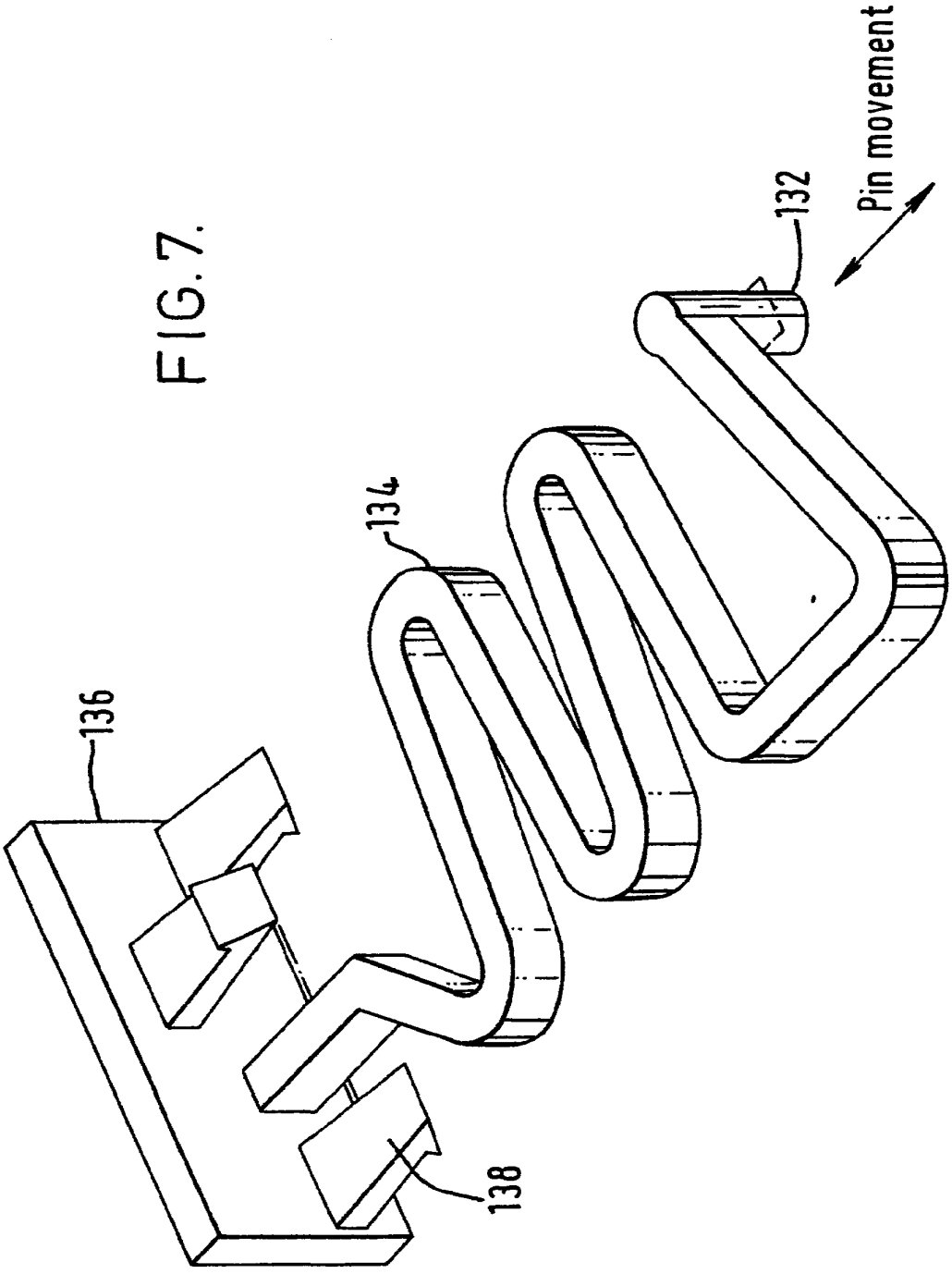


FIG.6.

IPR2025-00645 Page 00080

FIG. 7.



IPR2025-00645 Page 00081

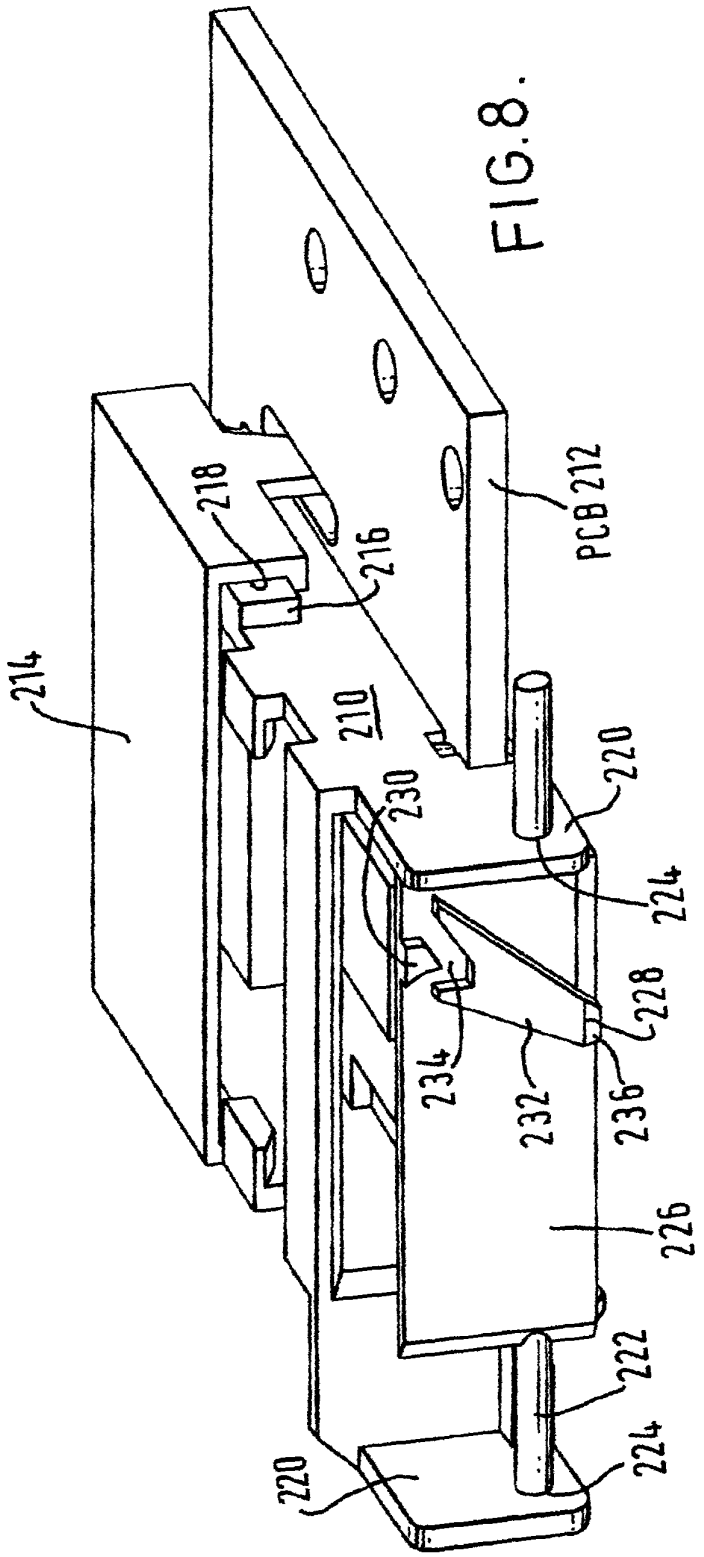
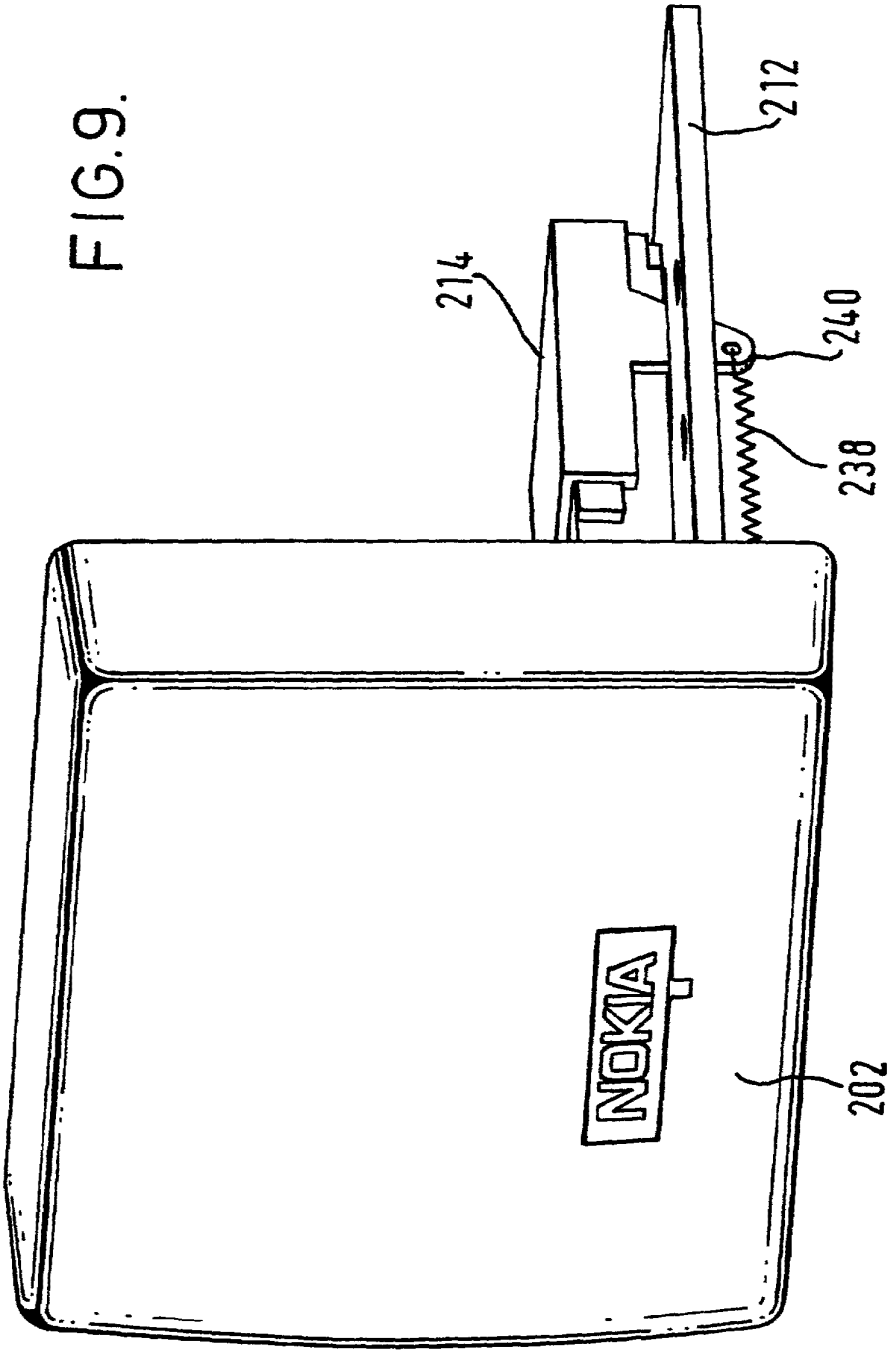


FIG.8.

IPR2025-00645 Page 00082

FIG.9.



IPR2025-00645 Page 00083

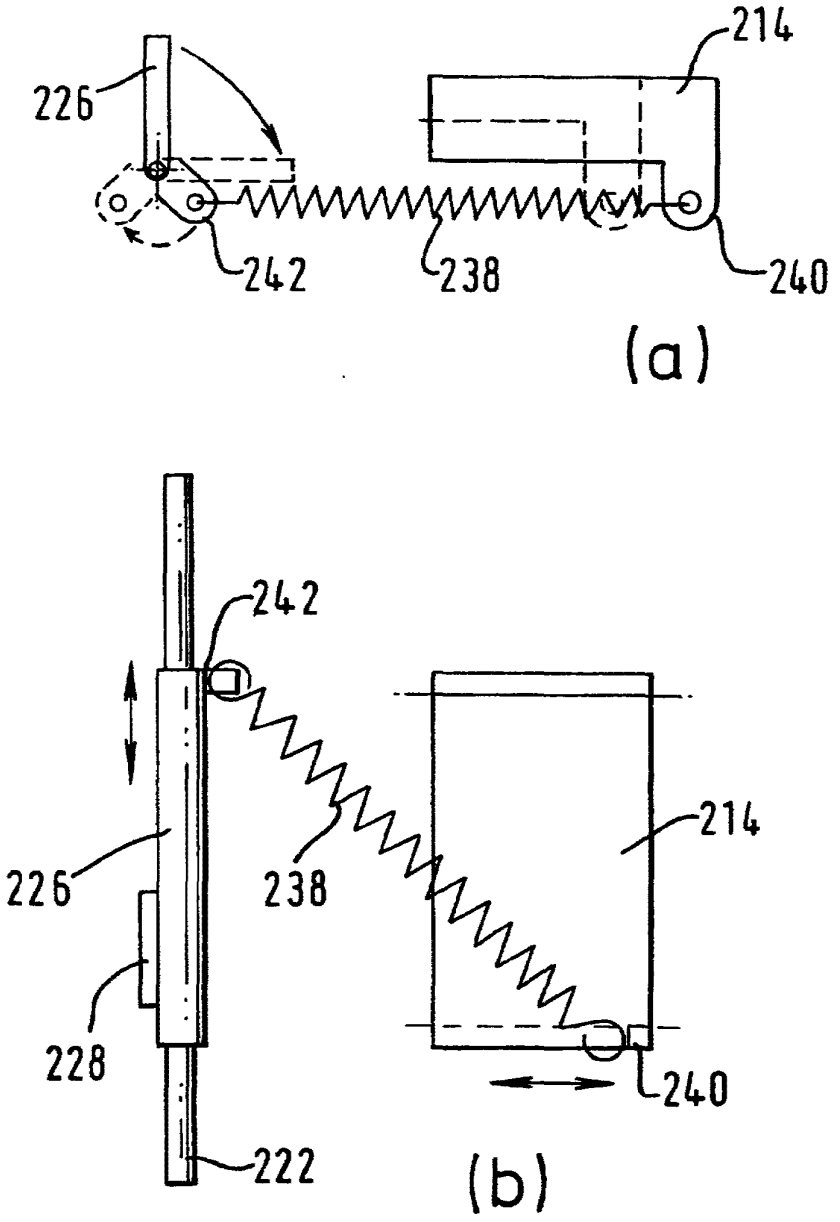


FIG.10.

IPR2025-00645 Page 00084

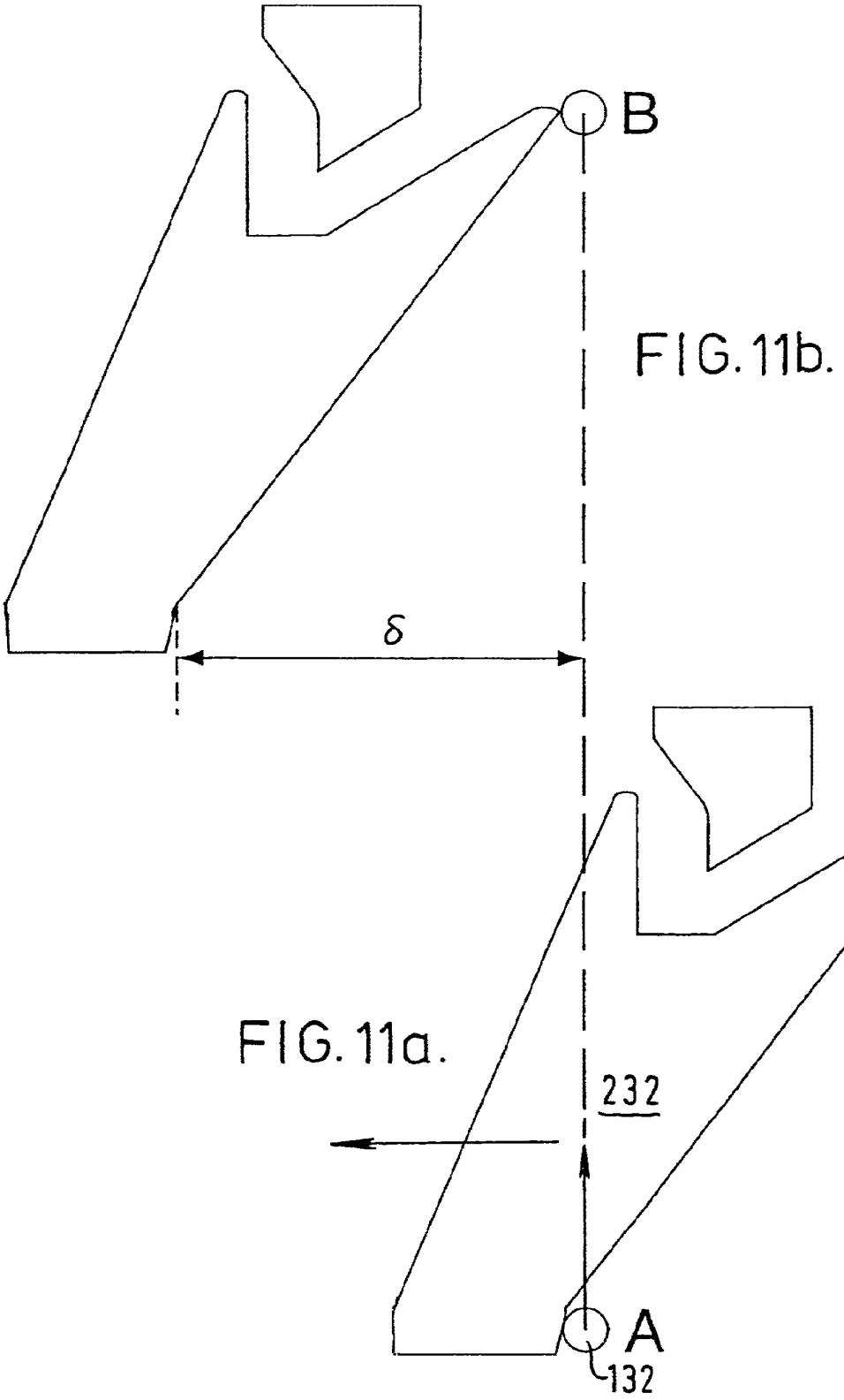


FIG. 11b.

FIG. 11a.

IPR2025-00645 Page 00085

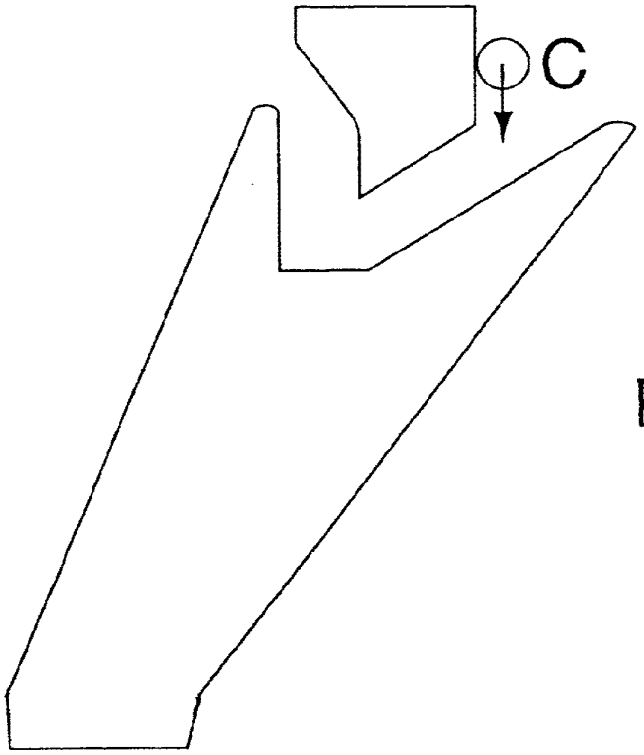


FIG. 11c.

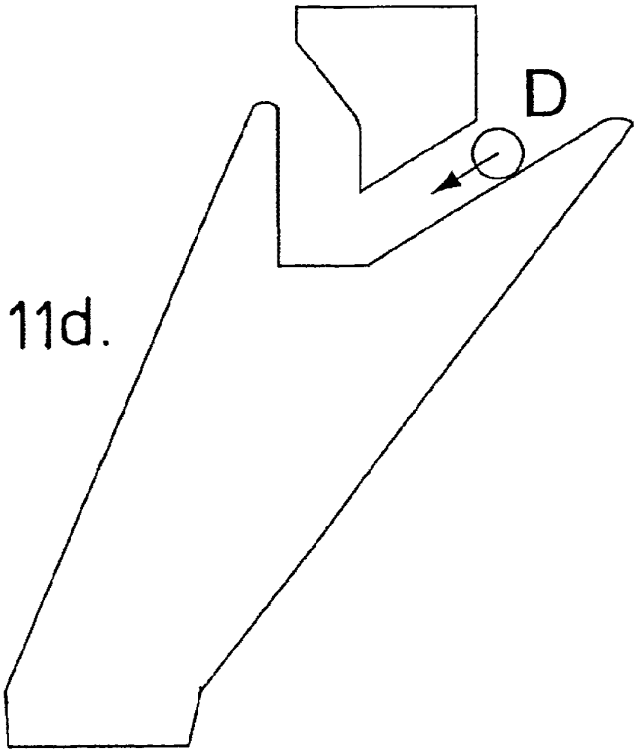


FIG. 11d.

IPR2025-00645 Page 00086

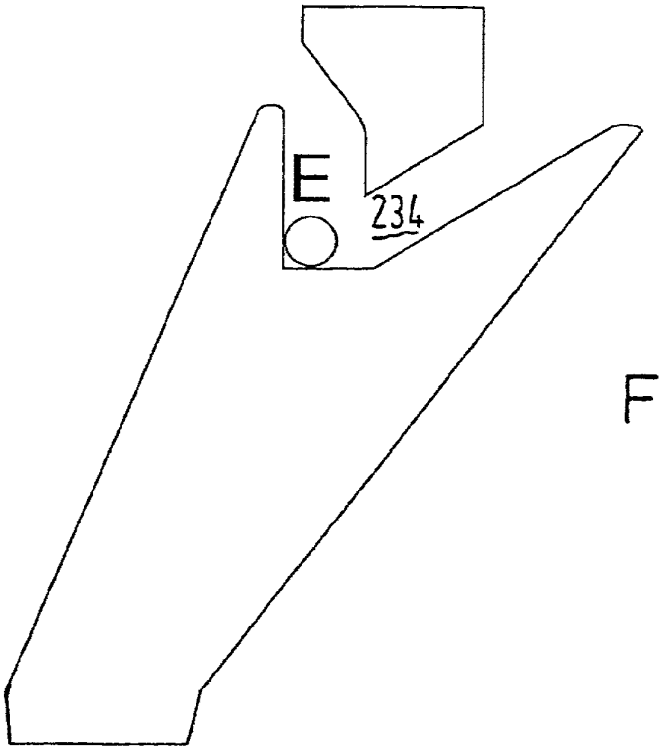


FIG. 11e.

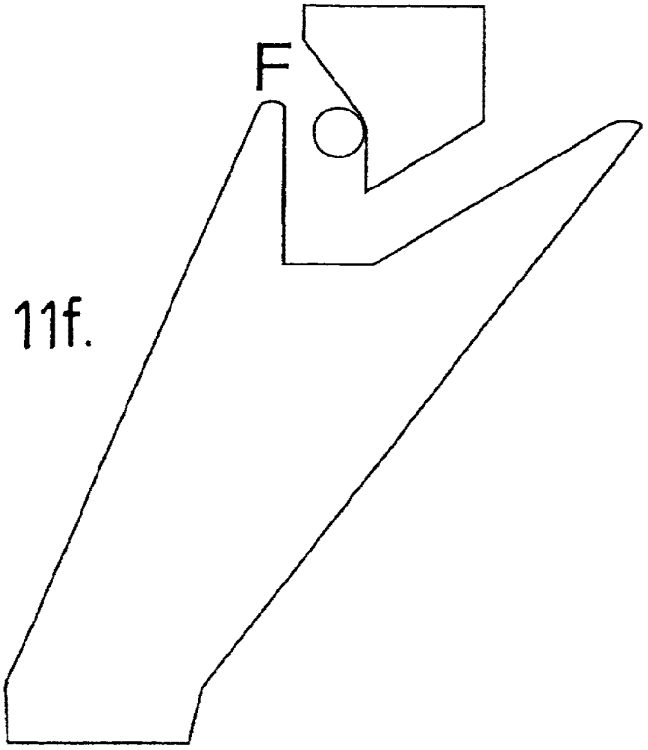


FIG. 11f.

IPR2025-00645 Page 00087

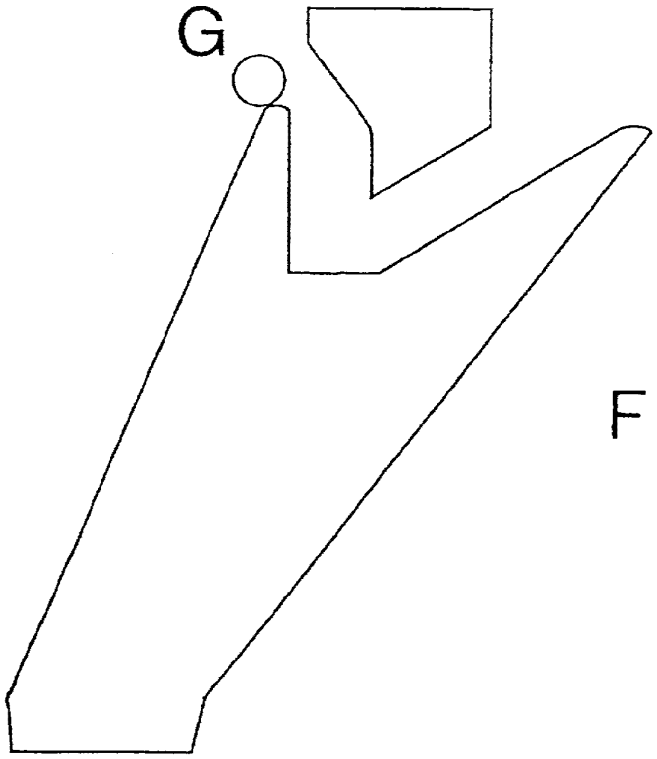


FIG. 11g.

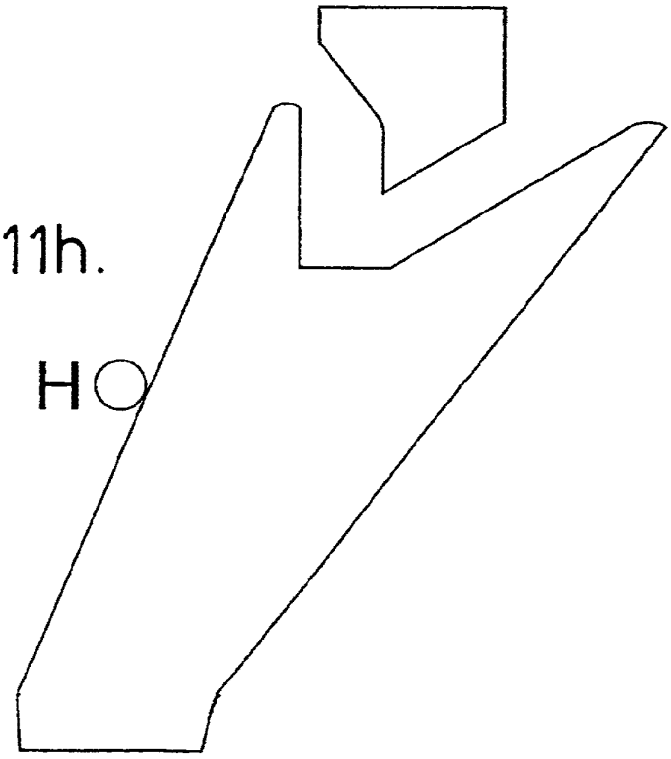


FIG. 11h.

IPR2025-00645 Page 00088

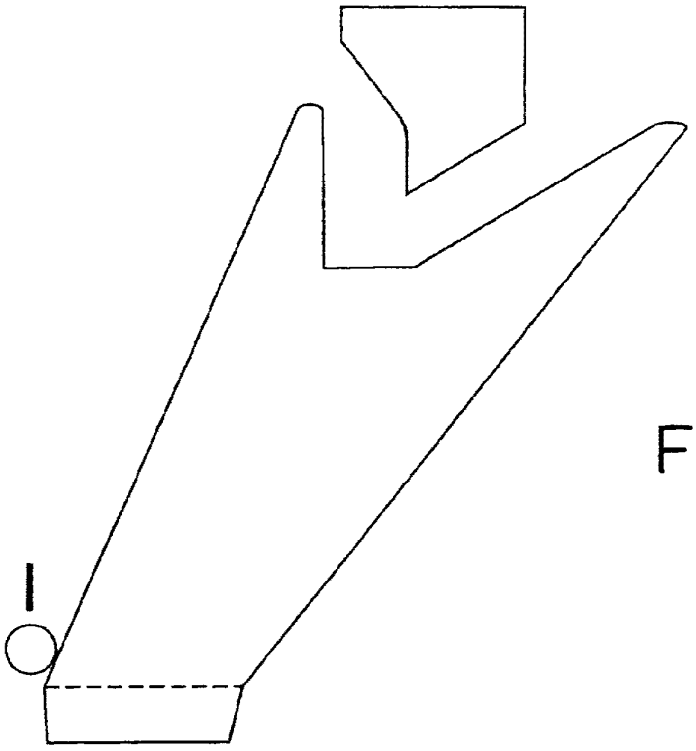


FIG.11i

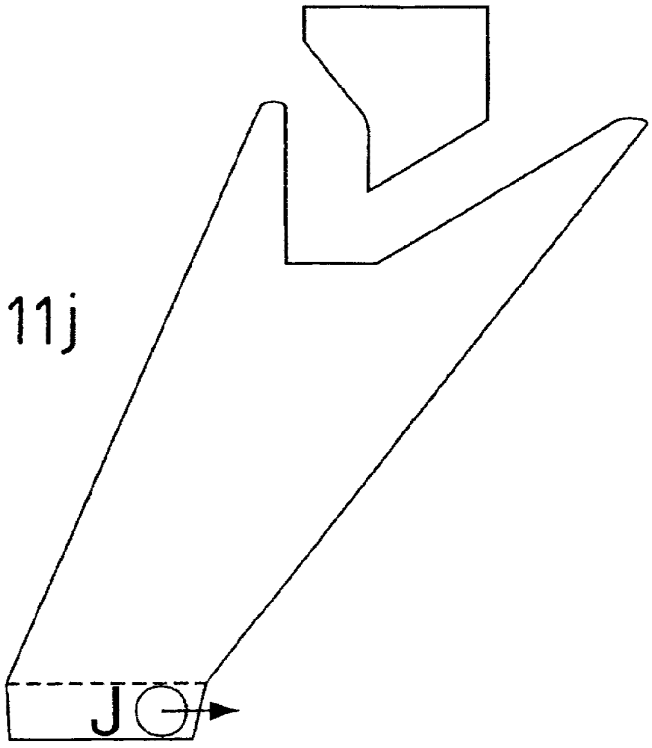


FIG.11j

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 117 068 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
18.07.2001 Bulletin 2001/29

(21) Application number: **99940552.5**

(22) Date of filing: **30.08.1999**

(51) Int Cl.[7]: **G06K 19/077**, G06K 17/00, H02J 7/00, G07F 17/00, G06F 17/60, G09F 27/00

(86) International application number:
PCT/JP99/04671

(87) International publication number:
WO 00/13139 (09.03.2000 Gazette 2000/10)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **31.08.1998 JP 24599598**

(71) Applicants:
- **C. Media Co. Ltd.**
  Bunkyo-ku, Tokyo 112-0014 (US)
- **ITOCHU CORPORATION**
  Minato-ku, Tokyo 107-8077 (JP)

(72) Inventors:
- **NAGAOKA, Jiro, C. Media Co. Ltd,**
  35-17 Sekiguchi
  Bunkyo-ku, Tokyo 112-0014 (JP)
- **NAKAJIMA, Satoki**
  Minato-ku, Tokyo 107-8077 (JP)

(74) Representative:
Manitz, Finsterwald & Partner GbR
Robert-Koch-Strasse 1
80538 München (DE)

(54) NONCONTACT IC MEDIUM AND SYSTEM USING THE SAME

(57) There is provided a cellular phone radio that is capable of utilizing a contactless IC media. A contactless IC media 20b is molded in the form of a coin and interchangeably born by a cellular phone radio 110. The cellular phone radio 110 includes a media holder 111, a radio transceiver circuit having an antenna 112, and a control circuit that conducts the read control and the write control of digital information with respect to both recording regions of a contactless IC media 20b within the media holder 111 and an external contactless IC media 20a, ICC, and also includes a processor that conducts information processing on the basis of the read digital information as occasion demands.

FIG. 1a

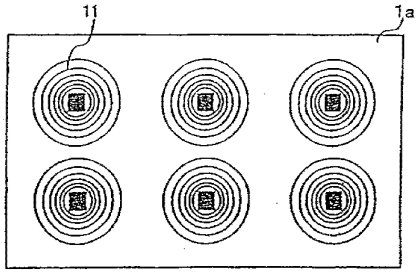
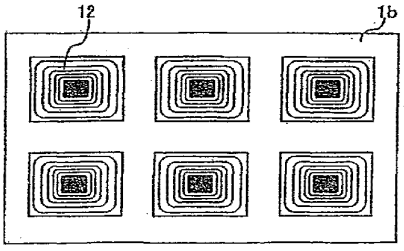


FIG. 1b



EP 1 117 068 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to a contactless IC media and a system to which the contactless IC media is applied. In the present specification, the term "contactless IC media" is directed to general media on which there is mounted a core module based on the specification of a contactless IC card which has been internationally standardized or subjected to international standardization deliberation, for example, in IEC (International Electrotechnical Commission) JTC1 (Joint Technical Committee 1)/SC (Sub-Committee) 17 of ISO (International Organization for Standardization), that is, a contactless IC module.

[0002] As specific examples of the system to which the contactless IC media is applied, the contactless IC media is born on a portable communication device, for example, an existing cellular telephone radio, a portable computer device or the like to execute various applications, the portable communication device is spread before an external contactless IC media to read recorded information from the contactless IC media and to execute required processing, information communication is conducted through the contactless IC media or a contactless reader/writer that bears the contactless IC media, and so on.

BACKGROUND ART

[0003] As a card type tool that requires security such as an electronic account settlement card or an identification card in an electronic commerce, a contact IC card having an electric contact has come into practical use. Because the contact IC card is so structured as to be electrically connected directly to the reader/writer through the contact, the operation is normally stable. However, because the card is inserted into or drawn off from the reader/writer with a physical contact, there is the possibility that a trouble such as contact failure occurs. Under the circumstances, in recent years, acontactless IC card on which a contactless IC media that enables the transmission of recorded information without any physical contact is mounted has appeared and has been studied for practical use.

[0004] The contactless IC card is normally structured by mounting a contactless IC media made up of a radio transceiver circuit having an antenna (coil) and an IC section having a processor and a memory on a card medium. The contactless IC card may be structured by a so-called memory card having no processor in the IC section.

[0005] The connection with the reader/writer in the contactless IC card is conducted through the radio transceiver circuit, and a power supply and clocks required for the operation are generally supplied from the reader/writer side. The transmission of information including a power component and so on from the reader/writer is conducted by using a signal resulting from modulating a radio carrier wave of, for example, 13.56 [MHz] in ASK (amplitude shift key) . On the other hand, the transmission of information from the card side is conducted by using a signal resulting from load-modulating sub-carrier waves (847.5/423.7 [kHz]) which combine a plurality of signals of, for example, 13.56 [MHz] together. Because it is predicted that a plurality of contactless IC cards are mixed together in the vicinity of the same reader/writer, a technique which is called "anti-collision" for preventing data collision between the respective cards has been established. At present, a modulating system conducted at the time of returning from the card side to the reader/writer is changed, or a return timing is changed, to thereby enable several cards to be identified. The anti-collision technique can be referred to the disclosures of Japanese Patent Unexamined Application Publication No. Hei 5-217032, Japanese Patent Unexamined Application Publication No. Hei 5-266267.

[0006] Also, in recent years, cellular phone radios such as PHSs (Personal Handyphone System) or wireless phones, and mobile computer terminals have been rapidly diffused, and many persons have come to carry the cellular phone radios or the mobile computer terminals. Under the circumstances, an attempt is made to variously add value to the cellular phone radio and so on with the use of the IC card. For example, Japanese Patent Unexamined Application Publication No. Hei 8-87655 discloses an information processing system in which when a holder of an IC card (an owner of the cellular phone radio) inserts the IC card on which information on a bank of account has been recorded into the cellular phone radio to purchase goods or offer paid service, a device for offering the goods or the like acquires the recorded information of the IC card through the cellular phone radio, and automatically conducts electronic account by aid of the acquired recorded information. In this example, the IC card is formed of a contact type IC card, and the cellular phone radio side is equipped with a contact type reader/writer having an electric contact.

[0007] As described above, because no electric contact is required for the contactless IC card, the IC module can be downsized, thinned and mass-produced as compared with the contact IC card. Also, even if a plurality of contactless IC cards are mixed together in the vicinity of the same reader/writer, since the reader/writer side can discriminate those IC cards, the same application mode as that of the contact type IC card is enabled. In addition, the reader/writer for reading the information recorded on the contactless IC card can be downsized and lighted in weight more than the contact type IC card.

[0008] However, most of the conventional contactless IC cards record the information in card unit. That is, the application of the IC card is determined in each of the cards. For that reason, the user is burdened down with holding a plurality of contactless IC cards according to

IPR2025-00645 Page 00091

the purposes of applications and finding out an appropriate IC card when using the IC card.

[0009] Also, for example, in the above-mentioned information processing system, if the contact type IC card is replaced by the contactless IC card, the reader/writer can be downsized, and the cellular phone radio per se is also expected to be lighted in weight. However, the conventional reader/writer of this application conducts only information interchange with a memory of a built-in contact type IC card (or the built-in contactless IC card) or an external contactless IC card, and it is not supposed that information is interchanged between the built-in contact type IC card (or the built-in contactless IC card) and the external contactless IC card.

[0010] As described above, up to now, it is supposed that the contactless IC media is embedded in a card-shaped medium and used in the card unit. However, the contactless IC media is not naturally limited to the conventional application mode. Also, it can be expected that the IC media is put to practical use not only in a specific field but also in various fields where the information communication is intervened for general purposes.

[0011] Under the above circumstances, an object of the present invention is to provide a contactless IC media excellent in general purposes.

[0012] Another object of the present invention is to provide an applied system which is capable of adding more values with the use of the contactless IC media.

DISCLOSURE OF THE INVENTION

[0013] In order to solve the above problem, according to the present invention, there is provided a contactless IC media characterized in that a contactless IC module having a recording area for recording computer readable digital information therein is embedded in a sheet-shaped medium of a given configuration, and an unseparable sticking member or a sticking member which can be again stuck after being separated exists on at least one surface portion of the sheet-shaped medium.

[0014] The contactless IC module is usefully portable because of the sheet configuration, and business card information including letter data and image data or encoded letter information can be recorded on the contactless IC module which is stuck on a business card, a postcard or the like.

[0015] The present invention is applied to not only the structure in which one contactless IC module is embedded in one sheet-shaped medium, but also a plurality of contactless IC modules are embedded in one sheet-shaped medium, and the respective contactless IC modules and the respective regions including portions at which the sticking members exist can be cut off in specific configurations. The contactless IC media thus structured can be mass-produced and is expected to remarkably reduce the costs. Also, such a contactless IC media can be readily carried by the user and is useful.

[0016] From the viewpoint of convenience of carriage, the contactless IC module can be embedded in a stick-shaped medium that can be installed in a stick-shaped housing.

[0017] Also, according to the present invention, there is provided a solid-type contactless IC media which is born by a media bearing member. The contactless IC media includes a solid-type module medium of a given configuration in which a contactless IC module having a recording region is embedded. The module medium is integral with an engagement mechanism that allows an engagement and disengagement with respect to the media bearing member by only displacing the position of the module medium so as not to be readily separated from the media bearing member.

[0018] When it is necessary to take the convertibility with the existing contact type IC card in use, an electrically conductive member for being rendered conductive to a contact of an external electronic circuit is disposed on a surface portion of the contactless IC module, and the contact type IC card is formed when the IC card is born by a recess of the card medium which is the same configuration as the media bearing member.

[0019] In order to solve the above other problem, according to the present invention, there is provided a contactless reader/writer comprising a media bearing member for bearing a contactless IC media having a recording region; a radio transceiver circuit including an antenna; and a control circuit for controlling read and write of digital information with respect to both of the recording regions of the contactless IC media which is born by said media bearing member and an external contactless IC media within a coverage of said antenna through said radio transceiver circuit.

[0020] The antenna is embedded in a housing part (for example, a cap that forms a partial structural element of the housing of the contactless reader/writer) positioned between the born contactless IC media and the external contactless IC media. Preferably, the antenna is embedded in the vicinity of the outermost periphery of the housing part so that the coverage of the antenna is not reduced by the housing of the contactless reader/writer.

[0021] A plurality of contactless IC media are born by the media bearing member, and the read control and the write control of the digital information with respect to the recording region of any contactless IC media may be selectively conducted through a single or a plurality of radio transceiver circuits. In the case of using a plurality of radio transceiver circuits, it is preferable that, for example, those radio transceiver circuits are operated under the respective different conditions or at the respective different timing, and the read control and the write control of the digital information with respect to the recording region of the contactless IC media suited for the above operating condition among the plurality of contactless IC media is selectively conducted.

[0022] According to the present invention, there is provided a contactless reader/writer comprising: a mov-

IPR2025-00645 Page 00092

able media bearing member which is capable of bearing a plurality of contactless IC media each having a digital information recording region on the same plane at the same time; a radio transceiver circuit having an antenna which is disposed at a specific position in parallel with said media bearing member; and a displacement mechanism which displaces said media bearing member on the plane so that said plurality of contactless IC media approach the specific position; wherein the digital information is transmitted/received with respect to a specific contactless IC media through said antenna.

[0023] Also, according to the present invention, there is provided a contactless reader/writer comprising: a media bearing member which is capable of bearing a plurality of contactless IC media each having a digital information recording region at the same time; a read/write mechanism bearing member on which a media read/write mechanism including an antenna and a radio transceiver circuit are mounted; and a displacement mechanism that displaces said read/write mechanism bearing member so that a specific one of said plurality of contactless IC media approach said antenna; wherein digital information is transmitted/received with respect to the specific contactless IC media through said antenna.

[0024] In the above contactless reader/writer, the media bearing member specifically includes a plate-shaped holder which is capable of bearing said plurality of contactless IC media at regular intervals at the same time. Said displacement mechanism brings the specific contactless IC media in close contact with said antenna.

[0025] The contactless reader/writer according to the present invention not only merely interchanges the digital information with respect to the contactless IC media or the external contactless IC media, but also realizes the same function as a function given to the contactless IC media on the basis of the recording region of the born contactless IC media. With this structure, the contactless IC media or the contactless IC card on which the contactless ICmedia is mounted can be recognized by an external electronic device or the like.

[0026] The contactless reader/writer includes information processing means that executes information processing on the basis of the digital information read through said control circuit, and the information processing result by the information processing means is recorded on the digital information reader, thereby being capable of reducing a range of a design modification of the electronic device side on which the contactless reader/writer should be mounted.

[0027] Also, the contactless reader/writer according to the present invention is accommodated in the card medium used in the information processing device on which the card reader/writer is mounted, thereby being capable of realizing a plurality of functions by one card medium.

[0028] Further, according to the present invention, there is provided a portable communication device which is capable of enhancing an added value with the use of a contactless IC media.

[0029] The portable communication device records, for example, sound source data and image data outputted in association with the sound source data on a single or a plurality of contactless IC media in a portable communication device on which a display is mounted or a portable communication device on which a display and a sound producing mechanism are mounted. Also, the portable communication device includes: a radio transceiver circuit having an antenna which is embedded in a device housing; a control circuit that reads the sound source data and the image data from any one of a contactless IC media born by said media bearing member and an external contactless IC media within a coverage of said antenna; information processing means having a sound source controller that allows the sound producing mechanism to reproduce a sound on the basis of the read information and/or a display controller that allows an image to be displayed on said display; wherein the recorded information of the contactless IC media can be visually or acoustically grasped.

[0030] In a portable communication device drivable by a battery, there are provided a coil for receiving an electric power component from the external in a contactless manner; and a charging circuit that converts the electric power component received through the coil into a charge electric power having a given value to charge said battery with the converted charge electric power; wherein the battery is charged with the use of the reader/writer function in the contactless manner.

[0031] Further, according to the present invention, there is provided various information transmission systems using a contactless IC media.

[0032] A first information transmission system includes: a portable communication device on which a contactless reader/writer according to the present invention is mounted; and a media issuance device that records digital information corresponding to a given value information on the contactless IC media and issues the digital information; wherein a kind of the digital information to be recorded on the contactless IC media can be arbitrarily selected in accordance with the value information. The media issuance device is so designed as to periodically update the digital information corresponding to the same value information, for example, periodical publication article information including letter data. The digital contents including an image, a sound or the like may be recorded on the contactless IC media and then issued.

[0033] A second information transmission system includes: a contactless IC media on a surface portion of which guide information which can be visually recognized by a person is described, and in an internal recording region of which mechanically readable digital information representative of the contents corresponding to the guide information is recorded; and a portable communication device according to the present invention

IPR2025-00645 Page 00093

which includes means for reproducing the digital information read from the contactless IC media; wherein said contactless IC media are dispersed at a plurality of appropriate positions, respectively. A plurality of contactless IC media may be embedded in the same guide panel on which the guide information is described.

[0034] A third information transmission system includes: a plurality of portable communication devices each including a single or a plurality of IC media and a contactless reader/writer according to the present invention; wherein each of the portable communication devices can mutually interchange the recorded information of the contactless IC media of the subject communication device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0035]

Fig. 1(a) is a front view showing a sheet on which a plurality of circular contactless IC media are formed, and Fig. 1(b) is a front view showing a sheet on which a plurality of plug-type contactless IC media are formed;

Fig. 2 is a perspective view showing the appearance of a stick-type contactless IC media;

Figs. 3(a) to 3(c) are diagrams showing an engagement mechanism that allows the engagement and disengagement of the contactless IC media with respect to a media holder by only displacement of the position of the engagement mechanism, in which Fig. 3(a) is a front view showing a media engagement mechanism at a media holder side, Fig. 3(b) is an explanatory diagram showing the engagement mechanism at a module medium side, and Fig. 3(c) is an explanatory diagram showing the application state;

Fig. 4 is a structural diagram showing a contactless reader/writer in accordance with a first embodiment;

Fig. 5 is a structural diagram showing a contactless reader/writer in accordance with a second embodiment;

Fig. 6 is a structural diagram showing a contactless reader/writer in accordance with a third embodiment in which one antenna is provided;

Fig. 7 is a structural diagram showing a contactless reader/writer in accordance with the third embodiment in which two antennas are provided;

Fig. 8 is a structural diagram showing a contactless reader/writer in accordance with a fourth embodiment in which one antenna is provided;

Fig. 9 is a structural diagram showing a contactless reader/writer in accordance with the fourth embodiment in which the number of antennas is identical with that of coin-type media;

Figs. 10(a) to 10(d) are structural diagrams showing a contactless reader/writer in accordance with a fifth embodiment and showing the structure of the contactless reader/writer in which a specific media is selected from a plurality of coin-type media, and data is read/written with respect to the selected media;

Figs. 11(a) to 11(c) are structural diagrams showing a contactless reader/writer in accordance with a sixth embodiment an showing the structure of the contactless reader/writer in which a specific media is selected from a plurality of coin-type media, and data is read/written with respect to the selected media;

Figs. 12(a) to 11(c) are structural diagrams showing a contactless reader/writer in accordance with a seventh l embodiment, in which Fig. 12(a) is a structural diagram showing the main portion of a contactless reader/writer mounted on a cellular phone radio that operates by means of a battery, Fig. 12(b) is a structural diagram showing the main portion of a contactless reader/writer mounted on a charging device, and Fig. 12(c) is an explanatory diagram showing the application state of the contactless reader/writer during charging;

Figs. 13(a) to 13(c) are structural diagrams showing a contactless reader/writer in accordance with an eighth embodiment, in which Figs. 13(a) and 13(b) are diagrams showing the structure of a PC card on which the contactless reader/writer is mounted, and Fig. 13(c) is an explanatory diagram showing the application mode of the PC card;

Fig. 14 is an explanatory diagram showing a use state of an image recording card for a digital camera on which a contactless reader/writer is mounted;

Fig. 15 is a perspective view showing the appearance of a cellular phone radio with which the contactless reader/writer shown in Fig. 4 or 5 is integrated;

Fig. 16 is a conceptual explanatory diagram showing an example of an application mode of the cellular phone radio;

Fig. 17 is a conceptual explanatory diagram showing another application mode of the cellular phone radio;

Fig. 18 is a cross-sectional view showing a cellular phone radio on which a contactless reader/writer is mounted where a plurality of coin-type media can be stacked one on another.

Fig. 19 is a cross-sectional view showing a cellular phone radio on which a contactless reader/writer is mounted where a plurality of coin-type media can be stacked one on another, and a plurality of antennas are provided;

Fig. 20 is a perspective view showing the appearance of a cellular phone radio on which a contactless reader/writer is mounted where a plurality of coin-type media can be arranged in parallel and one antenna is provided;

Fig. 21 is a perspective view showing the appearance of a cellular phone radio on which a contact-

IPR2025-00645 Page 00094

less reader/writer is mounted where a plurality of coin-type media can be arranged in parallel and antennas of the same number as that of the coin-type media are provided; and

Fig. 22 is a structural diagram showing a system which converts an article of a newspaper, a weekly magazine or a monthly magazine into digital information while periodically updating the article and offers the article to a user.

BEST MODE FOR CARRYING OUT THE INVENTION

[0036] Subsequently, embodiments of the present invention will be described in detail with reference to the accompanying drawings.

1. EMBODIMENT OF CONTACTLESS IC MEDIA

[0037] First, a contactless IC media according to an embodiment of the present invention will be described.

(1) Sheet-shaped contactless IC media

[0038] Fig. 1(a) is a front view showing a sheet la on which a plurality of circular contactless IC media 11 are formed, and Fig. 1(b) is a front view showing a sheet 1b on which a plurality of plug-type contactless IC media 12 are formed.

[0039] Notch portions 11a and 12a are formed along the outer peripheries of the respective contactless IC media 11 and 12 in the respective sheets 1a and 1b so that the contactless IC media 11 and 12 can be cut off from the respective sheets la and 1b one by one at the time of using the contactless media 11 and 12. Each of the contactless IC media 11 and 12 is designed in such a manner that a contactless IC module is embedded, for example, in a sheet medium made of thin resin, and a sticking member adheres to an entire or partial back surface of the contactless IC module. The sheet medium is subjected to a surface treatment so that the sheet medium can be printed, and as occasion demands, the sheet medium is subjected to water proofing. In an intended use that needs to maintain security, for example, in the case of adhering the contactless IC media to a finance card or the like in use, the contactless IC media is adhered to a card medium with an unseparable resin adhesive. In an intended use that does not always require the security, the contactless IC media 11 and 12 are made of a raw material which can be again adhered to other portions after the contactless IC media 11 and 12 are separated from portions to which the contactless IC media 11 and 12 are adhered. The latter sticking member can be more simply realized by use of a slow cure adhesive. A magnetic agent may be adhered to the sticking member through a shield member that magnetically shields the contactless IC module from the magnetic agent.

[0040] The contactless IC module may be formed of a known IC module including a radio transceiver circuit having an antenna and an IC portion. The IC portion is formed with at least a digital information recording region and a control circuit that controls data write and read between the radio transducer circuit and the recording region.

[0041] The recording of the digital information in the recoding region may be conducted ex post facto by a contactless reader/writer which will be described, or may be conducted at the time of producing a module in advance. Also, in the case where the control circuit can be replaced by a reader/writer side control circuit, the control circuit in the IC portion may be omitted.

[0042] The contactless IC media 11 and 12 thus structured can be adhered to an arbitrary position where the contactless reader/writer can read the digital information from the recording region. For example, the contactless IC media 11 and 12 can be adhered to a contactless reader/writer main body or an electronic device on which the contactless reader/writer is mounted in use.

[0043] Also, the profile, the address, the telephone No. of an individual or a company, etc., are recorded on the contactless IC media 11 and 12 in the form of letter information and image information, and the contactless IC media 11 and 12 are adhered to a mount of a business card or a pamphlet and then distributed to other persons. Information to be printed is recorded on the contactless IC media 11 and 12, and the contactless IC media 11 and 12 are adhered to a printed matter. Information to be mailed is recorded on the contactless IC media 11 and 12, and the contactless IC media 11 and 12 are adhered to the mail, or the contactless IC media 11 and 12 on which propaganda information on a company consisting of multi-media data is recorded are adhered to the leaflet of "company's prospectus" and then distributed. Thus, various use modes can be applied.

[0044] In the case where the contactless IC media 11 and 12 are adhered to the mount of the business card, if a logo mark of the company or the like is printed on a front surface of the contactless IC media 11 and 12, and the contactless IC media 11 and 12 are then adhered to a predetermined position of the mount, "electronic business card" which is not strange as compared with the normal business card can be realized.

[0045] The advantages obtained by realizing the electronic business card are as follows:

[0046] The manual input of data when the business card information is edited and managed by an electronic device becomes unnecessary.

[0047] The business card information can be utilized as it is in a device that automatically dials on the basis of phone No. information or a device that sets a destination of navigation or the like on the basis of address information.

[0048] Information on company's prospectus, a product catalog, a descriptive pamphlet, information, a written contract and so on can be recorded on the contact-

IPR2025-00645 Page 00095

less IC media 11 and 12 in addition to the information printed on the surface of the mount.

[0049] If voice information is recorded on the contactless IC media 11 and 12 together with the business card information as digital data, the individual information and the company information can be versatilely expressed.

[0050] When visiting a customer, the user carries one electronic business card so that the electronic business card can be read by a customer's reader/writer with the results that a binding of a pamphlet and carrying of the binding become unnecessary. The contactless IC media having the recorded information changed according to the intended use can be arbitrarily selected. For example, in case of an intended use that requires only the name, the address, the phone No., and so on, it is sufficient to prepare only an electronic business card having a small capacity, and it is not always necessary to distribute an expensive business card large in memory capacity on which all information is recorded.

[0051] Also, digital contents including periodical publication article information such as a newspaper or a magazine, a photographic image or a graphic image, sound data such as a voice, BGM or bird sound, etc., may be recorded on a plurality of contactless IC media 11 and 12 at the same time so that those contactless IC media 11 and 12 can be sold one by one. A person who receives the contactless IC media 11 and 12 reads digital information from the recording region through a contactless reader/writer which will be described later or a normal contactless reader/writer and conducts required information processing, display processing on a display, etc.

[0052] The contactless IC media according to the present invention may be embedded in the sheets 1a and 1b, or a single contactless IC module may be embedded in a sheet medium. For example, the contactless IC module can be embedded in a postcard to provide an IC postcard, or the IC module can be embedded in the above-mentioned mount of the business card to provide an IC business card mount.

(2) Stick-shaped contactless IC media

[0053] Fig. 2 is a diagram showing the appearance of an example of a stick-type contactless IC media.

[0054] A contactless IC media 13 is structured in such a manner that a contactless IC module is embedded in a stick-shaped medium 1c having a recess 1d identical in configuration with an upper end portion of a stick-shaped housing, for example, a pen-shaped housing such as a writing implement.

[0055] The contactless IC media 13 thus structured enables the recorded information to be read therefrom or the digital information to be recorded thereon only if the upper end portion of the pen-shaped housing approaches a contactless reader/writer not shown. The contactless IC media 13 where a processor is not mounted on the IC portion but only a data recording region is formed can be used, for example, for an intended use that data is intended to be recorded instantly, or for recording the digital information for only the purpose of reproduction. In the case where a processor and an application program recording region are formed on the IC portion in addition to the data recording region, higher-graded information processing can be conducted, for example, the execution result of application program by the processor can be transmitted to the reader/writer side, or the execution result can be saved in the data recorded region instantly.

(3) Solid-type contactless IC media

[0056] The contactless IC media according to the present invention is not only sheet-shaped or stick-shaped, but also may be formed of a solid-type media having a certain configuration.

[0057] In this example, a coin-type media is exemplified as one example. The coin-type media is born by a media holder (a media bearing member), a portable audio device, a notebook personal computer, a portable game machine, a digital camera, a cellular phone radio, a portable terminal (PDA), a wrist watch, a card medium or the like in an interchangeable state, in use.

[0058] The coin-type media is formed in such a manner that a known contactless IC module is embedded in a coin-shaped module medium. The coin-shaped module medium is basically sufficiently of a simple structure that the module medium can be born by the media holder. However, for example, in the case where the module medium is used in a state where the module medium is exposed from the media holder, in order to prevent the module medium from being separated from the media holder in use, the configuration and the structure need to be devised. In this embodiment, an engagement mechanism that allows the engagement and disengagement of the module medium with respect to the media holder by only displacement of the position of the engagement mechanism is integrated with the module medium.

[0059] The engagement mechanism corresponds to a media engagement mechanism 31 at the media holder side as exemplified in Fig. 3(a), and its specific structure is shown, for example, in an upper portion of Fig. 3(b). That is, projections 10a that can be engaged with the media engagement mechanism 31 are formed integrally with a rear surface of a coin-shaped module medium 10. When the coin-shaped module medium 10 is used, as shown in Fig. 3(c), the module medium 10 is inserted into the media engagement mechanism 31 and relatively rotated so as to be engaged with the media engagement mechanism 31. When the module medium 10 is disengaged from the media engagement mechanism 31, the module medium 10 is rotated in a counter direction to a rotating direction at the time of engagement.

[0060] If the structure shown in the figures is replaced

IPR2025-00645 Page 00096

by a structure in which a hinge member a thickness of which changes in a tapered shape in an engaging direction is integrated with a part of the outer peripheral portion of the module medium, and the media engagement mechanism can be engaged with the module medium when the thickness of the hinge member reaches an end of the tapered shape, the configurations and the structures of the module medium and the media holder can be more simplified.

[0061] Also, the above description is given of an example of the coin-type media, but if the same engagement mechanism is formed in case of a plug-type media or a solid-type media having another configuration, the module medium can be prevented from being readily disengaged from the media holder. It is needless to say that even if the sheet-shaped contactless IC media 11 shown in Fig. 1(a) is adhered to the coin-shaped module medium, the IC media can be employed as the above-mentioned coin-type media.

[0062] In case of a card medium identical in configuration with the general-purpose IC card, when the card medium is intended to be used as the contact type IC card in addition to the contactless IC card in the state where the media holder interchangeably bears the solid-type media, an electrically conductive member is deposited or adhered on a surface portion of the contactless IC media. The electrically conductive member is so designed as to be rendered conductive to a contact of an external electronic circuit, and is normally connected in parallel with a contact portion of the radio transceiver circuit and the IC portion.

[0063] The electrically conductive member may be deposited or adhered onto a surface of the sheet-shaped contactless IC media 11 and 12 shown in Figs. 1(a) and 1(b).

2. Contactless reader/writer

[0064] Subsequently, a description will be given of an embodiment of a contactless reader/writer for using the contactless IC media according to the present invention, or for realizing the same function as that given to the contactless IC media by using the contactless IC media.

[0065] This embodiment shows an example of using a simple structure, that is, a coin-type media 20 without the provision of the above-mentioned engagement mechanism 10a as the contactless IC media. Similarly, if the above-mentioned sheet-shaped contactless IC media 11 is adhered to the coin-shaped module medium, the IC media can be employed as the coin-type media 20.

(1) FIRST EMBODIMENT

[0066] Fig. 4 is a structural diagram showing a contactless reader/writer in accordance with a first embodiment and shows a basic structure of other contactless reader/writers which will be described below.

[0067] A contactless reader/writer 40 intervenes an antenna 42 between a media holder 41 for bearing an internal coin type media 20b and another external coin type media 20a. The antenna 42 is normally embedded in a housing cap of the contactless reader/writer. The antenna 42 is connected with a transceiver circuit 43, and the transceiver circuit 43 is connected with a control section 44, a power supply section 47 and a clock supply section 48. The power supply section 47 is so designed as to output a power component which is superimposed on a carrier wave in the transceiver circuit 43, and the clock supply section 48 is so designed as to output a clock component, having a predetermined period which is superimposed on the carrier wave. The control section 44 controls the operation of reading recorded information from a memory (M) 45, the operation of writing the information in the memory 45, a timing of transmit/receive waves in the transceiver circuit 43 and communication of information with respect to the external electronic circuit through an external interface (I/F) 46. The control section 44 also has a function of preventing congestion between a plurality of coin type media due to a known anti-collision system.

[0068] Each of the coin type media 20a and 20b includes at least an antenna 21, a transceiver circuit 22, a control circuit 23 and a memory 24.

[0069] The control circuit 23 produces an electric power and clocks on the basis of a power component and a clock component which are received from the contactless reader/writer 50 through the antenna 21 and the transceiver circuit 22 and adjusts the operating environments of the contactless module. Also, the control circuit 23 also controls the operation of writing data into the memory 24 (data IN) and the operation of reading data from the memory 24 (data OUT), and transmits the read data, commands and so on to the contactless reader/writer 40 side through the transceiver circuit 22 and the antenna 21. In the memory 24 are recorded identification data for identifying the coil type media, data inherent to the user, simple application program, data, digital contents and so on, as occasion demands.

[0070] In case of an intended use that requires the security, a processor that serves as one information processing means is disposed in the coin type media 20b, and a code key, a decode key and a code algorism which are readable by the processor are recorded on the memory 24. With this structure, the same function as that given to the coin type media 20b, that is, the encoding function and the decoding function can be realized by the contactless reader/writer 40. Likewise, in the case where application program of an execute form is recorded in the memory 24 of the coin type media 20b, the application program can be executed by the contactless reader/writer 40. Also, the executed result of the application program can be recorded in the memory 24 of the coin type media 20b.

[0071] The transmit/receive of information between the contactless reader/writer 40 and the coin type media

IPR2025-00645 Page 00097

20a, 20b can be realized by the same operating environment as that of the normal contactless reader/writer and the contactless IC card.

[0072] For example, the transmission of information from the contactless reader/writer 40 to the coin type media 20a and 20b can be conducted by using a signal resulting from ASK-modulating a radio carrier wave of 13.56 [MHz], and the transmission of information from the coin type media 20a and 20b to the contactless reader/writer 40 can be conducted by using a signal resulting from load-modulating sub-carrier waves (847.5/423.7 [kHz]) combining a plurality of signals of 13.56 [MHz] together. As with the conventional contactless IC card, a clock component and a power component in addition to a data component are transmitted to the coin type media 20a and 20b from the contactless reader/writer 40.

[0073] The contactless IC card thus structured can conduct information read control and information write control with respect to the recording regions of both of the internal coin type media 20a and the external coin type media 20a within the coverage of the antenna 42 by means of the control section 44. This function does not exist in the conventional contactless reader/writer. Even if those two coin type media 20a and 20b exist at the same time, since the above-mentioned anti-collision function is effected and those coin type media 20a and 20b can be readily identified by decoding the identification data, data inherent to the user and so on which are recorded in the memories 24 of the respective coin type media 20a and 20b, there arises no problem.

(2) SECOND EMBODIMENT

[0074] Fig. 5 is a structural diagram showing a contactless reader/writer in accordance with a modified example of the above first embodiment, in which the elements identical in function are designated by like symbols for convenience. The contactless reader/writer 50 has two radio transceiver systems having the antennas which operate independently.

[0075] In other words, the antenna 42a, the transceiver circuit 43a, the power supply section 47a and the clock supply section 48a operate with respect to the external coin-type media 20a whereas the antenna 42b, the transceiver circuit 43b, the power supply section 47b and the clock supply section 48b operate with the coin type media born by the media holder 41. The control section 44 grasps the operating conditions of those coin type media and selectively conducts the read control and the write control of the digital information with respect to the recording regions of the external coin type media 20a and/or the born coin type media 20b.

[0076] In the contactless reader/writer 50 thus structured, since the data is transmitted and received between the external coin type media 20a and the internal coin type media 20b through the radio transceiver systems independent from each other, there hardly occurs a problem of congestion.

(3) THIRD EMBODIMENT

[0077] Figs. 6 and 7 are structural diagrams showing the contactless readers/writers 55 and 56 in which a plurality of coin type media 20 can be born by the media holder 51 at the same time, and the elements having the same functions as those in Fig. 4 are designated by like symbols.

[0078] Fig. 6 is an example in which one antenna 42 is used, and Fig. 7 is an example in which two antennas 42a and 42b are used.

[0079] In case of the contactless reader/writer 55 shown in Fig. 6, the control section 44 conducts the data read control or the data write control while shifting a timing between the plurality of coin type media 20, or conducts the data read control or the data write control with respect to only a returned response to a sent different command. With this operation, the control section 44 can selectively execute a plurality of application programs in a state where the plurality of coin type media 20 are born at the same time.

[0080] In case of the contactless reader/writer 56 shown in Fig. 7, the control section 44 conducts the data read control or the data write control under conditions different from each other according to the use. For example, in an intended use that requires real-time property, high-speed data read is conducted by using the antenna 42a, and in an intended use that requires a high quality property rather than the real-time property, the data read is conducted at a low speed and with a high quality. With this operation, the contactless reader/writer 56 enables multi-purpose data processing according to the use.

[0081] Although a description is omitted, the data read control or the data write control can be conducted with respect to the external coin type media through the antennas 42 and 42a, respectively.

(4) FOURTH EMBODIMENT

[0082] Fig. 8 is a structural diagram showing a contactless reader/writer 57 that conducts the data read control or the data write control through one antenna 42 between a media holder 52 which can bear a plurality of coin type media 20 in a state where those coin type media 20 are arranged on the same plane and those coin type media 20. The elements having the same functions as those in Fig. 4 are designated by like symbols for convenience.

[0083] The antenna 42 is embedded, for example, in a housing cap in parallel with the respective coin type media 20. The basic operation is identical with that in the contactless reader/write 55 shown in Fig. 6.

[0084] Fig. 9 is a structural diagram showing a contactless reader/writer 58 in which antennas 42 having the same number as that of the coin type media 20 arranged within the media holder 52 shown in Fig . 8 is disposed. Each of the antennas 42 is embedded in the

IPR2025-00645 Page 00098

housing cap in parallel with the coin type media 20. Although the basic operation is identical with the contactless reader/writer 56 shown in Fig. 7, since the individual antennas 42 can be brought in close contact with the coin type media 0, there is advantageous in that the occurrence of cross-talk can be reduced as compared with the cases shown in Figs. 7 and 8.

(5) FIFTH EMBODIMENT

[0085] Figs. 10(a) to 10(d) are diagrams showing the structure of a contactless reader/writer which selects a specific one to be subjected to data read/write from a plurality of coin type media.

[0086] The contactless reader/writer accommodates a movable media holder having a displacement mechanism within a housing and a radio transceiver system including a close-contact type antenna.

[0087] As shown in Fig. 10(a), the movable media holder is structured in such a manner that a plurality of hollow portions 62 having the same configuration as that of the coin type media 20 are formed in an annular plate 61 having substantially the same thickness as that of the coin type media 20, and a displacement mechanism 63 for rotating itself on the same plane is fixed onto a center portion of the annular plate 61.

[0088] Fig. 10(b) is an internal structural diagram showing a positional relationship of the movable media holder within a housing 64, Fig. 10(c) is a top view showing the housing 64, and Fig. 10(d) is a side cross-sectional view showing a contactless reader/writer 60. Reference numeral 61a denotes a housing window for accommodating the coin type media 20 in the hollow portions 62 or for disengaging the coin type media 20 from the hollowing portions 62, and reference numeral 65 is a close-contact type antenna.

[0089] In the contactless reader/writer 60 thus structured, a plurality of coin type media 20 on which different digital information, for example, application program and security data are recorded are accommodated in the hollow portions 62, and the user displaces the displacement mechanism 63 so that a desired coin type media 20 approaches the close-contact antenna 65. The digital information read through the close-contact antenna 65 is sent out to an external electronic device through an external interface circuit not shown. In this manner, an appropriate coin type media 20 can be selectively employed in accordance with the use.

[0090] The annular plate 61 is exemplified and it is needless to say that the annular plate 61 may be replaced by another plate differently configured. For example, the present invention encompasses a structure in which a plurality of hollow portions are arranged in a rectangular plate, a fan-shaped plate or the like, and the plate is reversibly slid on the same plane with the use of the displacement mechanism such as a gear so that a desired coin type media 20 approaches the close-contact type antenna. Also, the close-contact type antenna may be replaced by an antenna having a directivity.

(6) SIXTH EMBODIMENT

[0091] Figs. 11(a) to 11(c) are diagrams showing the structure of another contactless reader/writer that selects a specific one to be subjected to data read/write from a plurality of coin type media.

[0092] The contactless reader/writer accommodates a fixed media holder and a movable read/write mechanism bearing member on which a media read/write mechanism including an antenna and a radio transceiver system is mounted within a housing.

[0093] As shown in Fig. 11(a), the media holder is designed in such a manner that a plurality of hollow portions 72 for accommodating a plurality of coin type media 20 therein are formed in an annular plate having substantially the same thickness as that of the coin type media 20. The media holder is loaded at a predetermined position within a housing of the contactless reader/writer after it has born the coin type media 20. Reference numeral 73 denotes a hole defined in the center of the annular plate 71.

[0094] Fig. 11(b) is a structural diagram showing a read/write mechanism bearing member. This embodiment shows an example in which a mechanism that reads and writes digital information with respect to the coin type media 20 is structured by making an antenna, a radio transceiver circuit and its downstream circuits into a module. The read/write mechanism bearing member is structured in such a manner that a support member where a displacement mechanism 76 is formed in the center of an annular plate 75 having substantially the same diameter as that of, for example, the annular plate 71, the support member is slidably inserted into a hole 73 of the annular plate 71, and a module 74 having an antenna is embedded in a middle portion of the annular plate 75. The module 74 is embedded at a position where the antenna is brought in close contact with each of the plural coin type media 20 by rotation of the annular plate 75.

[0095] The contactless reader/writer 70 thus structured enables the same use mode as that in the fifth embodiment except that a member to be displaced is the module 74 including the antenna. That is, the annular plate 75 is allowed to rotate with the hole 73 as a fulcrum by manipulation of a displacement mechanism ring 76 by the user so that the antenna of the module 74 can approach a desired coin type media 20 as shown in Fig. 11(c).

[0096] It is needless to say that the annular plate 75 may be replaced by a plate having another configuration as in the media holder. Also, the module 74 may be replaced by a structure in which only the antenna and the radio transceiver circuit are embedded in the annular plate 75, and the downstream circuits are connected to an internal circuit of an electronic device on which the contactless reader/writer 70 is mounted through an

IPR2025-00645 Page 00099

electric contact disposed along a rotating path of the annular plate 75, and so on.

(7) SEVENTH EMBODIMENT

[0097] Fig. 12(a) is a structural diagram showing the main portion of a contactless reader/writer that is mounted on an electronic device actuated by a battery, for example, a cellular phone radio or a PDA. The contactless reader/writer 80 includes at least an antenna 42 embedded in a housing cap, a transceiver circuit 43 connected to the antenna 42, and a charging circuit connected to an output side of the transceiver circuit 43. The charging circuit 81 includes a constant voltage circuit 811 that supplies a constant voltage to the structural parts of a downstream reader/writer function from a power supply and stably outputs a power of a constant value to a charging terminal of a battery B.

[0098] Fig. 12(b) is a structural diagram showing the main portion of a contactless reader/writer 85 that is mounted on a charging device for charging an electronic device. The contactless reader/writer 80 includes an antenna 42 embedded in a housing cap, a transceiver circuit 43 connected to the antenna 42, a transceiver circuit 43 connected to the antenna 42 and a power converting circuit 86 for converting a commercial power into a charging power. The power converting circuit 86 corresponds to the power supply sections 47, 47a and 47b shown in Figs. 4 to 8.

[0099] The antenna 42 and the transceiver circuit 43 function as an electromagnetic induction coil that induces an electric power by means of electromagnetic induction at the electronic device side when the charging device side and the electronic device side approach each other.

[0100] In use, as shown in Fig. 12(c), an electronic device D1 is set in the vicinity of a charging device J1, and a charging power is supplied to the electronic device D1 side from the charging device J1 side through the contactless reader/writer 85. The contactless reader/writer 80 at the electronic device D1 side inputs the power induced by the antenna 42 and the transceiver circuit 43 to the charging circuit 81. The charging circuit 81 stabilizes the induced power to a constant value higher than a rated voltage of the battery B by means of the constant voltage circuit 811 and supplies the stabilized power to the charging terminal 82 of the battery B. As a result, the battery B of the electronic device DI is charged.

[0101] An exclusive charging device is normally provided in the electronic device D1, and the electronic device is set at a predetermined position of the charging device so that their contacts are brought in contact with each other, to thereby enable charging. Therefore, a charging device different in the model, the configuration and so on cannot be employed. However, in this embodiment, battery charging is enabled regardless of the model, the configuration and so on.

(8) EIGHTH EMBODIMENT

[0102] The contactless reader/writer according to the present invention can be mounted on a card medium such as a PC card in use. For example, a PC card 90 the appearance of which is shown in Fig. 13(a) accommodates a contactless reader/writer 91 in the interior of a housing and is formed with a media holder 92 for detachably bearing a coin type media 20 on a surface portion thereof. As shown in Fig. 13(b), a structure may be made in such a manner that a contactless reader/writer 95 having a media holder 96 forbearing aplurality of coin type media 20 is installed in an inner space 93 of a PC card 94. Application program and data are recorded on the coin type media 20.

[0103] The PC cards 90 and 94 are equipped into a card slot 97 of a personal computer or the like in use as shown in Fig. 13(c), and its use mode depends on the sort of the born coin type media 20. For example, the coin type media 20 can be employed as a rim-bubble recording device of a personal computer PC, employed as a recording medium of a program code read and executed by the personal computer PC, or employed as a transmission medium of electronic data read from an external electronic device. In case of a PC card having a communication function, communication environmental data can be saved in the coin type media 20 in use.

[0104] Also, as shown in Fig. 15, the PC card can be employed as an image record card of a digital camera DC. That is, the coin type media 20 is inserted into a card-shaped media holder 98, and photograph data is allowed to be recorded on the coin type media 20. Thereafter, the image record card 98 is inserted into a card slot 99 of the digital camera DC for saving the image data, etc. The image record card 98 is offered to a photo-laboratory or the like whereby a record image can be outputted to a printing sheet or outputted to a high-resolution printer.

(9) NINTH EMBODIMENT

[0105] The contactless IC reader/writer according to the present invention can be so structured as to execute information processing on the basis of read digital information in addition to read and write of the digital information (program code, data, etc.) with respect to the coin type media 20, 20a and 20b. Specifically, the contactless IC reader/writer includes a processor that reads and executes the digital information and a memory that records required program or the like thereon. The processor and the memory may be made into an IC chip and accommodated within the housing. The information processing result by the processor is outputted to a display or the like of an electronic device on which the contactless IC reader/writer is mounted and recorded on a digital information reading device.

[0106] Since the contactless IC reader/writer thus structured can conduct information processing only in-

IPR2025-00645 Page 00100

ternally by the processor, a range of a design modification at the electronic device side on which the contactless IC reader/writer is mounted can be reduced.

[0107] Also, the same function as that given to the coin type media can be easily realized on the basis of the digital information recorded on the coin type media.

3. PORTABLE COMMUNICATION DEVICE

[0108] Subsequently, a description will be given of an embodiment of a portable communication device on which the above contactless reader/writer is mounted. This embodiment shows an example of the cellular phone radio, but the present invention is not limited to this example. Also, the cellular phone radio includes a narrowly interpreted cellular phone as well as a PHS, a portable transceiver, an automobile phone and so on.

[0109] First, a description will be given of a cellular phone radio on which the above-mentioned contactless reader/writer 40, 50, 55, 56, 57 or 58 is mounted. Those contactless reader/writer may be built in the cellular phone radio as they are. However, this embodiment shows an example in which a cellular phone radio integrated with the contactless reader/writer.

[0110] Fig 15 is a perspective view showing the appearance of a cellular phone radio 110 where the contactless reader/writer 40/50 shown in Fig. 4 or 5 is integrated withtin the housing. The lower portion of the back surface of the cellular phone ratio 110 is formed with a media holder 111 for bearing the coin type media 20 and a cap 112. The antenna 42 is embedded in the cap 112 of the housing and becomes in parallel with the coin type media 20 when the cap 112 is closed.

[0111] In the cellular phone radio 110 thus structured, the coin type media 20 can be used as, for example, an SIM (subscriber identity module). A subscriber identity ID is recorded on the SIM. As a result, in the case where a new cellular phone radio 110 is purchased or the cellular phone radio 110 is selectively used according to the intended use, the SIM may be replaced. Also, it is possible to receive the same service through various cellular phone radios by replacing the SIM. That is, the cellular phone radio can be employed as in a public phone.

[0112] Also, as shown in Fig. 16, since the read and write of the digital information can be conducted with respect to the recording regions of both the coin type media 20b born by the media holder 111 and an external contactless IC card ICC, a coin type media 20a or a contactless IC media 20b' having another configuration, it is possible to access to the external contactless IC card ICC, the coin type media 20 or another system by using the security information recorded on the internal coin type media 20.

[0113] In the case where a processor or the like is provided in the contactless reader/writer as in the ninth embodiment, and the security information or the program code recorded on the internal coin type media is read to execute required information processing, the processing result can be recorded on the coin type media 20. For example, it is possible that the cellular phone radio 110 is spread before a POS terminal, an automatic vending machine, a portable settling terminal or the like to conduct electronic settlement processing, and its result is recorded on the coin type media.

[0114] As other applications that can be realized by the cellular phone radio 110, there is a prepaid card such as a gift card, a novelty card, a ticket card or a telephone card. Also, if the cellular phone radio 110 is spread before the prepaid card, a prepaid value can be taken in the interior of the cellular phone radio 110 so as to conduct the electronic settlement.

[0115] The name and the address are written in the memory region of the coin type media 20 by the cellular phone radio 110 per se, and the coin type media 20 can be utilized as an electronic business card. Also, if data is read and written with respect to the electronic business card by spreading the cellular phone radio 110 before a counterpart electronic business card, the convenience can be enhanced. In addition, it is possible that the identification data or the key information of an automobile owner is recorded on one coin type media, and the cellular phone radio 110 is used as an electronic key, or an automobile travel state is recorded on another coin type media, and utilized for analysis of the travel history.

[0116] Also, as shown in Fig. 17, the cellular phone radios 110 are permitted to approach each other so that the recorded information of the respective coin type media 20b can be exchanged.

[0117] Not only one coin type media 20 but also a plurality of coin type media 20 can be born at the same time. Fig. 18 is a cross-sectional view showing the cellular phone radio 120 having a media holder 121 which is capable of stacking a plurality of coin type media 20 one on another.

[0118] An antenna 42 is embedded in a cap 122. A cellular phone radio 120 is integrated with the contactless reader/writer 55 shown in Fig. 6. Fig. 19 is a cross-sectional view showing a cellular phone radio 130 integrated with the contactless reader/writer 56 shown in Fig. 7. An antenna 42a is embedded in a housing cap 132, and an antenna 42b is embedded in a bottom portion 133 of a media holder 131. Fig. 20 is a cross-sectional view showing a cellular phone radio 140 integrated with the contactless reader/writer 57 shown in Fig. 8, and Fig. 21 is a cross-sectional view showing a cellular phone radio 150 integrated with a contactless reader/writer 58 shown in Fig. 9. The antenna 42 is embedded in caps 142 and 152 corresponding to media holders 141 and 151 and become in close contact with the coin type media 20 in parallel when the caps 142 and 152 are closed.

[0119] The contactless readers/writers 60 and 70 having the structures shown in Figs. 10 and 11 can be integrated with the cellular phone radio.

[0120] It is normal that the cellular phone radios 110

IPR2025-00645 Page 00101

to 150 are provided with a display and a sound producing mechanism. The chip having a processor and so on shown in the ninth embodiment is mounted on the cellular phone radio so that required information processing can be executed on the basis of the digital information read from a plurality of coin type media 20.

[0121] The processor has a sound source controller that reproduces a sound on the basis of sound source data and a display controller that allows an image to be displayed on a display on the basis of image data, by executing the program code recorded on a memory. The sound source data is recorded on one of the coin type media 20, and the image data outputted in association with the sound source data is recorded on the other coin type media 20. Then, the sound source data is read so that the sound producing mechanism is permitted to reproduce a sound by the sound source controller, and an image is displayed on the display on the basis of the image data read in synchronism with the sound source data. The cellular phone radios 110 to 150 thus structured are used while the coin type media 20 are appropriately interchanged, whereby letter data is displayed on the display, and a voice or BGM (background music) corresponding to the letter data can be listened by a receiver or an ear phone.

[0122] For example, the cellular phone radio can be employed as a portable KARAOKE machine. That is, it is possible that a song is sung while the text is displayed on a display and melody is listened by an earphone, and the sung contents are recorded.

[0123] It is possible to only display the letter data or to produce the sound on the basis of the sound source data.

[0124] The above description is given of the cellular phone radio. However, the present invention can be applied to a personal computer, a portable terminal (PDA), a portable audio device and so on, likewise.

4. INFORMATION TRANSMISSION SYSTEM

[0125] Subsequently, a description will be given of an embodiment of an information transmission system to which the present invention is applied.

[0126] This embodiment shows an example in which information transmission is conducted by using the above-mentioned contactless IC media and portable communication device. As the portable communication device, there is used, for example, a cellular phone radio 110. The cellular phone radio 110 mounts a contactless reader/writer having the above-mentioned built-in processor, etc., thereon. In the case of using the contactless reader/writer, an appropriate function is assigned to one of the operation bottoms of the cellular phone radio 110.

(1) PERIODICAL PUBLICATION ARTICLE ISSUANCE SYSTEM

[0127] The system converts an article of a newspaper, a weekly magazine or a monthly magazine into digital information while periodically updating the article and offers the user the article. Fig. 22 is a structural diagram of the system. In the present specification, the digital information is directed to letter data, image data, digital contents and so on, and includes sound source data as occasion demands. As the contactless IC media for recording the digital information, the above-mentioned coin type media 20 is employed for convenience, however, it is needless to say that a sheet-shaped media may be used.

[0128] The periodical publication article issuance system 200 is made up of a cellular phone radio 210 that interchangeable bears the coin type media 20 and a media issuance device 220.

[0129] The media issuance device 220 includes a display 221, a data input device 222, a cash throwing-in mechanism 223, an input/output interface 224, an article database DB, and a media issuance mechanism 229. In addition, the media issuance device 220 includes the functional blocks consisting of a menu display section 225 formed by reading and executing a given program code by the internal processor, an article specifying section 226, a database management section 227 and an information recording section 228.

[0130] The menu display section 225 allows a menu screen for guiding the periodical article dealt with by the subject device to be displayed on a display 221 through the input/output interface 224. The data input device 222 inputs the select information on the periodical article. When the article specifying section 226 receives the select information on the specific article from the data input device 222 and cash throwing-in information (value information) from the cash throwing-in mechanism 223, the article specifying section 226 notifies the database management section 227 of information for specifying the periodical article. The database management section 227 reads the digital information from the article database DB on the basis of the information, and delivers the digital information to the information recording section 228. The information recording section 228 records the digital information on the coin type media 20 and issues it.

[0131] The guide information on the periodical article of the kind and contents according to an amount of money is displayed on a menu screen so that the user can arbitrarily select the guide information through the data input device 222. The contents of the article database DB is periodically updated by the database management section 227 on the basis of data transmitted from, for example, an external system. The publication article to be updated is updated every data if it is a newspaper, every week if it is a weekly magazine and every month if it is a monthly publication.

[0132] The user purchases the coin type media 20 on which the digital information is recorded from the media issuance device 220 and inserts the coin type media 20 into a media holder of the cellular phone radio 210 and

IPR2025-00645 Page 00102

permits the recorded information to be displayed on a display 211 by depression of an operating button. In the case where sound source data is also recorded on the coin type media 20, its contents are listened by a receiver or an earphone.

[0133] The information transmission system according to the present invention can be applied to a system that periodically or non-periodically issues the digital contents other than the periodical publication article information.

(2) INFORMATION GUIDE SYSTEM

[0134] An address, a postcode, a map code, an area announcement, an announcement of establishment, a train schedule, a business describing pamphlet or the like is made into digital information and then recorded on the contactless IC media. Then, the contactless IC media is embedded in a water-repellent plate and located or stuck on an appropriate place. The information is read from the plate by using a portable communication device on which the contactless reader/writer of the present invention is mounted, for example, the cellular phone radio and then displayed on a display. The place where the plate is located is, for example, a building or a telegraph in case of "the address, etc.", an address indicating board in case of "the map or the map code", the outer wall of the building in case of "the area announcement", the institution doorway in case of "the announcement of establishment", a wall surface of a station platform in case of "train schedule", and the doorway of a store or a business establishment in case of "trade prospectus".

[0135] The user depresses an appropriate operation button and spreads the cellular phone ration before those plates. As a result, the reader/writer function of the cellular phone radio is effected, and the digital information is read and visualized and displayed on a display.

[0136] A plurality contactless IC media can be embedded in the same guide panel on which the guide information is drawn or stuck on the guide panel. Also, a gate having a built-in contactless reader/writer is located on the gate of a concert or sports site so that side guide information can be delivered by spreading the cellular phone radio before the gate by the user.

INDUSTRIAL APPLICABILITY

[0137] As was described above, according to the present invention, the contactless IC media excellent in general purpose is obtained. Also, there can be provided an applied system which can add more values by using the contactless IC media.

Claims

1. A contactless IC media, characterized in that a contactless IC module having a recording area for recording computer readable digital information therein is embedded in a sheet-shaped medium of a given configuration, and a sticking member which is not separable after being adhered exists on at least one surface portion of the sheet-shaped medium.

2. A contactless IC media, characterized in that a contactless IC module having a recording area for recording computer readable digital information therein is embedded in a sheet-shaped medium of a given configuration, and a sticking member which can be again adhered after being separated exists on at least one surface portion of the sheet-shaped medium.

3. The contactless IC media as claimed in claim 1, characterized in that a plurality of contactless IC modules are embedded in one sheet-shaped medium, and the respective contactless IC modules and the respective regions including portions at which the sticking members exist can be cut out in specific configurations.

4. A contactless IC media where a contactless IC module having a recoding region is embedded in a sheet-shaped medium of a given configuration, characterized in that:

   information visible by a human is described on a surface portion of said sheet-shaped medium;
   mechanically readable digital information including the contents corresponding to said information is recorded on said recording region; and
   a sticking member for sticking the sheet-shaped medium on a position where a given digital information reading device can read said digital information is fixed onto a rear surface of said sheet-shaped medium.

5. A contactless IC media, characterized in that a contactless IC module having a recording region for recording at least digital information thereon is embedded in a stick-shaped medium having a structure which can be installed in a stick-shaped housing.

6. A contactless IC media of a solid type born by a media bearing member, characterized by comprising a solid-type module medium having a given configuration in which a contactless IC module having a recording region is embedded, and in that an en-

IPR2025-00645 Page 00103

gagement mechanism that allows the engagement and disengagement of said solid-type module medium with respect to said media bearing member by only displacing said engagement mechanism is integral with said solid-type module medium.

7. The contactless IC media as claimed in claim 1 or 5, wherein an electrically conductive member for being rendered conductive to a contact of an external electronic circuit is disposed on a surface portion of said contactless IC module, and a contact-type IC mounted card is formed by allowing a recess of a card medium having the same configuration as that of said media bearing member to be born by said media bearing member.

8. A contactless reader/writer comprising:

a media bearing member for bearing a contactless IC media having a recording region;
a radio transceiver circuit having an antenna; and
a control circuit for controlling the read and write of digital information with respect to both of the recording regions of a contactless IC media which is born by said media bearing member and an external contactless IC media having a recording region within a coverage of said antenna through said radio transceiver circuit.

9. The contactless reader/writer as claimed in claim 8, characterized in that said antenna is embedded in a housing part positioned between said born contactless IC media and said external contactless IC media.

10. A contactless reader/writer, comprising:

a media bearing member for bearing a contactless IC media having a recording region;
a first radio transceiver circuit that conducts communication with said contactless IC media born by said media bearing member through a first antenna in a contactless manner;
a second radio transceiver circuit that conducts communication with an external contactless IC media having a digital information recording region through a second antenna in a contactless manner; and
a control circuit that selectively conducts the read control and the write control of the digital information with respect to the recording region of said contactless IC media or said external contactless IC media through said first radio transceiver circuit or said second radio transceiver circuit.

11. A contactless reader/writer comprising:

a media bearing member which is capable of bearing a plurality of contactless IC media each having a recording region at the same time;
a radio transceiver circuit having an antenna; and
a control circuit that selectively conducts the read control and the write control of digital formation with respect to any recording region of said plurality of contactless IC media born by said media bearing member through said radio transceiver circuit.

12. A contactless reader/writer comprising:

a media bearing member which is capable of bearing a plurality of contactless IC media each having a recording region;
a plurality of radio transceiver circuits each having an antenna which operate under different conditions, respectively; and
a control circuit that selectively conducts the read control and the write control of digital information with respect to the recording region of a contactless IC media conforming to the operating condition among said plurality of contactless IC media born by said media bearing member through said plurality of radio transceiver circuits.

13. A contactless reader/writer, characterized by comprising:

a movable media bearing member which is capable of bearing a plurality of contactless IC media each having a digital information recording region on the same plane at the same time;
a radio transceiver circuit having an antenna disposed at a specific position which is in parallel with saidmedia bearing member; and
a displacement mechanism that displaces said media bearing member on said plane so that a specific one of said plurality of contactless IC media approaches said specific position;
wherein the digital information is received and transmitted between said specific contactless IC media and said antenna.

14. A contactless reader/writer, characterized by comprising:

a media bearing member which is capable of bearing a plurality of contactless IC media each having a digital information recording region at the same time;
a read/write mechanism bearing member on which a media read/write mechanism including an antenna and a radio transceiver circuit is mounted; and

IPR2025-00645 Page 00104

a displacement mechanism that displaces said read/write mechanism bearing member so that a specific one of said plurality of contactless IC media approaches said antenna;
wherein the digital information is received and transmitted with respect to said specific contactless IC media through said antenna.

15. The contactless reader/writer as claimed in claim 13 or 14, characterized in that saidmedia bearing member includes a plate-shaped holder which is capable of bearing said plurality of contactless IC media at given intervals at the same time; and
in that said displacement mechanism brings said specific contactless IC media in close contact with said antenna.

16. The contactless reader/writer as claimed in any one of claims 8 to 15, characterized in that the same function as a function given to said contactless IC media is realized on the basis of the digital information recorded on said born contactless IC media.

17. The contactless reader/writer as claimed in claim 16, characterized by further comprising information processing means for executing information processing on the basis of the digital information read through said control circuit;
wherein the information processing result by said information processing means is recorded on said specific contactless IC media from which the digital information has been read.

18. The contactless reader/writer as claimed in claim 16, characterized in that said contactless IC media is accommodated in a card medium used in an information processing device on which the card reader/writer is mounted.

19. A portable communication device on which a display is mounted, characterized by comprising:

a media bearing member for interchangeably bearing a contactless IC media having a recording region;
a radio transceiver circuit including an antenna embedded in a device housing;
a control circuit that conducts the read control and the write control of digital information with respect to both of recording regions of said contactless IC media born by said media bearing member and an external contactless IC media disposed within a coverage of said antenna; and
information processing means that executes information processing on the basis of said read digital information, displays the result information of the information processing on said display, and records the result information on the recording region of said born contactless IC media or said external contactless IC media through said control circuit.

20. The portable communication device as claimed in claim 19, characterized in that said control circuit selectively receives the digital information originated from a plurality of external contactless IC modules and stores the received digital information on said born contactless IC media.

21. A portable communication device on which a display and a sound producing mechanism are mounted, characterized by comprising:

a single or a plurality of contactless IC media on which sound source data and image data outputted in association with the sound source data are recorded;
a media bearing member that interchangeably bears a single or a plurality of contactless IC media;
a radio transceiver circuit having a housing embedded antenna;
a control circuit that reads the sound source data and the image data from any recording region of said contactless IC media born by said media bearing member and said external contactless IC media within the coverage of said antenna; and
information processing means having a sound source controller that permits said sound producing mechanism to reproduce a sound on the basis of said read sound source data and a display controller that permits said display to display an image on the basis of said read image data.

22. A portable communication device drivable by a battery, characterized by comprising:

a coil for receiving an electric power component from the external in a contactless manner; and
a charging circuit that converts an electric power component received through said coil into a charging electric power of a constant value and charges said battery by using the converted charging electric power.

23. An information transmission system, characterized by comprising:

a portable communication device including a media bearing member that interchangeably bears a single or a plurality of contactless IC media on which digital information is recorded,
a radio transceiver circuit having an antenna

IPR2025-00645 Page 00105

embedded in a device housing, a control circuit that reads the digital information from the recording region of said contactless IC media born by saidmedia bearing member through said radio transceiver circuit, and means for reproducing the read digital information; and
a media issuance device that records the digital information corresponding to a given value information on said contactless IC media and issues the digital information;
wherein the kind of the digital information to be recorded on said contactless IC media can be arbitrarily selected in accordance with the value information.

24. The information transmission system as claimed in claim 23, characterized in that said media issuance device periodically updates the digital information corresponding to the same value information.

25. The information transmission system as claimed in claim 23, characterized in that the digital information is periodical publication article information including letter data.

26. The information transmission system as claimed in claim 23, characterized in that the digital information is digital contents.

27. An information transmission system, characterized by comprising:

a contactless IC media on a surface portion of which guide information visible by a person is described and in an inner recording region of which mechanically readable digital information representative of the contents corresponding to the guide information is recorded; and
a portable communication device including a radio transceiver circuit having a housing embedded type antenna, a control circuit that reads the digital information from said contactless IC media through said radio transceiver circuit, and means for reproducing the read digital information;
wherein said contactless IC media are dispersed at a plurality of appropriate locations, respectively.

28. The information transmission system as claimed in claim 27, characterized in that said plurality of contactless IC media are embedded in the same guide panel on which the guide information is described.

29. An information transmission system, characterized by comprising:

a plurality of portable communication devices, each including: a media bearing member that interchangeably bears a single or a plurality of contactless IC media, a radio transceiver circuit having a housing embedded type antenna, and a control circuit that conducts the read control and the write control of the digital information with respect to both of recording regions of said contactless IC media born by said media bearing member and an external contactless IC media existing within a coverage of said antenna through said radio transceiver circuit;
wherein each of said portable communication devices can mutually interchange the recorded information of the contactless IC media with another portable communication device.

30. The information transmission system as claimed in any one of claims 23 to 29, characterized in that said portable communication device is a cellular phone radio.

IPR2025-00645 Page 00106

FIG. 1a

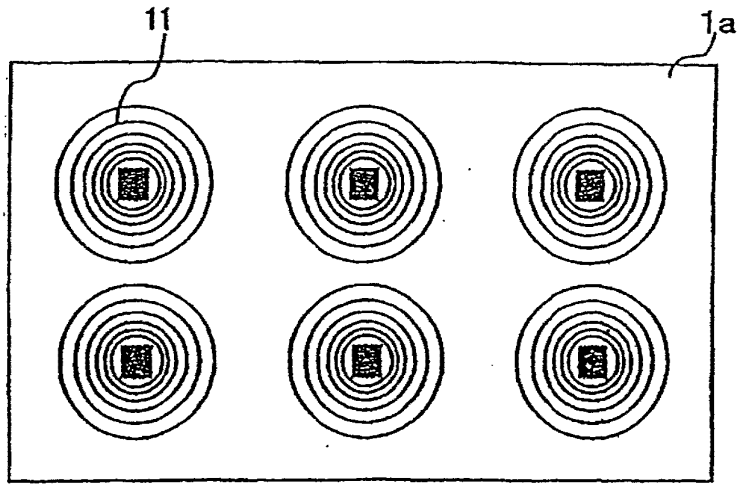
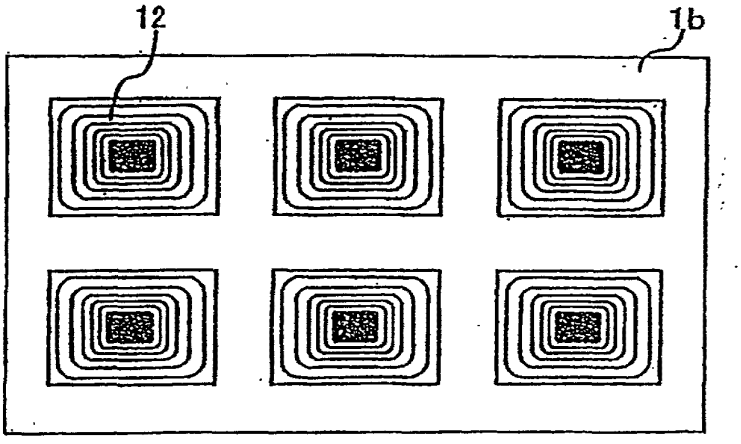


FIG. 1b



IPR2025-00645 Page 00107

FIG. 2

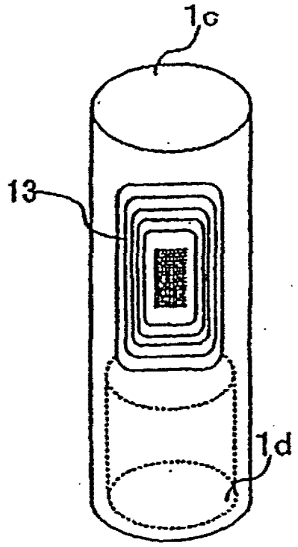
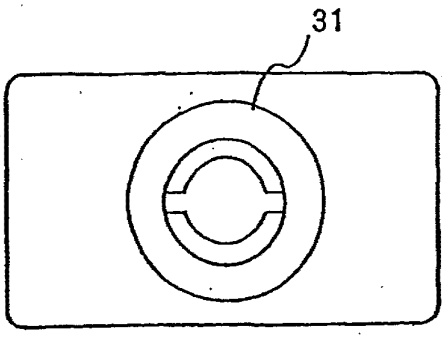


FIG. 3a



IPR2025-00645 Page 00108

FIG. 3b

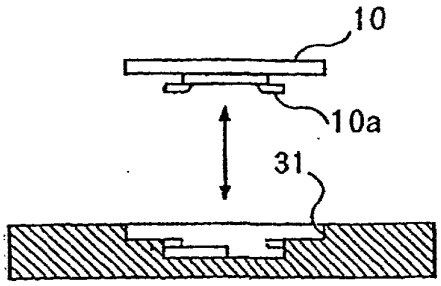
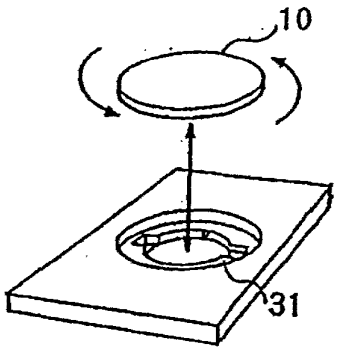


FIG. 3c



IPR2025-00645 Page 00109

FIG. 4

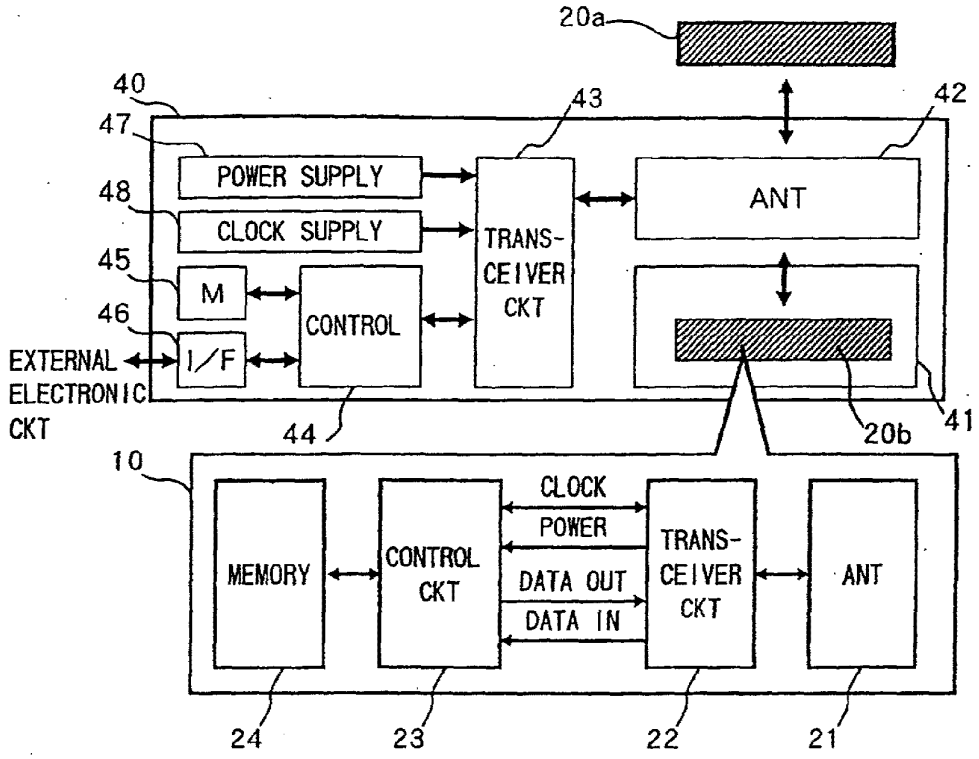
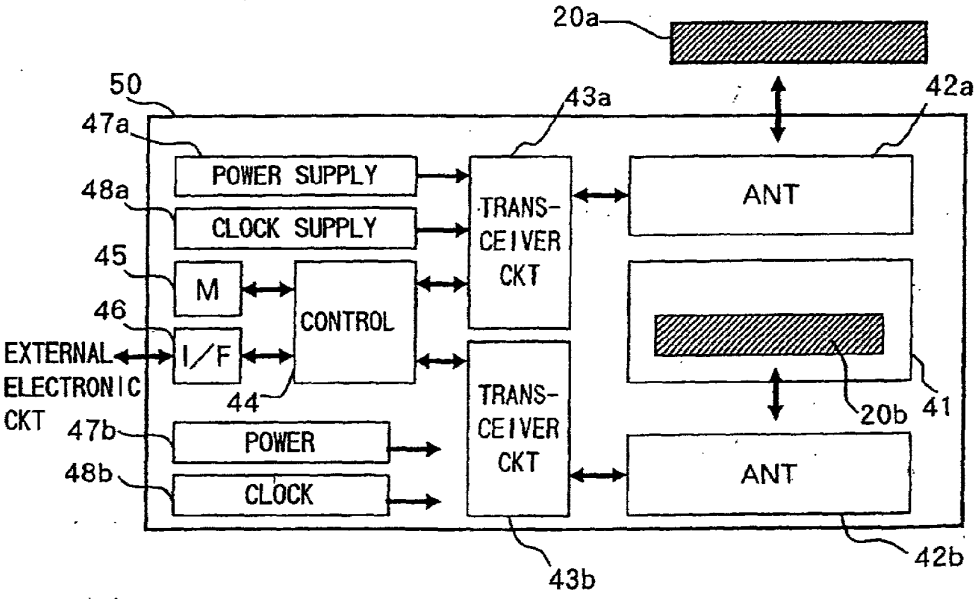


FIG. 5



IPR2025-00645 Page 00110

FIG. 6

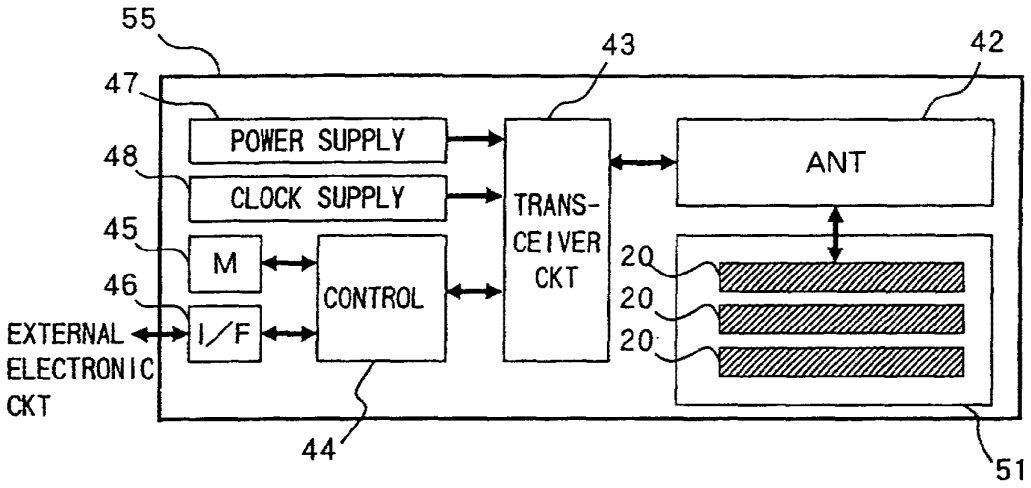
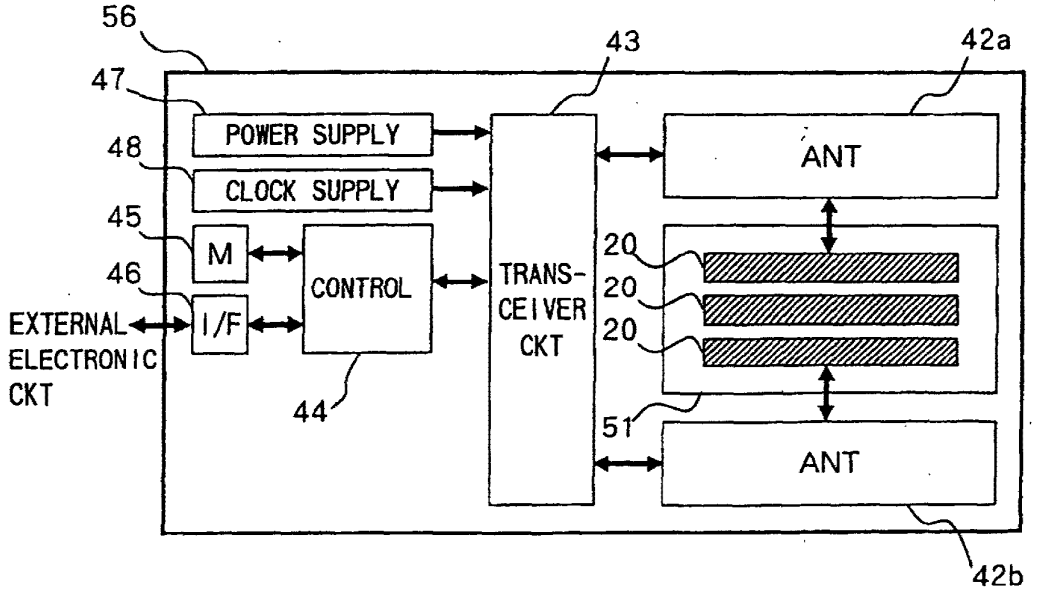
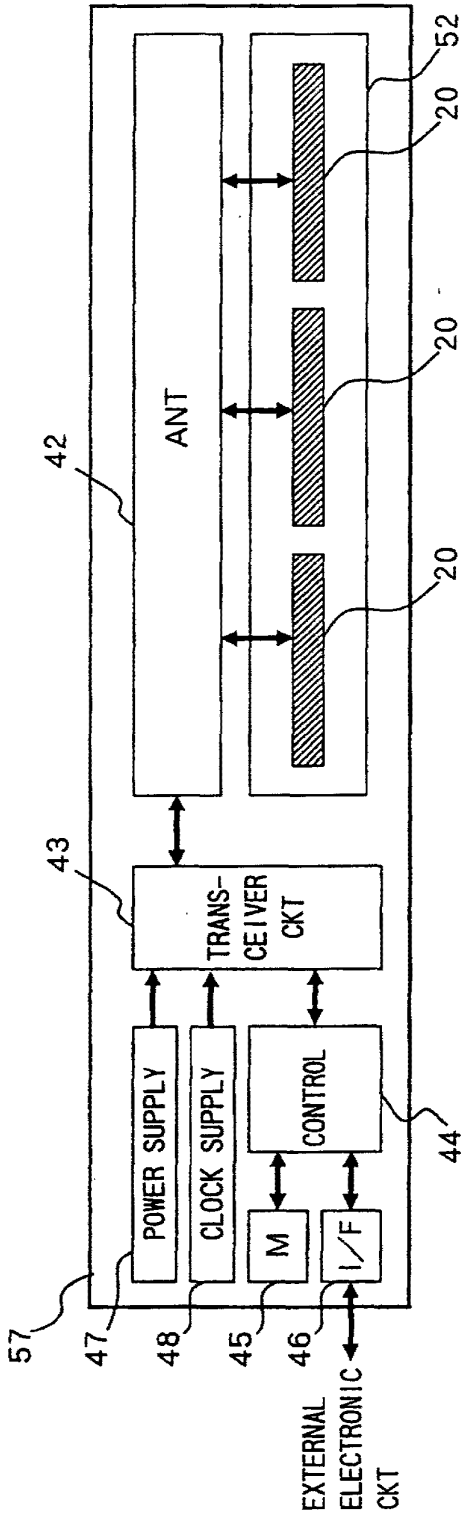


FIG. 7



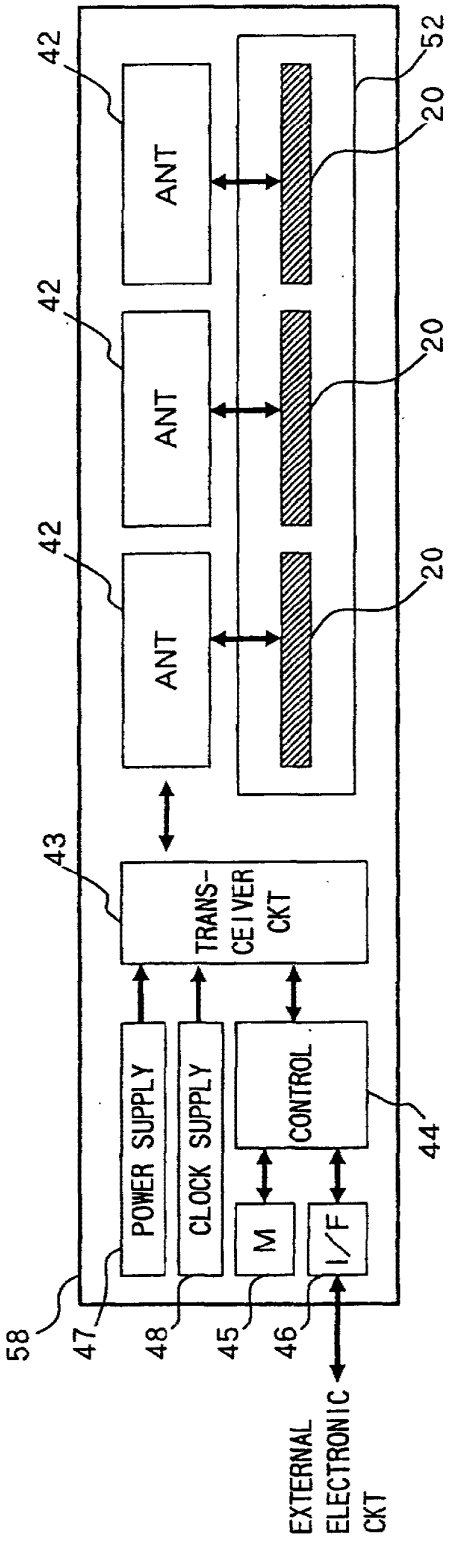
IPR2025-00645 Page 00111

FIG. 8



IPR2025-00645 Page 00112

FIG. 9



IPR2025-00645 Page 00113

FIG. 10a

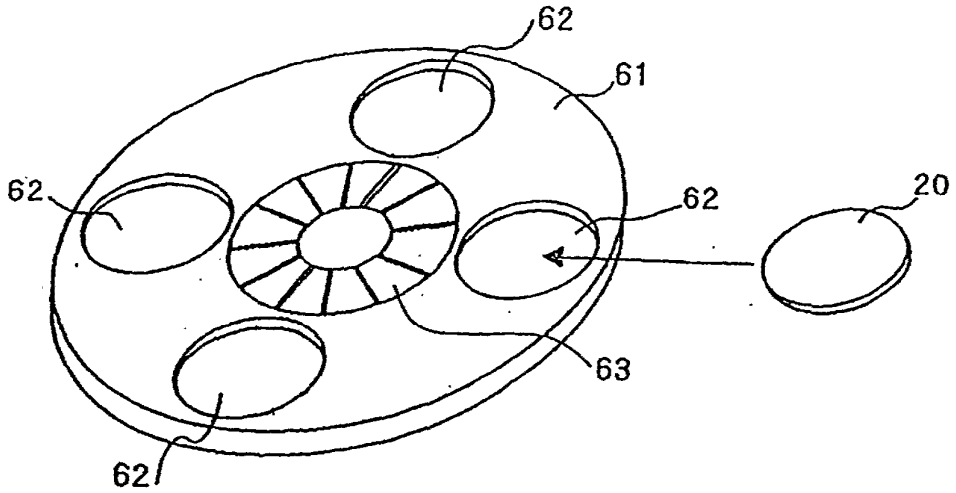
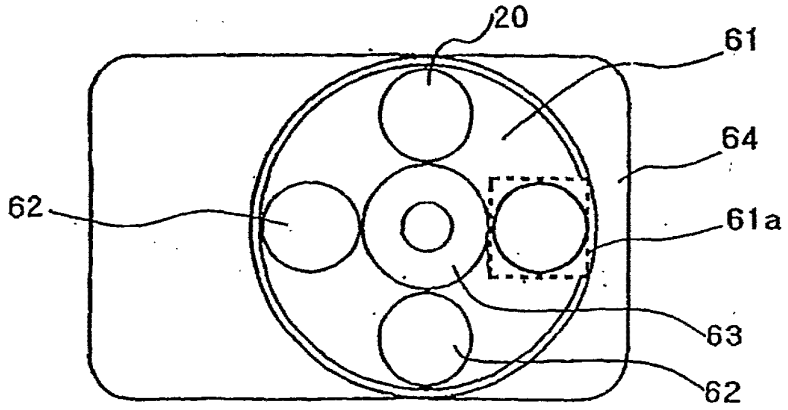


FIG. 10b



IPR2025-00645 Page 00114

FIG. 10c

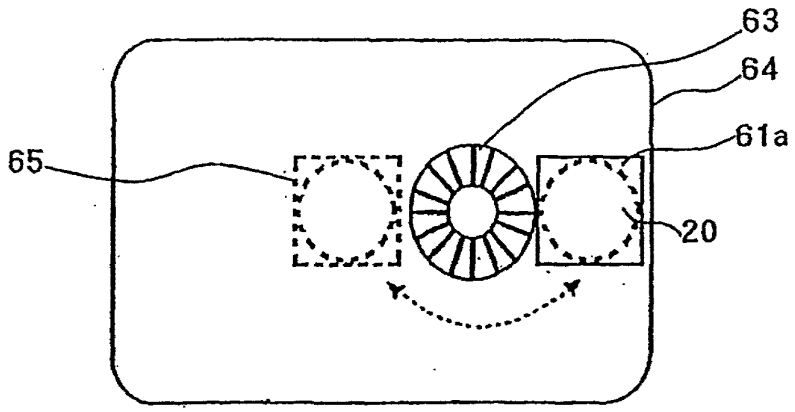
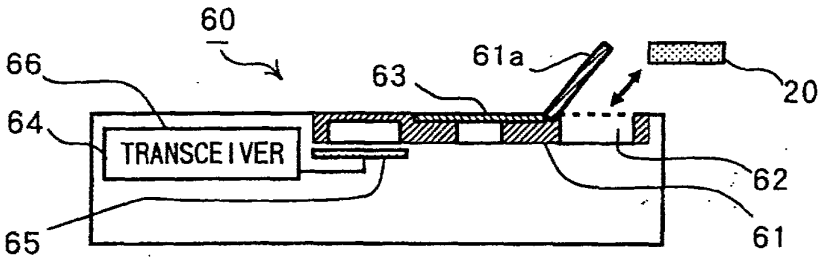


FIG. 10d



IPR2025-00645 Page 00115

FIG. 11a

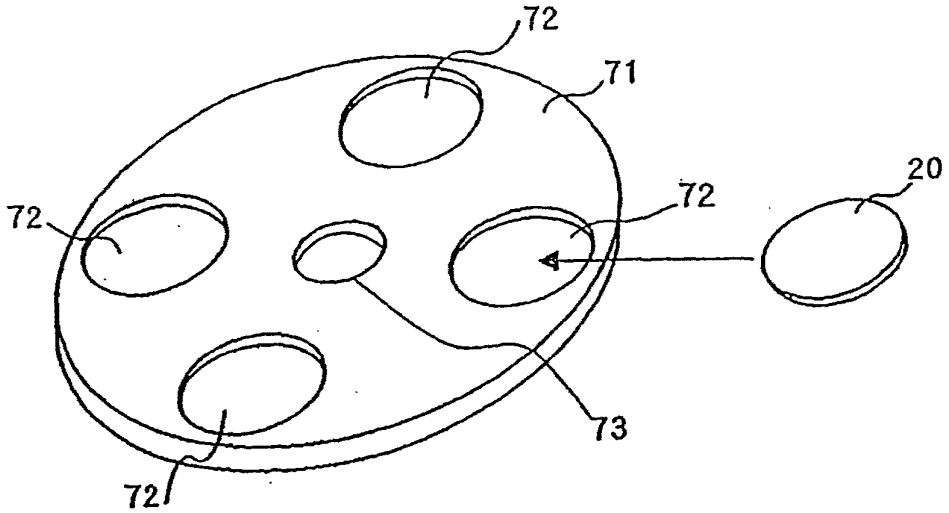
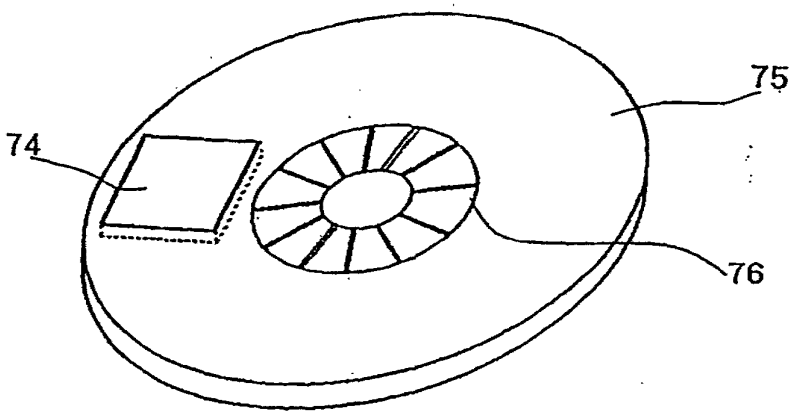
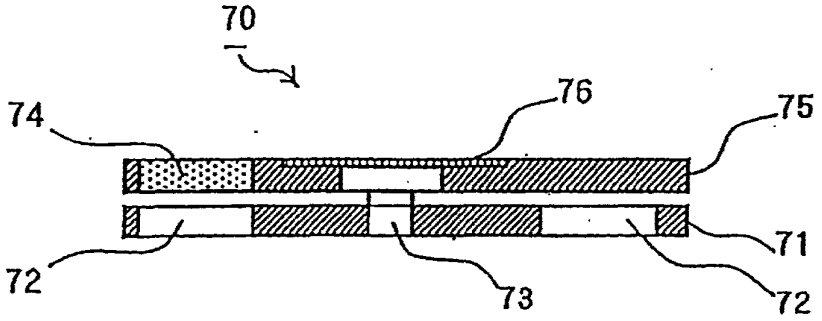


FIG. 11b



IPR2025-00645 Page 00116

FIG. 11c



IPR2025-00645 Page 00117

FIG. 12a

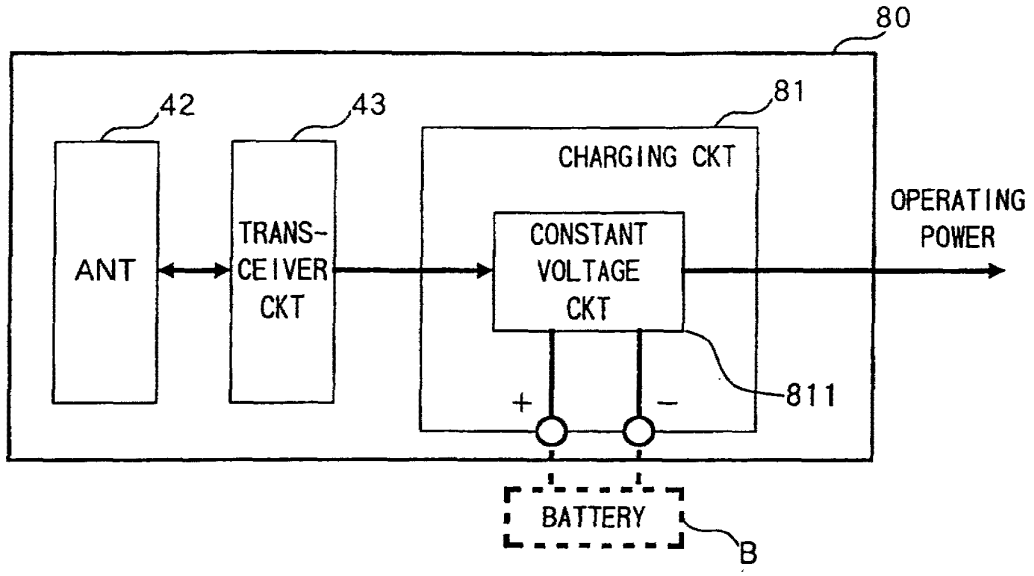
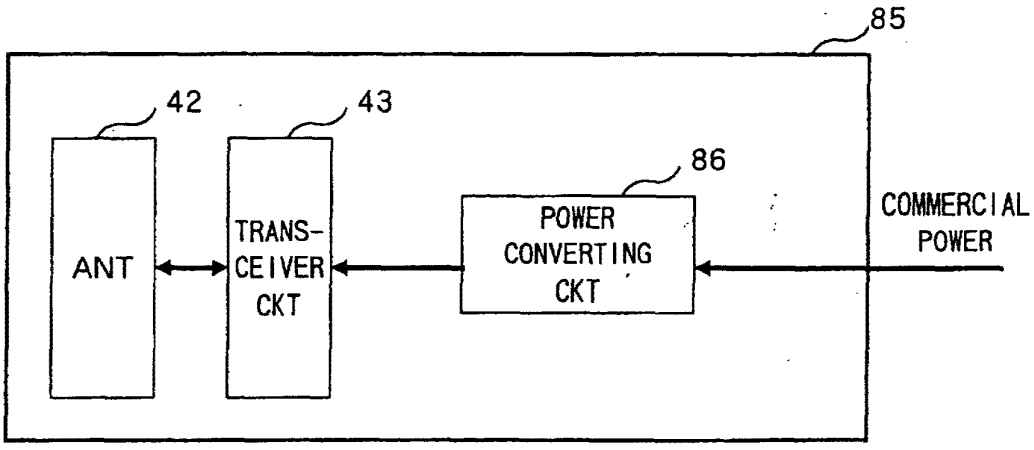


FIG. 12b



IPR2025-00645 Page 00118

FIG. 12c

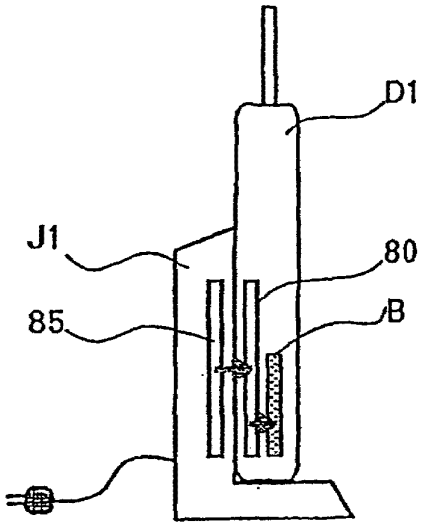
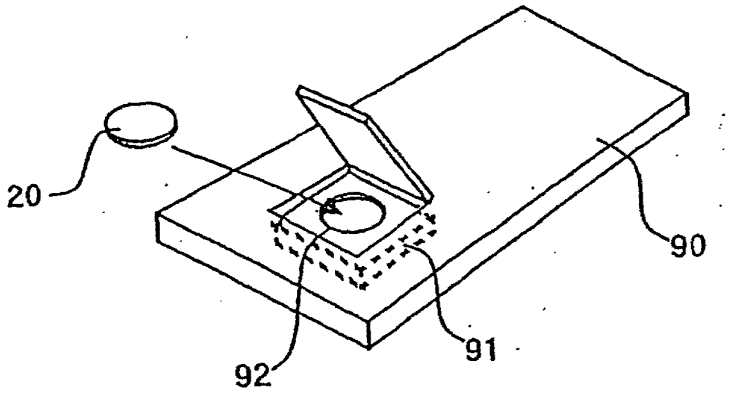


FIG. 13a



IPR2025-00645 Page 00119

FIG. 13b

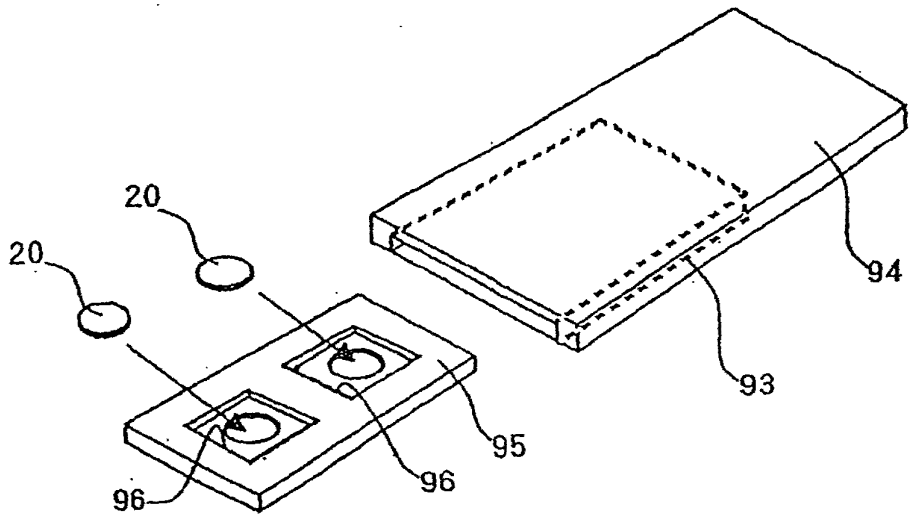
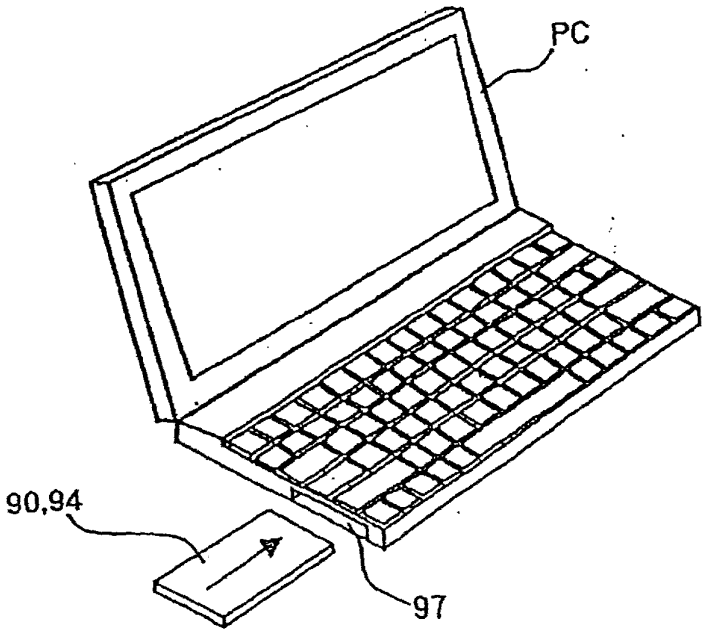


FIG. 13c



IPR2025-00645 Page 00120

FIG. 14

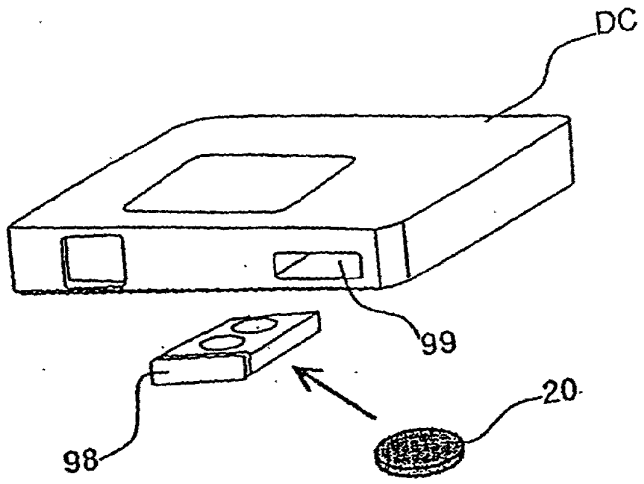
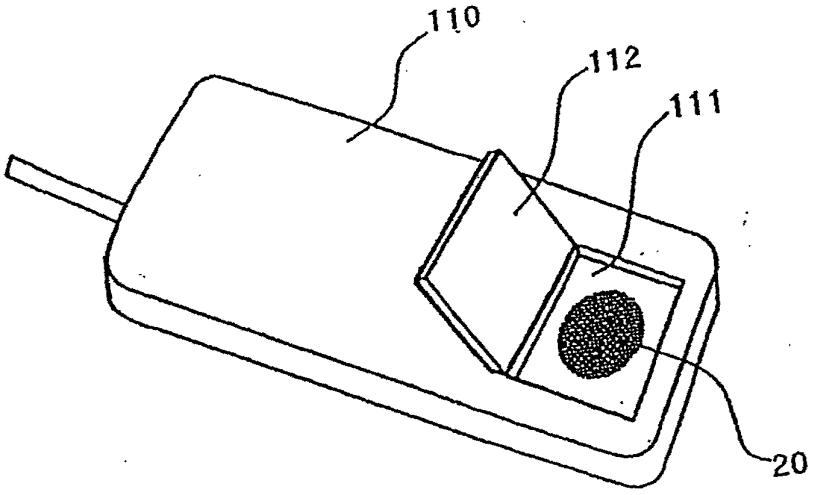


FIG. 15



IPR2025-00645 Page 00121

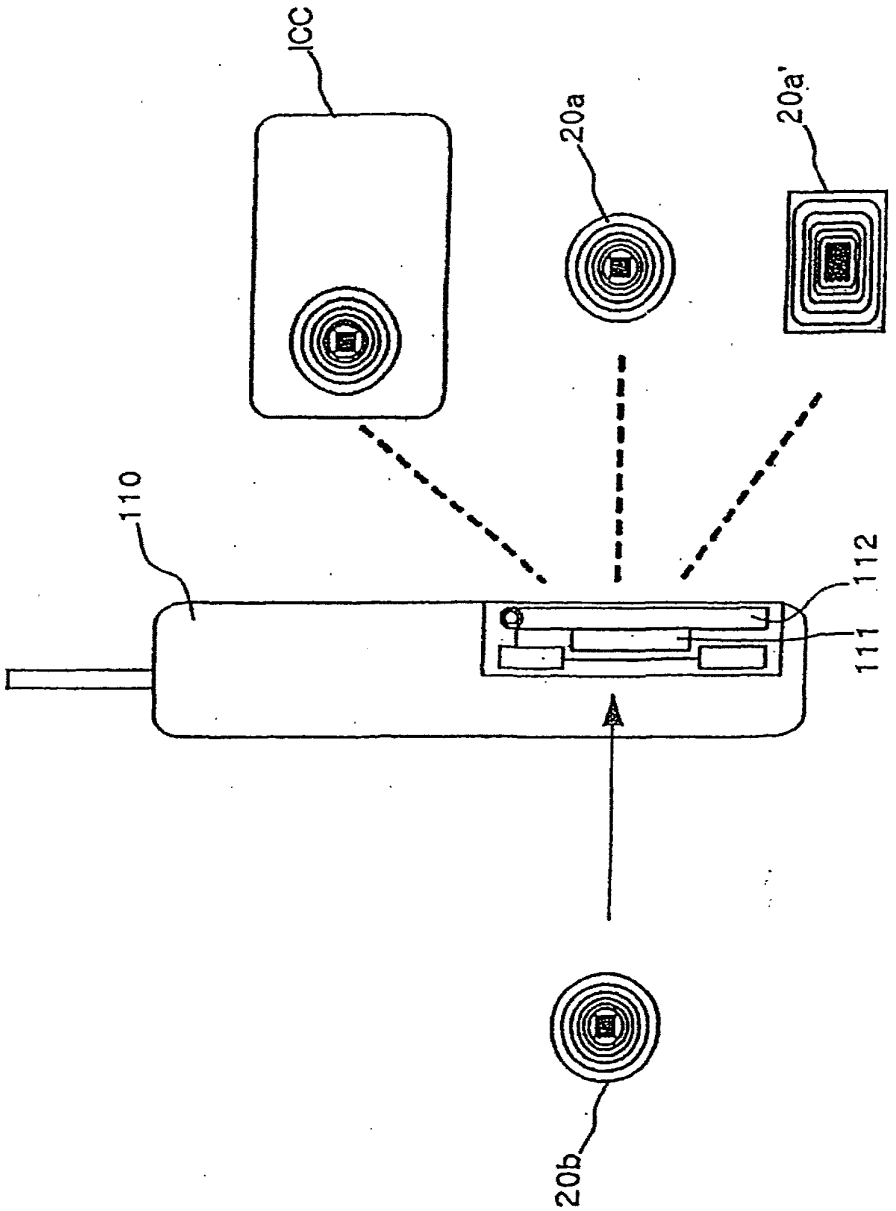


FIG. 16

IPR2025-00645 Page 00122

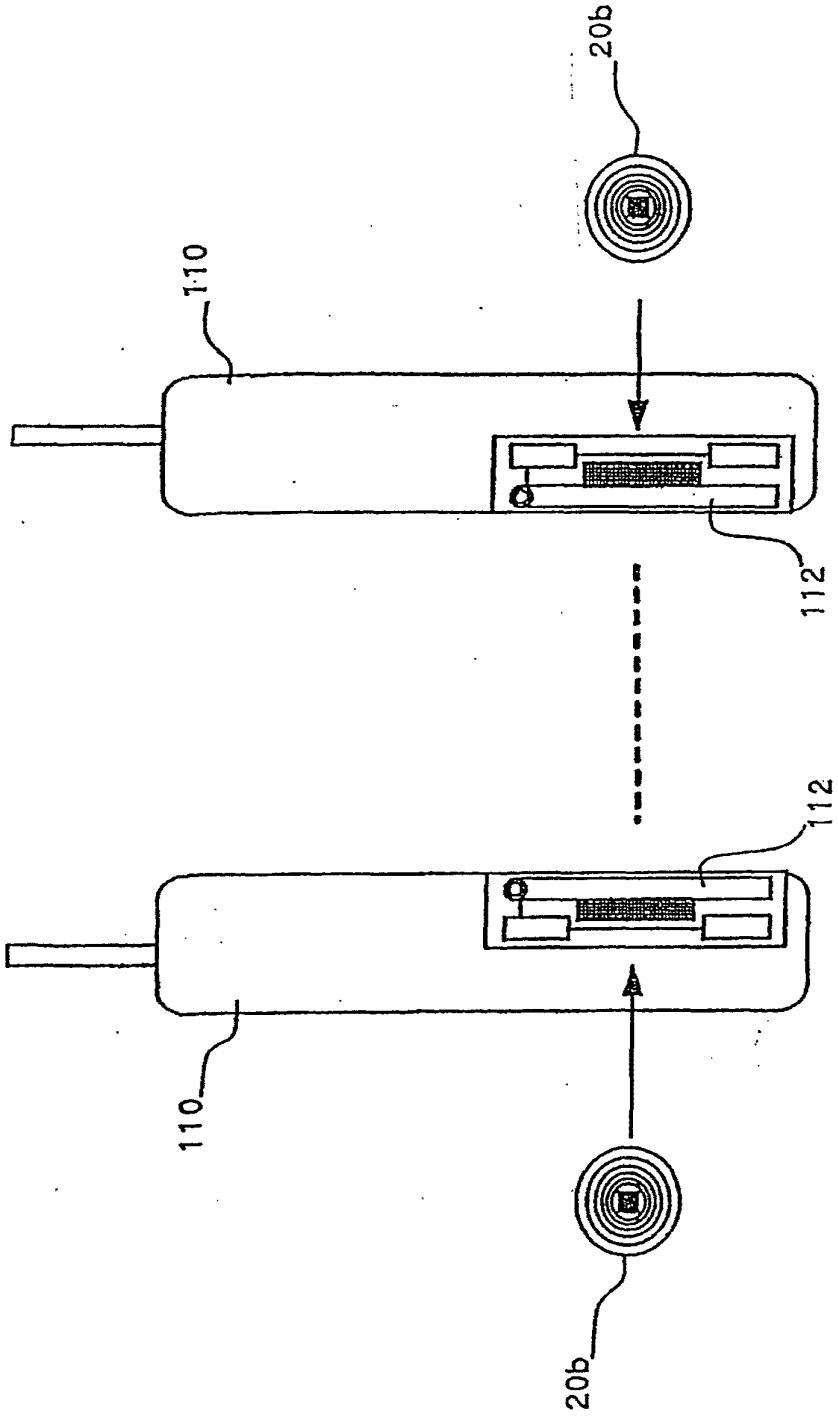


FIG. 17

IPR2025-00645 Page 00123

FIG. 18

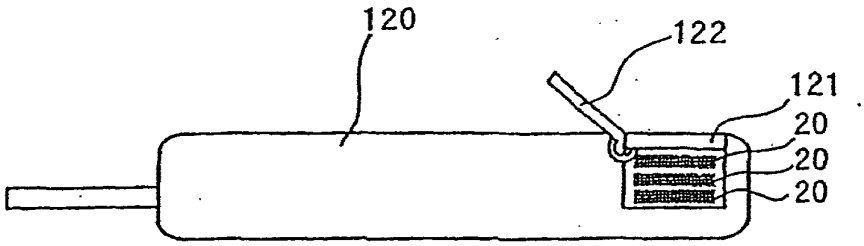
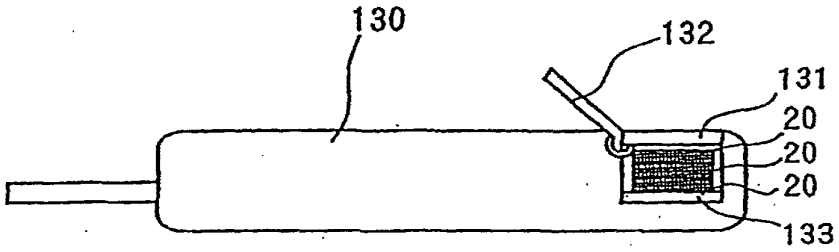


FIG. 19



IPR2025-00645 Page 00124

FIG. 20

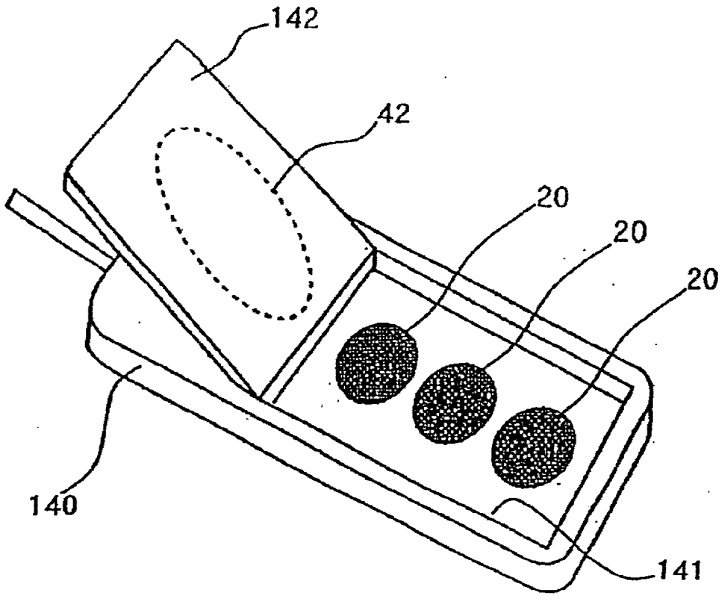
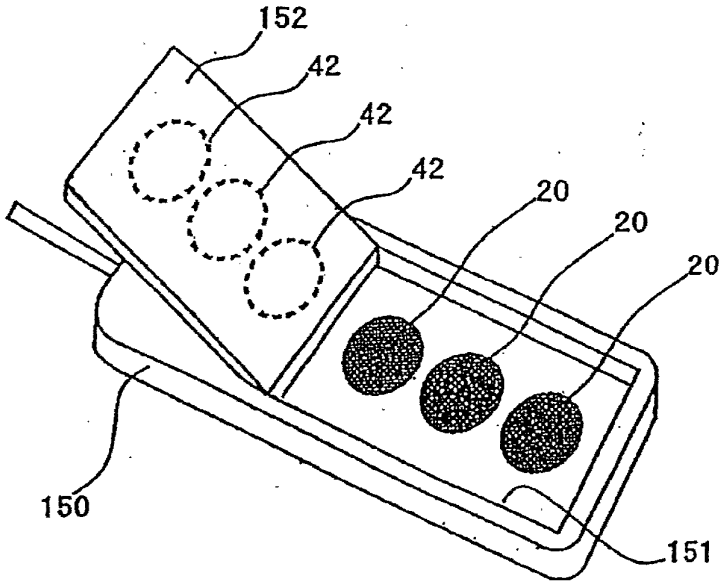
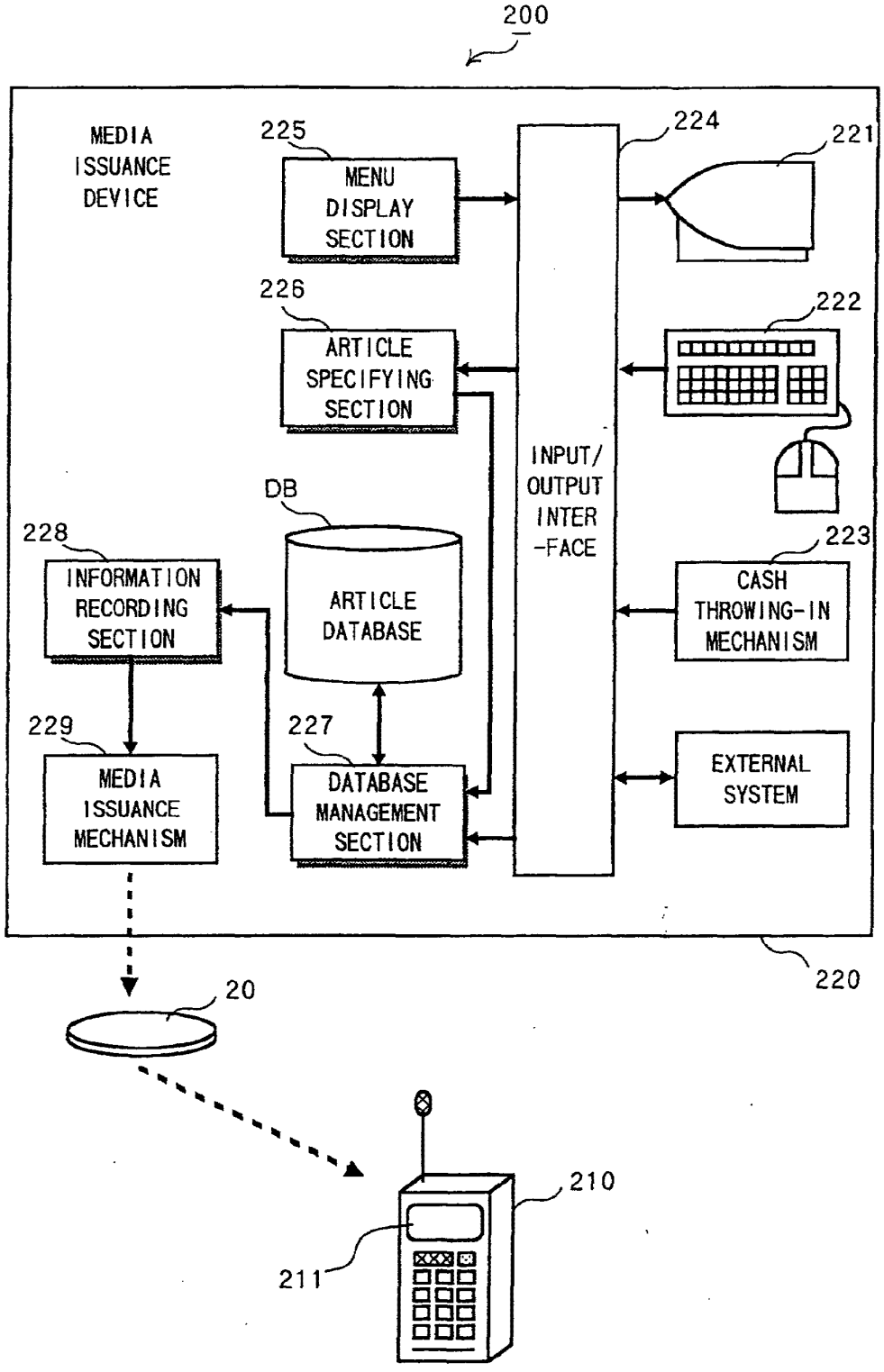


FIG. 21



IPR2025-00645 Page 00125

FIG. 22



IPR2025-00645 Page 00126

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/04671

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl[7] G06K19/077, G06K17/00 H02J7/00, G07F17/00, G06F17/60, G09F27/00

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)
Int. Cl[7] G06K19/077, G06K17/00 H02J7/00, G07F17/00, G06F17/60, G09F27/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Toroku Jitsuyo Shinan Koho 1994-1999

Electronic data base consulted during the international search (name of data base and, where practicable, 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 Y	JP, CD-ROM of specification and drawings first annexed to the request of Japanese Utility Model Application No. 24032/1992 (Laid-open no. 83866/1993) (Nitto Denko K.K.), 12 November, 1993 (12.11.93), Par. No. 4, Figs. 1,2 (Family: none)	1,5 3,4,7
X Y	JP, CD-ROM of specification and drawings first annexed to the request of Japanese Utility Model Application No. 80147/1991 (Laid-open no. 30874/1993) (Nitto Denko K.K.), 23 April, 1993 (23.04.93) (Family: none)	2 4
Y	US, 4900386, A (Durgo AG), 13 February, 1990 (13.02.90), Column 5, lines 24 to 26 & JP, 63-317389, A Column 8, lines 12 to 13 & EP, 292827, A1	3

☒ 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 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 December, 1999 (17.12.99)	11 January, 2000 (11.01.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2025-00645 Page 00127

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/04671

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 9-104189, A (DENSO CORPORATION), 22 April, 1997 (22.04.97), Par. No. [0026] (Family: none)	4
X	JP, 63-246292, A (TOSHIBA CORPORATION), 13 October, 1988 (13.10.88) (Family: none)	6
X	JP, 2-62295, A (Matsushita Electric Industrial Co., Ltd.), 02 March, 1990 (02.03.90) (Family: none)	6
Y	JP, 7-239922, A (DAINIPPON PRINTING CO., LTD.), 12 September, 1995 (12.09.95) (Family: none)	7
Y	JP, 7-325895, A (TOSHIBA CORPORATION), 12 December, 1995 (12.12.95) (Family: none)	8-12,16,17
Y	JP, 9-22449, A (TOKAI RIKA CO., LTD.), 21 January, 1997 (21.01.97) (Family: none)	8-12,16,17
X	JP, 10-92673, A (TDK Corporation), 10 April, 1998 (10.04.98) & US, 5923544, A	22
Y A	JP, 4-178689, A (Hitachi, Ltd.), 25 June, 1992 (25.06.92) (Family: none)	23-26 19-21,29,30
Y	JP, 6-119552, A (Sony Corporation), 28 April, 1994 (28.04.94) (Family: none)	23-26 19-21,29,30
Y	JP, 6-12571, A (RHYTHM WATCH CO., LTD.), 21 January, 1994 (21.01.94) (Family: none)	23-26
X Y	JP, 9-244567, A (Masayuki Koguri), 19 September, 1997 (19.09.97) (Family: none)	27 28

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

IPR2025-00645 Page 00128

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/04671

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The technical feature of the inventions of claims 1 to 30 is only the "noncontact record carrier having an IC module", which is well known as an "IC tag" or a "noncontact IC card". Therefore, the feature is not a special technical feature under PCT Rule 13.2.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1992)

IPR2025-00645 Page 00129

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 178 450 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.02.2002 Bulletin 2002/06

(51) Int Cl.[7]: **G07F 19/00**

(21) Application number: **01114153.8**

(22) Date of filing: **25.10.1995**

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI NL PT SE

(30) Priority: **28.10.1994 FI 945075**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
95935472.1 / 0 739 526

(71) Applicant: **Vazvan, Behruz**
00420 Helsinki (FI)

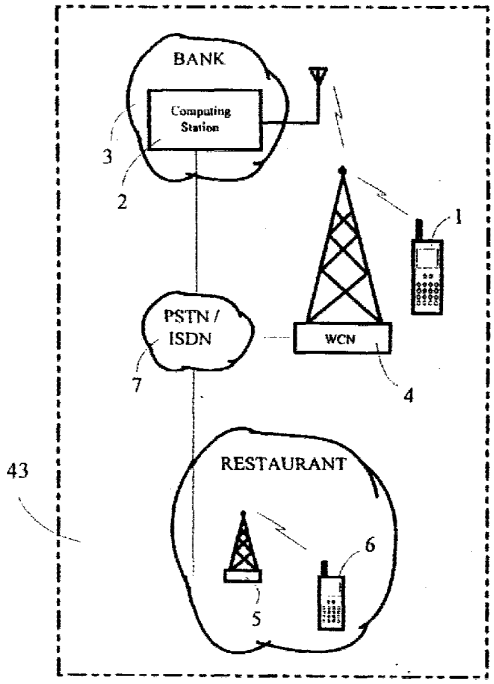
(72) Inventor: **Vazvan, Behruz**
00420 Helsinki (FI)

Remarks:
This application was filed on 11 - 06 - 2001 as a divisional application to the application mentioned under INID code 62.

(54) Real time tele-payment system

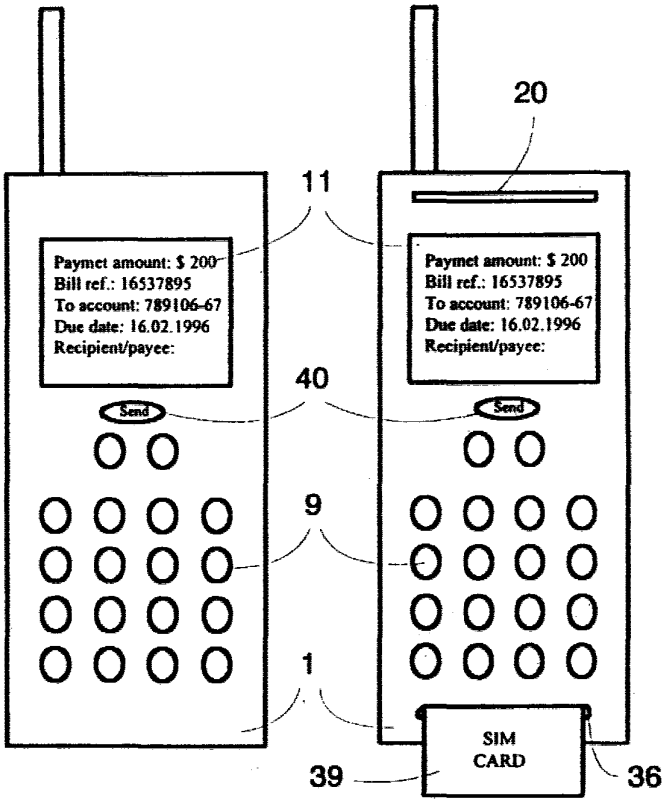
(57) This invention is a real time mobile payment system and a method that relates to the payments and bills of the mobile users and providing the mobile users with the information about their accounts, account balance, the statement of account, or the movement on the account and other required messages by using their mobile terminals (1, 6) under any wireless telecommunication system. According to one embodiment of the invention short message service facilities of at least one mobile wireless communication network (4) or a digital cordless communication system (5) are utilized through which user mobile terminals (1, 6) can send and receive to or from remote computing stations (2) payment messages and/or at least messages about the account balance, the statement of account, or the movement on the account of said mobile terminal's subscriber or user, and communicating banking, payment, and/or commerce related and other required messages. The system in one of its embodiments characterized in that means are provided for encrypting/decrypting and completely securing messages communicated between a mobile terminal (1, 6) and/or a identity module (10, 21, 39, 42) such as SIM (Subscriber Identity Module) or equivalent and a computing station using a security algorithm.

FIG 1



EP 1 178 450 A2

FIG 4



IPR2025-00645 Page 00131

Description

[0001] This invention is a real time mobile payment system that relates to the payments and bills of the mobile users and providing the mobile users with the information about their accounts, account balance, the statement of account, or the movement on the account and other required messages in a real time basis by using their mobile terminals under any wireless telecommunication system.

BACKGROUND OF THE INVENTION

[0002] There are several mechanical and electronical payment systems for retail business operations like, for example, what is introduced by US patent US-A-5 202 825, in which a hand-held data terminal generates a record of purchases made by a customer for charging a customer in accordance with customer-indicated payment preferences. In these systems the waiter sends by use of a data terminal the customer's order to a customer service station which is a typical cash register based in the restaurant. These systems reduce the time requirements for processing customers at check-out counters in comparison with those of more traditional check-out procedures of the recent past. These systems are only for sending the customer order to the cash register in the retail business.

[0003] On the other hand in the fixed telecommunication networks a user (subscriber) can be connected from his personal computer to his/her bank via telephone lines and thereby pay his/her bills. In such systems user must use a data modem between his/her computer and the telephone wire. Another disadvantage of such systems is that in order to pay his/her bills, user must have access to his own personal computer connected through his telephone line to the fixed telephone infrastructure, therefore user mobility in such systems is completely limited. On the other hand in the existing telephone banks when a telebank is called, the computer identifying the DTMF-voice frequency signals available through the telephone network i.e. the central voice applications platform (the CVAP) answers and the caller talks with the CVAP by pushing certain keys suggested by a predetermined program. A considerable problem in such systems is that no payment or any equivalent value or code is sent from the user terminal to the central system for charging the users in real time for the connection time or data messaging. Moreover, no payment or its equivalent value is transferred by the user's terminal to an account for user's mobile bills or commerce. Another considerable problem in such systems is that no data is visualized in user's mobile terminal to allow user to input or select an item, and no real time data messaging technique is adapted for users' bill payments and banking issues but users must listen to an instruction, during a call, and then by pushing certain keys pay a bill without seeing any data, and then cut off the connection which also is not charged in real time.

[0004] The published WO 94/11849 discloses a payment system which uses the GSM-network user's A-number for user authentication when a call is set up to service providers. In order to register the telephone to the network the user is first authenticated in the authentication center of the GSM network when he enters his PIN-code, as is well known. Then the payer selects the transmitter of the transaction, e.g. a bank, a credit company, based on which a call is placed to the transmitter's payment system. In the call set-up, the subscriber is identified using the subscriber A-number. The caller's A-number identity is used to administrate the user's rights and to connect the user to the service.

[0005] According to the publication in telephone (i.e. voice) banking services the terminal is a standard GSM telephone. According to the description and claims of the publication when a telephone alone is used an audio connection is taken from the telephone for banking services. In data-based banking services the terminal is a normal computer linked to the GSM telephone e.g. Motorola MicroTac-phone serial port by means of cable. No data is controlled neither displayed by said telephone itself. The banking services are handled by calling transmitter's payment system, forming a connection with said system, giving the amount to be paid, confirming the amount, approving the payment, giving the payment an identification number, producing a receipt of the transaction to the customer, recording the transaction in the seller terminal and in the payment system, and after that charging the telephone connection time, and cutting off the connection. As it is clear to a person skilled in the art the publication presents the method of the GSM system where subscriber's A-number is used to authenticate a user in the call set-up in accordance with the GSM system standards.

[0006] A considerable problem in the method and system explained in WO 94/11849 is that no data is controlled by said telephone neither said data is displayed on the screen of said telephone but for data-based banking a personal computer is used which is connected to a standard GSM-telephone's serial port. Therefore, for data services, the user terminal is comprised of a normal personal computer connected by cable to a GSM telephone whereby a data call is made to the bank. The telephone disclosure of said publication is not arranged with means to control and display required data messages for bill payment transaction and mobile commerce, neither a method for securing said messages. Another considerable problem in said system is that no transaction is encrypted end to end neither digital signatures techniques used for user authentication and securing the transactions. The publication does not provide a wireless and modemless data messaging solution neither methods for improving such technologies, as it is provided by the present invention. Furthermore, the method and system of said publication dose not disclose a user authentication method based on utilizing

IPR2025-00645 Page 00132

short data messaging. The publication does not specify a specific applications and client module for running banking, commerce and other applications and securing the messages, as the present invention provides. Moreover, in the method and system of said publication no smart card or accounts are arranged to be charged in real time for users communications or service being in use, neither any payment is transferred from said terminal to a user account. According to the system of publication WO 94/11849 the telephone connection is only charged using the traditional billing systems and after the transaction has been completed and a receipt has been produced for the customer. Therefore, problems of bad debit are not solved by the invention of WO 94/11849 because the user account is not charged in real time. Other inefficiencies of the system presented in said publication is that it does not provide an interactive real time messaging system and method for running applications and requesting information, such as account information or any other messages by means of a mobile terminal and by sending request messages, that are structured and displayed in said mobile terminal in a user friendly format, to the remote computing stations for retrieving the information required and displaying in user's mobile terminal. The publication presents the GSM system's authentication method wherein the subscriber's A-number is used to authenticate the subscriber in a call set-up, while in the present invention messages are also encrypted and secured using any security algorithms and any users codes to securely identify the users and encrypt messages.

[0007] Mobile terminals have limited resources that should be used efficiently. Therefore for data services terminals and services should be specifically designed to allow introduction of services via resource limited mobile terminals. In GSM and other mobile systems the standard data communication is designed to be used for one way data transmission using fax devices or personal computers connected by means of cable to a mobile telephone i.e. no data is arranged to be handled and displayed by a mobile terminal neither any cordless means and environment is arranged in connection with user's mobile terminal in order to communicate with other devices without using any cable connections between said terminal and other devices. Furthermore, before this invention the messaging facilities of the existing mobile systems and terminals, such as GSM, were limited to the basic SMS techniques so that the user was allowed to send and receive only to/from other mobile users at most a 160 characters short message each time. Another problem with the basic SMS services is that the messages sent, received or displayed are not structured in an user friendly format, to present inquiries, menus enabling users to input or select an item, but the messages are communicated using standard GSM terminals without any especial design and operations. While SMS is a point-to-point short message service it is not arranged to carry out messaging in real time but message formats are specified for one way communication without taking into account the need for possible responses, results of queries etc. Furthermore, before the present invention short data messaging was not utilized and adapted for bill payment and mobile commerce. The basic SMS is not arranged for banking, retail and commerce businesses neither to provide interactive services. Before this invention mobile terminals and smart cards were not arranged with means for digitally encryption and decryption of messages to provide secure messaging between a mobile user and a remote computing station. Furthermore, smart cards (SIM) were not arranged with means to control a user interface for controllable menus and inquiries, for real time sending and retrieving information and performing mobile commerce.

[0008] There continues to exist a need to further improve the efficiencies of payment and messaging systems. The system and method according to the subject invention provides preferable solutions to the above mentioned problems.

ADVANTAGES OF THE INVENTION

[0009] A solution to the posed problem of the invention is defined in the independent claims. Preferred embodiments and other features of the invention are defined in the dependent claims. In one embodiment of the present invention a real time payment system and method is provided for charging the mobile users in real time, as the time and call/service is going on, for their mobile bills. In another embodiment of this invention a system and method is provided to allow users of mobile terminals to display, send and receive bills, payments, account information, structured inquiries, menus, and other messages (e.g. 11), for banking, commerce, retail and the like businesses, to/from computing stations via wireless messaging means of a digital mobile or cordless system without using any data modem in connection with said terminal. In one embodiment this invention provides a generic message format making short messaging a real time application messaging system. According to one embodiment of the present invention the user mobile terminal is arranged with a client module that communicates with a computing station over a digital mobile or cordless communication system to allow service providers, commerce, banks, retail and the like businesses to provide their services to users in a user friendly manner. In the present invention the users are allowed to set up interactive communications with computing stations by sending request codes and messages that are structured and displayed in an efficient and user friendly format 11, a menu, to allow a user to select and input an item, send a message, a code (e.g. 33) to said computing station wherein the information required, e. g. the statement of an account, bills, commerce related messages, are retrieved in real time and sent to said users' mobile terminals. A structured user friendly menu

IPR2025-00645 Page 00133

11, 33, an inquiry is displayed for user that allows user to select, input, and activate a required item and whereupon communicate via a wireless system with a remote computing station, send and receive messages. Another aspect of the present invention is that user is allowed by means of his mobile terminal to send and receive the required amount of payment, to send the payment to the payee's account or terminal, to transfer the payment from a smart card, mobile payment part, to a payee's account or terminal and to store the payment in said smart card (SIM or equivalent). Yet, in another embodiment of the present invention messages communicated between said mobile terminal, mobile payment part and computing stations are secured and encrypted using security algorithms and any necessary codes to provide a complete secure system. In another embodiment of the present invention a wireless messaging communication system is provided wherein the users' mobile terminal, a computing station and other terminals are allowed to send and receive long data information such as account statements via short messaging means. In this invention the user mobile terminal and the computing stations are further arranged with means to combine short messages or divide long data information to several parts, and to send them to a terminating system or terminal enabling said terminal to control and structure said messages and display said messages and data information for user through a display of said terminal. Yet, another advantage of this invention is that the user terminal is arranged to operate both as a digital mobile terminal via digital mobile networks and as a digital cordless terminal via a digital cordless system (e.g. a restaurant's, a shop's etc. cordless system). According to another aspect of this invention said user mobile terminal and smart card (SIM) are arranged to display, receive, send, store and control at least one structured inquiry or menu 11, 33 allowing said user to select an item, input or accept an item wherein said inquiry or menu in one embodiment has at least one question and answering field. According to another embodiment of this invention a smart card (SIM), operable in a mobile terminal, comprises controlling means and means to secure, send, receive, and store short data messages, menus, inquiries and means to allow the user to select and input an item and whereby to set up real time interactive wireless and modemless messaging through a user mobile terminal with at least one computing station. Other preferred embodiments of the invention are defined in claims of this invention.

DESCRIPTION OF THE INVENTION

[0010] In order to serve such current needs, the present invention provides a new and unique mobile payment and messaging system. In the inventive system a mobile terminal can be used in order to pay bills or transfer money or request information, for example account information. Certain features of the invention are intended as an expansion of value-added services of currently existing mobile communications systems. This invention addresses needs created by users mobility. For example, suppose that you are traveling and you want to pay a certain bill or transfer some amount of money to a person's account but you do not have time for going to the bank or the bank may be closed and you may neither have access to your personal computer (which can be connected to the bank via telephone wire). This invention provides you the possibility to pay your bills in an convenient and user friendly way, by using your mobile terminal while you are in move, regardless of weather the banks are closed or not, regardless of weather it is night or weekend etc. This invention also provides the retail businesses (for example restaurants, shops, etc. and other service providers) the possibility to charge their customers, via mobile telecommunication networks, by using their mobile terminals. For example, a waiter in a restaurant, after having entered the amount of payment or the customer's information (like account number etc.) to his/her mobile terminal sends the payment information to the inventive computing station. In the computing station either the customer's account can be charged or the payment amount received from the waiter's mobile terminal can be transferred to the restaurant's account. The most important advantage gained by the inventive system is that all mobile telephone users (subscribers etc.) can pay their bills by using their mobile telephones (in which the inventive mobile payment part is included) and user identity or codes, without requiring any data modem, personal computer, and conventional debit or credit cards etc. In this invention the user identification module and user identity and codes can function as the user's credit card enabling secure payment transactions and messaging.

[0011] By implementing the inventive mobile payment system a mobile user (subscriber etc.) can pay all his/her bills and handle all his/her banking issues where ever under the coverage of a mobile communications network. These and other improvements and advantages are realized by providing a system, a method, a mobile terminal (including the inventive mobile payment part) and a computing station. The present invention will now be described by way of examples with reference to the accompanying drawings, in which:

[0012] **Fig. 1** is a schematic representation of the inventive Real Time Tele-payment System 43.

[0013] **Fig. 2** represents, as an general example, a payment flow diagram between the mobile terminal and the computing station, located in the bank 3.

[0014] **Fig. 3** represents, as an general example, a payment flow diagram in which a mobile user pays his/her bills or request the statement of account or other information by using his mobile terminal. In this figure also the payee is informed about the reception of a payment.

[0015] **Fig. 4** is a schematic representation of two type of mobile terminals: one is a mobile telephone that in-

IPR2025-00645 Page 00134

cludes the inventive mobile payment part 10. The other one is a mobile terminal that uses the inventive mobile payment part in a user-friendly smart card 39, includes a charge slip printer and a user-friendly (SIM etc. smart cards) card reader (SIM: Subscriber Identification Module).

[0016] When a mobile user wants to pay a bill or transfer money to his account or other, he can enter all information required for payment (like his account number, the payee's account number, payment's due date, bill's reference number, etc.) to his mobile terminal 1 (for example through the keypad). As it is the object of this invention, the user's own account information dose not need to be entered if the computing station 2, can identify the calling party. This needs that the user information (identity) should be confirmed by his/her telephone operator or service provider, for example, in the mobile communications network 4 and then be sent to the bank as a confirmation of user (subscriber) identification. User identity can be sent by user's mobile terminal, telephone operator or service provider to the computing station 2.

[0017] Monitoring a calling party's number or information at a receiving terminal is a feature provided by today's digital telephone systems. In this invention, in order to implement such procedure, for example the switching systems at the mobile network side can be used so that only when a user sets up a call or sends a message (by using short messaging means of the mobile communications systems) to the computing station 2 his/her identity can be monitored in the computing station 2 in order to identify who is the calling party. Therefore, in this invention the computing station 2 can receive at least the confirmed user identity via the user's telephone operator or service provider of a mobile communications network 4 in order to identify who is in charge for payment of bills sent by mobile terminal 1. Other required information like passwords or access codes to the user's bank account can be sent by user through his/her mobile terminal 1.

[0018] In today's mobile communication systems the user identity, included in his/her SIM card, is checked and confirmed by network 4 every time his/her mobile terminal 1 is turned on and attached to the telephone network 4. In this invention the user identity, transmitted from the mobile terminal 1 to the network 4, can be completely encrypted and secured and also the payment messages between mobile terminal 1 and computing station 2 are quite secured because of: first, the security algorithms used in said digital mobile telecommunication system and mobile telephone, and secondly, because of the user's password or access codes used for payment messages in the inventive mobile payment system. All kind of wireless communications networks can be used in order to communicate the payment and bill messages between the mobile terminal and computing station. For example, if in a restaurant there is a cordless system like DECT (Digital European Cordless Telephony) 5 the user terminal 6 can be connected through such cordless system and PSTN (Public Switched Telephone Network) or ISDN (Integrated Services Digital Network) 7 to the computing station 2.

[0019] The payment question-answering procedure between the user and his mobile terminal 8 is entered by using the user interface 9 and received and handled by the inventive mobile payment part 10, 39. The bill and payment information entering procedure 11 is an interactive procedure between the mobile payment part 10 and the user through a user interface 9. Then, the computing station's number is dialed (activated) 12 (either automatically or by user) which after the mobile terminal 8 sends the required information for call set-up to the mobile network 15 and then payment messages 13 to the computing station 14 via the network 15. If the user identity or codes are not sent from the user mobile terminal 8 to the computing station 14, then the mobile network 15 confirms and sends the user identity to the computing station 14 either directly or through the fixed public network 16. The computing station 14 checks the calling party's account and account number of payee (the account to which the payment should be transferred) and then transfers the received amount of payment to the payee's account or terminal or charges the payer's account 17, 28, 30. Then the computing station 14 sends a short message 18 to the mobile terminal 8 indicating "payment completed" or if there is not enough credit (money) in the payer's account a "No effects" message 19 is sent to the user mobile terminal 8, meaning that the payment can not be performed. For retail businesses, mobile terminal includes also a charge slip printer 20. If the mobile terminal receives a "payment completed" command 18, the charge slip printer 20 prints a receipt for the customer. In this invention, for example, for the retail and trading businesses, the customer's SIM (or other smart card) 39 is entered in the card reader 36 of mobile terminal 1 (of a waiter in a restaurant, for example, if user doesn't have his own terminal) temporary in order to pay the bill. The account number of payee (for example account number of the restaurant) can be stored in the memory of his/her mobile terminal in order to reduce the information entering procedure. This means that only the payment amount should be entered to the terminal. After that the payment amount has been entered to the mobile payment part 10 and the computing station's 14 number has been dialed, the mobile network 15 sends the customer's identity, which can be the subscriber identity or a different code (a code different than that of subscriber identity, number etc.) to the computing station 14. The computing station 14 can identify the calling party (the payer) because it can receive the calling party's identity from the network 15 and compare with the calling party's identity based in the computing station 14, when required. Therefore the payment amount received from the mobile terminal 8 is transferred to the payee's account. The user identity sent from the mobile network

IPR2025-00645 Page 00135

15 to the computing station 14 can be different than the user's, identity sent by the mobile terminal 8 to the mobile network 15 but both of these identities can belong to one user (subscriber). Alternatively the payer's, identity or codes, included in his/her (SIM) card 39 or entered to the mobile terminal by using user interface 9, can be sent directly from the mobile terminal 8 to the computing station 14. It should be understood that for the simplicity of the description, messages for outgoing call set-up and incoming call or short messages services procedures are not explained with details since these procedures are already well known in the mobile communications systems.

[0020] Following is an example, in which a mobile user pays his/her bills or transfers money to his/her or other person's account, or requests the computing station for statement of account, by using his/her mobile terminal.

[0021] First, the payer enters the bill's information 22 (for example: account number of payee, the amount of money which should be transferred, due date of the bill, reference number 11) to the mobile payment part of his/her mobile terminal 41. Then, after activating an OK function by user the number of the computing station 24 is used and the mobile terminal sends the payment information 25 to the computing station 24 via a mobile communications network 26 and a fixed network 27. Then, computing station 24 transfers the amount of payment, on the bill, to the payee's account 28. Then, computing station 24 sends a "Payment Completed" short message 29 to the mobile terminal. If the payee has also a mobile terminal 37, then his/her mobile terminal 42 can receive a "Payment Reception message" 30, from the computing station 24, indicating the amount of payment, the payer and the payment date. However, before dialing (activating) the number of computing station the mobile payment part may ask the payer (the user of mobile terminal) "Any other payment ?" 31. The answer can be respond by activating for example "Yes/No" function 32 or an OK function of the mobile payment part 21. Then the user can enter another bill information to his terminal (mobile payment part) and when all information required has been provided, the required number can be dialed (activated). After this, all bills information (payment messages) are sent to the computing station 24 as explained above. Furthermore, for requesting information such as account balance, the statement of account, or the movement on the account from the computing station 24, there is a code under a user friendly command name such as "send the statement of account" or the like 33. When user selects such a command 33, the mobile payment part 21 sends a message either by setting up a call or by using short message facilities of a mobile communications network 26 to the computing station 24 as a request for account information. Then computing station 24 sends the required account balance or the statement of account 34 to the mobile terminal 41. The computing station 24 is also arranged to send for example a "Monthly Statement of Account" 35, to the mobile terminals 41, 42 for example once or twice per month. Then mobile terminal's printer (38) can print it for the user to be filed as a record, if required.

[0022] Following is an example in which the payee (for example a restaurant or a retail seller) has a mobile terminal by which the payer (a customer) can be charged.

[0023] Suppose that a customer wants to pay his/her bill in a restaurant for the service he/she has received. The customer can give his/her smart card SIM or the like smart card 39 to the waiter to be entered to the waiter's mobile terminal 6, 8. Then waiter dials (activates) the number of computing station 14, or the number is dialed (activated) automatically after the customer's card 39 has been read by card reader 36 of the waiter's mobile terminal. For example the number of computing station 14 can be stored in the memory of waiter's mobile terminal, and every time a customer's smart card (SIM) is entered to the mobile terminal 1, 8, the terminal automatically contacts the computing station 14. The computing station 14 either transfers the received payment or checks the account information of payer (a customer) and then transfers the transaction amount (the sum on the bill) to the payee's (the restaurant's) account 17. If the payer's account do not have enough credit (money) the mobile terminal 8 may receive a "No effects" message 19, from the computing station or the computing station's operator (e.g. bank) may pay the transaction's amount on behalf of the payer and then later charge the payer or his/her bank for the prepaid transaction. On the other hand if the payer's account information (account number, account identity) is false the computing station 14 may send a "transfer not accepted" message to the payee's mobile terminal, which means that the payer (customer) should pay the amount of transaction in cash as explained in the previous examples. If the mobile terminal receives from the computing station 14 a "payment completed" short message 18, then the charge slip printer 20 prints a receipt for the customer, as explained in the previous example.

[0024] It should be considered that in all above-mentioned examples, bill and payment and other messages can be sent and received both by setting up a call or through the short messaging means of the wireless communication networks.

[0025] In the current mobile communications systems, like GSM, there is a facility called "Short Message Services, (SMS)". In SMS a mobile telephone user can send a short message to another subscriber without setting up an interactive communication. In order to send the bill, payment and other messages by SMS, the software of SMS installed in the user mobile terminal can be modified so that it can also handle the parameters and/or commands of the inventive mobile payment part. By using the short messaging means of a mobile communications network 15, the bills, payment and other information can be sent and received to/from the computing station. When computing station receives e.g. a bill

IPR2025-00645 Page 00136

or payment message 13 via SMS, it also sends a message to the mobile terminal in order to inform it if the payment has been completed 18 or not 19. However, if a user wants to enter and send many payments/bills at once and receive also balance or statement of his/her bank account and the like information from the computing stations, such long message can be divided to smaller parts and then be combined at the mobile terminal or computing station. This means that e.g. each bill information can be sent for example separately through short messaging. This action is transparent to the user of the mobile terminal. For example several bill and payment information can be entered to the user terminal. Then when user selects the "Send" function 40 on the mobile terminal 1, each bill can be sent by one short message in accordance with the short messages' lengths. For example, suppose a short message may not include more than 100 characters. If the bill and payment messages or the statement of account (sent by computing station) or other information needs more (space) than the assumed 100 characters, then such long information is divided into two or several short messages and then is sent one by one or all at once to the mobile terminal or computing station. By utilizing this inventive method, user's mobile terminal can send and receive long data information without using modems or data cards.

[0026] In this invention said computing station can send and receive messages via PSTN (Public Switched Telephone Network) and ISDN (Integrated Services Digital Network) and other fixed networks or via only a mobile or cordless communications network. The computing station includes all means for handling, transmitting and receiving payment and banking messages via the wireless networks.

Claims

1. A mobile payment system for bill payment of mobile users and/or providing users with means for mobile banking, commerce, trading, and/or sending and receiving information, the system comprising:

   - at least one mobile terminal (1, 6, 8, 37, 41) using at least one subscriber/user identity module (SIM or equivalent smart card 10, 21, 39, 42), said terminal and/or said subscriber/user identity module comprising means for encryption/decryption and digitally securing messages communicated between said terminal (1, 6) or said smart card (10, 21, 39, 42) and at least one computing station (2) using a security algorithm, said terminal and/or smart card further comprising means for short messaging (SMS);
   - at least the one computing station (2, 14, 24) located in a bank (3) or any other required places, said computing station comprising means for encryption/decryption and digitally securing messages communicated between said terminals (1, 6) and/or said smart card (10, 21, 39, 30, 42, mobile payment part) and said computing station using a security algorithm;
   - short message service facilities of at least one mobile wireless communication network (4) or a digital cordless communication system (5) through which said mobile terminal can send and receive to or from said computing stations payment messages and/or at least messages about the account balance, the statement of account, or the movement on the account of said mobile terminal's subscriber or user, and communicating banking, payment, and/or commerce related and other required messages;

   whereby:
   means are provided for encrypting/decrypting and completely securing messages communicated between said mobile terminal or said identity module and said computing station using a security algorithm.

2. A mobile payment system according to claim 1, **characterized in that** before sending messages from said mobile terminal or said smart card to said computing station said messages are encrypted and completely secured using a security algorithm in said smart card (10, 21, 39, 42) or in said mobile terminal (1, 6, 8, 37, 41).

3. A mobile payment system according to any preceding claim, **characterized in that** messages received by said mobile terminal or said smart card or computing station are decrypted using said security algorithm.

4. A mobile payment system according to any preceding claim, **characterized in that** messages received by said computing station are decrypted, checked and users are authenticated by digital signatures.

5. A mobile payment system according to any preceding claim, **characterized in that** messages communicated between said mobile terminal or said smart card and said computing station are encrypted/decrypted and completely secured using said security algorithm and a user codes.

6. A mobile payment system according to any preceding claim, **characterized in that** in said system at least bills, banking, commerce and account information and other related messages, menus and inquiries are, as much as required, arranged and displayed (11, 33) for user through the screen of said mobile terminal (1, 6) to allow said user to see, accept, select and input an item or any required infor-

IPR2025-00645 Page 00137

mation and to send and receive said messages to/from said computing stations and other terminals without using any data modem with said mobile terminal, and that said system further comprises means for allowing said user using said terminal (1, 6) to have real time interactive messaging with said computing station by sending at least one request code, a message (11, 33) to said computing station, said codes and information (11, 33) are either sent by said computing station to said terminal or accessed by user from said terminal or its smart card's (SIM or equivalent) memory and displayed for user in a structured user friendly format (11, 33), said codes and/or information presented under command names like "statement of account, account balance" (11, 33) or the like, said codes referring to commerce and information units like account balance, statement of account, banking, retail, trading, purchase, bill payment and other required messages, accessible and/or purchasable from/through said computing stations, and means for transmitting said requested information (11, 34) to said terminal.

7. A method in a mobile payment system, the system according to any preceding claim, **characterized in that** messages communicated between said mobile terminal and said computing station are encrypted/decrypted and completely secured by said mobile terminal (1, 6, 8, 37, 41) or said identity module (10, 21, 39, 42) and said computing station (2, 14, 24) using a security algorithm.

8. A method according to claim 7, **characterized in that** before sending messages from said mobile terminal or said smart card to said computing station said messages are encrypted and completely secured using said security algorithm in said smart card (10, 21, 39, 42) or in said mobile terminal (1, 6, 8, 37, 41) producing at least one digital signature.

9. A method according to any preceding claim, **characterized in that** messages received by said mobile terminal or said smart card or computing station are decrypted using said security algorithm.

10. A method according to any preceding claim, **characterized in that** messages communicated between said mobile terminal or said smart card and said computing station are encrypted/decrypted and completely secured using a security algorithm and a user codes; and that messages received by said computing station are decrypted, checked and users are authenticated by digital signatures.

IPR2025-00645 Page 00138

FIG 2

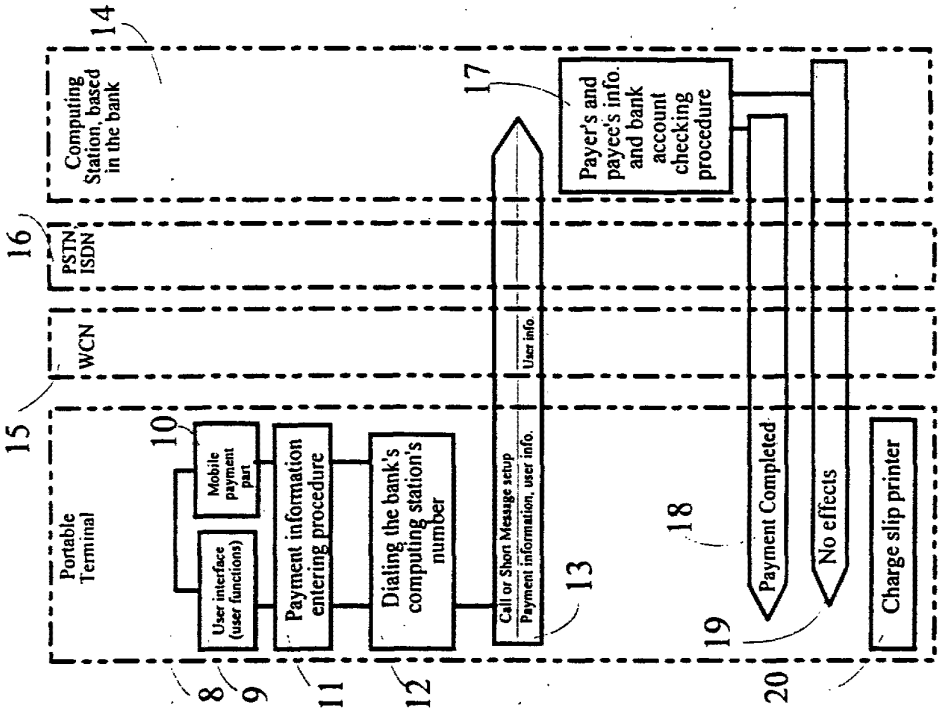
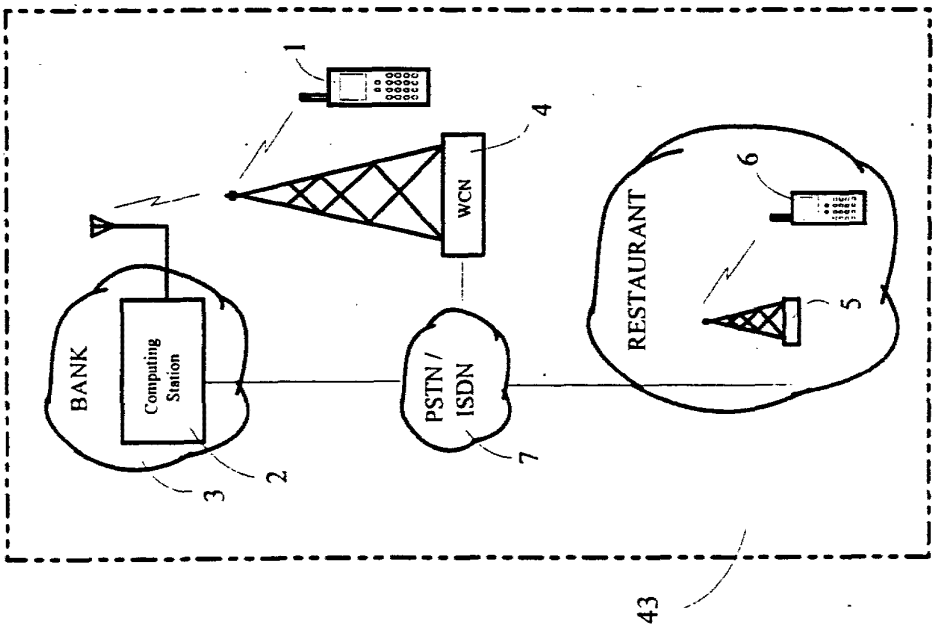


FIG 1



IPR2025-00645 Page 00139

FIG 4

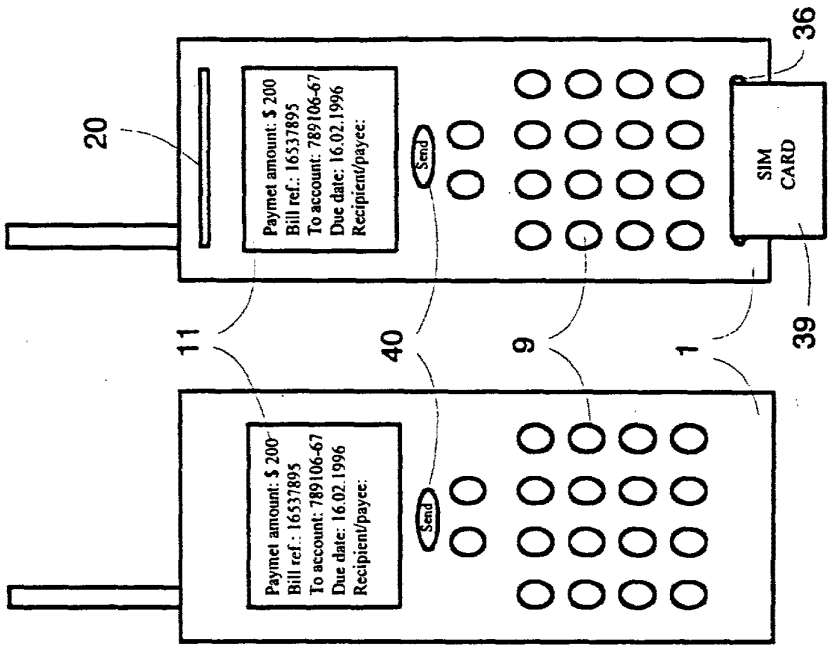
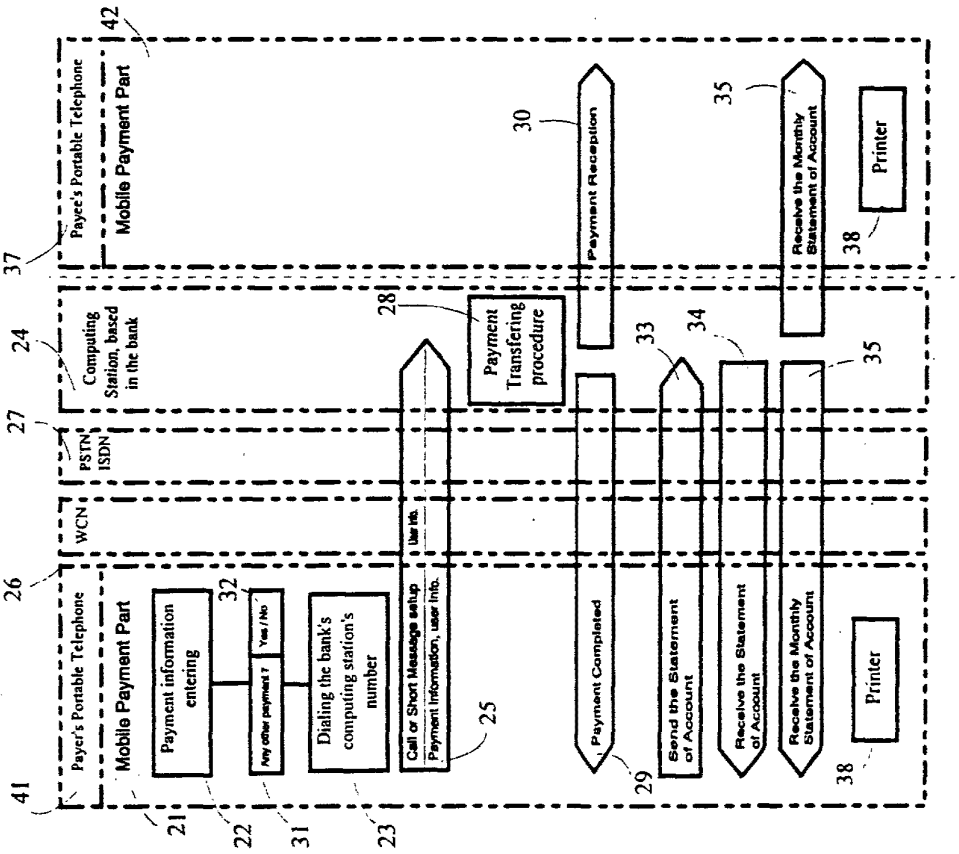


FIG 3



IPR2025-00645 Page 00140

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 189 465 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.03.2002 Bulletin 2002/12

(51) Int Cl.[7]: **H04Q 7/32**

(21) Application number: **00120475.9**

(22) Date of filing: **19.09.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Sony International (Europe) GmbH**
10785 Berlin (DE)

(72) Inventors:
- **Christensen, Per Hartmann**
9000 Aalborg (DK)
- **Yamagashi, Yutaka, Digital Telecomm. Europe**
85609 Aschheim (DE)
- **Ushino, Tatsuji,**
Digital Telecommunications Europe
85609 Aschheim (DE)

(74) Representative: **Körber, Martin, Dipl.-Phys. et al**
Mitscherlich & Partner
Patentanwälte
Sonnenstrasse 33
80331 München (DE)

(54) Mobile terminal with removable memory having SIM card function

(57) The present invention relates to a mobile terminal (1) for a wireless telecommunication system, with a terminal control means (2) for controlling the functions of the mobile terminal (1), and a removable memory module (5, 12) comprising a memory means (7) and a memory control means (6) for controlling the memory means (7). The memory module (5, 12) is removably connected to the terminal control means (2) by an interface (4) having several connections for exchanging information between the terminal control means (2) and the memory control means (6). The memory module (5, 12) further comprises a subscriber identity means (8) for providing subscriber identity information to the terminal control module (2) via at least one of said several connections of said interface (4). The removable memory module according to the present invention thus advantageously combines an extended memory function and a subscriber identity module function.

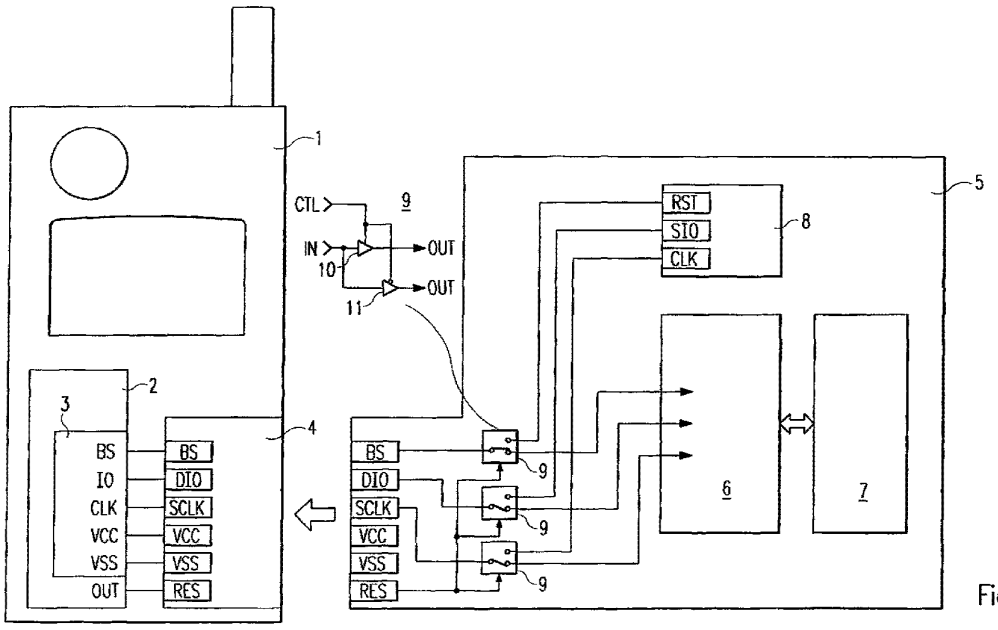


Fig. 1

EP 1 189 465 A1

Description

[0001] The present invention relates to a mobile terminal for a wireless telecommunication system, such as the GSM or the UMTS system, having a removable memory module.

[0002] Mobile terminals, such as portable telephones, palmtops, personal digital assistants or the like, of wireless telecommunication systems of the second generation and the third generation are recently developing into more and more versatile and powerful multimedia devices. Due to the higher transmission data rates between the mobile terminal and respective base stations of the wireless telecommunication system, increasing data amounts have to be stored and managed in the mobile terminals. Thus, the concept of removable memory modules has been proposed by the applicant. These removable memory modules, which are called and protected as memory sticks, comprise essentially a memory means such as a random access memory (RAM) of any kind and a memory control means controlling the data reading and writing from and to the memory means. Such a removable memory module considerably extends the storage capacity of modern mobile terminals. Further, the removable memory module may be used on the basis of standardised interface connections with several different electronic devices, so that a user may use valuable information, such as eMail addresses, telephone numbers etc., flexibly in different devices by simply interchanging the removable memory module. On the other hand, mobile terminals for wireless telecommunication systems generally require the insertion of a subscriber identity module card or SIM card before to be operated by a user. A subscriber identity module card comprises subscriber identity information identifying a user or a subscriber to the respectively used wireless telecommunication system. Hereby, a respective user is recognised while communicating in the wireless telecommunication system so that the respectively contracted features can be provided by the system and the user can be billed.

[0003] EP 0 564 105 A2 proposes a memory module adapter which may be removably inserted into a cellular radio telephone. The memory module adapter has the size and configuration, i.e. electrical contacts, to be compatible with a reader for a credit card sized SIM card in the cellular radio telephone. Further, the memory module adapter comprises a memory module reader such as a plug for a small SIM card. Generally, the memory module adapter is described to be a data card or any other form of package enclosing or carrying a memory device. However, the only disclosure in relation to the exchange of information between the memory module adapter and the cellular telephone is that contacts are provided, which are compatible in size and configuration with a credit card size SIM card reader of the telephone.

[0004] The object of the present invention is therefore to provide a mobile terminal for a wireless telecommunication system which combines the necessity of providing subscriber identity information in a removable device with the advantages of a removable memory module considerably expanding the storage capacity of the mobile terminal. The above object is solved by a mobile terminal for a wireless telecommunication system according to claim 1, which comprises a terminal control means for controlling the function of the mobile terminal and a removable memory module comprising a memory means and a memory control means for controlling the memory means. The memory module is removably connected to the terminal control means by an interface having several connections for exchanging information between the terminal control means and the memory control means, whereby the memory module further comprises a subscriber identity means for providing subscriber identity information to the terminal control module via at least one of said several connections of said interface.

[0005] Thus, the mobile terminal according to the present invention advantageously combines the functions of a removable memory module and a removable SIM card in a single removable device in a simple and effective way. Particularly, the integration of the subscriber identity function and the memory module function into a single removable device ensures a high level of integration. Further, since the subscriber identity means and the memory control means use at least one common connection for exchanging information with the terminal control means a high level of simplicity is achieved.

[0006] Advantageously, the subscriber identity means comprises a connector means for connecting a removable subscriber identity module card. In this case, the removable memory module carries a port or a connector to insert a separate subscriber identity module card.

[0007] Alternatively, the subscriber identity means advantageously comprises a subscriber memory means for storing subscriber identity information. In this case, the subscriber identity function is integrated in the removable memory module and the subscriber memory means is a permanent part of the memory module.

[0008] Advantageously, the subscriber identity means is connected via respective switch means to said at least one of said several connections of said interface. Here, the respective switch means can selectively switch the respective connection of said interface between said memory control means and said subscriber identity means. The subscriber identity means and the memory control means share at least one common connection of the interface and the selective switch means ensures that the wanted subscriber identity function or the memory function of the removable memory module can be selected in a simple way.

[0009] Particularly, switch means can be easily controlled by respective control signals and are easy to integrate so that the entire removable memory module

IPR2025-00645 Page 00142

can be based on a highly integrated IC technology. Advantageously, said at least one connection selectively connected to said subscriber identity means and said memory control means is a data in/out connection. Hereby, data stored in the memory means or subscriber information provided by the subscriber identity means are selectively supplied to or from the same connector connecting the respective data line to a corresponding data in/out connector and line of the terminal control means.

[0010] Advantageously, the respective switch means is controlled by the terminal control means. Hereby, the terminal control means sends a control signal to the respective switch means in order to switch the respective line between the memory control means and the subscriber identity means.

[0011] Alternatively, the respective switch means is advantageously controlled by the memory control means. Hereby, the memory control means transmits a control signal to the respective switch means in order to switch it between the subscriber identity means and the respective line of the memory control means.

[0012] The mobile terminal according to the present invention therefore integrates the subscriber identity function and an additional memory function on a separate removable device in a simple and effective way. Particularly, the integration of these two functions in a single device reduces the space requirements in the mobile terminal. Further, by using the same interface connections for the subscriber identity means and the memory control means of the removable memory module, the number of necessary connections is considerably reduced.

[0013] In the following description, advantageous embodiments of the present invention are explained in more detail in relation to the enclosed drawings, in which

figure 1 shows a mobile terminal and a first embodiment of the removable memory module according to the present invention, and

figure 2 shows a second embodiment of a removable memory module according to the present invention to be used with the mobile terminal shown in figure 1.

[0014] Figure 1 shows a mobile terminal 1 for a wireless telecommunication system, as e.g. the GSM or the UMTS system. The mobile terminal 1 comprises all necessary elements for the operation in a wireless telecommunication system, such as input keys, display, loudspeaker, microphone, antenna, and the like. For the sake of clarity, only the elements important and necessary for the present invention are shown.

[0015] The mobile terminal 1 comprises a terminal control means 2 for controlling the functions of the mobile terminal 1. The terminal control means 2 may e.g. be a microcontroller, a microchip, or the like. Particularly, the terminal control means 2 is adapted to control the information exchange with a removable memory module 5 as shown in a first embodiment in figure 1 or a removable memory module 12 as shown in a second embodiment in figure 2. It is to be understood, that the removable memory modules 5 and 12 shown in figure 1 and 2, respectively, are only shown schematically and that their real sizes are considerably smaller as compared to the size of the mobile terminal 1 according to the present invention.

[0016] The terminal control means 2 of the mobile terminal 1 comprises a group 3 of input/output connections or input/output pins respectively being connected to a corresponding connection or terminal of an interface 4. The removable memory module 5 or 12 is adapted to be removably connected to the interface 4, e.g. by means of a snap-in connection or the like.

[0017] The interface 4 of the mobile terminal 1 comprises, as shown in figure 1, a bus state connection BS connected with a corresponding bus state pin of the terminal control means 2 for providing a bus state signal to a connected memory module 5 or 12. Further, the interface 4 comprises a data input/output connection connected to a corresponding data input/output pin IO of the terminal control means 2 for exchanging input/output data with a connected memory module 5 or 12. The interface 4 further comprises a clock signal connection SCLK connected to a corresponding clock pin CLK of the terminal control means 2 for providing a clock signal to a connected removable memory module 5 or 12. Further, the interface 4 comprises a control voltage terminal VCC connected to a corresponding control voltage pin VCC of the terminal control means 2 for providing a control voltage to a connected removable memory module 5 or 12. The interface 4 further comprises a steady voltage connection VSS connected to a corresponding steady voltage pin VSS of the terminal control means 2 for providing a steady voltage to a connected removable memory module 5 or 12. Typically, the steady voltage terminal VSS of the terminal control means 2 is connected to ground. The interface 4 may further comprise a reserve connection RES connected to a corresponding output pin OUT of the terminal control means 2. The reserve connection RES is e.g. a connection reserved for further use designed to have space for future extensions of the functionality.

[0018] In case of the first embodiment shown in figure 1, the terminal control means 2 supplies a control signal via the output pin OUT and the reserve connection RES of the interface 4 to the connected removable memory module 5 in order to control the switching of the switch means 9 as explained below in more detail. In case of the second embodiment of the removable memory module 12 shown in figure 2, the reserve connection of the interface 4 is not needed to control the removable memory module 12.

[0019] The removable memory module 5 shown in figure 1 comprises a number of electrical connections or terminals to be connected with the connections BS, DIO,

IPR2025-00645 Page 00143

SCLK, VCC, VSS and RES of the interface 4 of the mobile terminal 1. The removable memory module 5 further comprises a memory control means 6 for controlling a memory means 7. The memory control means 6 may e. g. be a microprocessor, a microcontroller or the like. The memory means 7 controlled by the memory control means 6 is a storage unit to which data can be written and from which data can be read.

[0020] Further, the removable memory module 5 comprises a subscriber identity means 8 for providing subscriber identity information. The subscriber identity means 8 is either a connector means for connecting a removable subscriber identity module card or comprises a subscriber memory means for storing subscriber identity information. In the latter case, the subscriber identity means 8 may further comprise a subscriber identity controller means for controlling the reading and writing of subscriber data from and to the subscriber memory means.

[0021] Respective switch means 9 selectively connect some of the connections or terminals of the removable memory module 5 with corresponding connections or terminals of the subscriber identity means 8 and the memory control means 6 in order to control and provide a data exchange as necessary. A first switch means 9 is connected between the bus state signal connection BS of the memory module 5 a reset signal connection RST of the subscriber identity means 8 and a bus state signal connection of the memory control means 6. A second switch means 9 is connected between the data input/output connection DIO of the memory module 5, a subscriber data input/output connection SIO of the subscriber identity means 8 and a data input/output connection of the memory control means 6. A third switch means 9 is connected between the clock signal connection SCLK of the memory module 5, a clock signal connection CLK of the subscriber identity means 8 and a clock signal connection of the memory control means 6. The first, second and third switch means 9 are connected to the reserve connection RES of the memory module 5 to be selectively and simultaneously switched between the respective connections of the memory control means 6 and the subscriber identity means 8.

[0022] The first, second and third switch means 9 may e.g. be configured as shown enlarged in figure 1. In the shown example, the first, second and third switch means 9 respectively comprise a first diode 10 and a second diode 11. A control signal CTL supplied via the reserve connection RES is supplied directly to the first diode 10 but supplied as an inverted signal to the second diode 11. Depending on a supplied control signal CTL, an input signal IN, as e.g. a signal supplied from one of the connections BS, DIO or SCLK, is either supplied via the first diode 10 to the respective connection of the subscriber identity means 8 or via the second diode 11 to the memory control means 6. The control means CTL is supplied from the terminal control means 2 via the OUT pin depending on which of the functionalities of the memory module 5 is required.

[0023] Thus, the connections BS, DIO and SCLK of the memory module 5 are selectively used by the subscriber identity means 8 or the memory control means 6 depending on which of the functionalities is requested by the terminal control means 2. In case that the first, second and third switch means 9 are switched to the subscriber identity means 8, the bus state signal supplied from the terminal control means 2 via the respective bus state signal connections BS is used in the subscriber identity module 8 as a reset signal. Similarly, one or more clock signals supplied from the terminal control means 2 via the respective clock signal connections SCLK is used as a clock signal in the subscriber identity means 8. Subscriber identity data can be supplied to the subscriber identity means 8 via the respective data input/output terminals DIO or read from the subscriber identity means 8 to the terminal control means 2. In case that the first, second and third switch means 9 are switched to the memory control means 6, a bus state signal supplied via the bus state signal connections BS and a clock signal supplied via the clock signal connections SCLK are used in a corresponding way. Data are exchanged via the data input/output connections DIO under the control of the memory control means 6 between the memory means 7 and the terminal control means 2.

[0024] It is to be noted, that the control voltage connection VCC and the steady voltage connection VSS are also connected to the memory control means 6 and/or the subscriber identity means 8 as necessary. However, their function is not important for the understanding of the present invention and thus no connections are shown. Further, the interface 4 as well as the removably memory module 5 may further comprise additional and not shown connections or terminals necessary for further functions as required.

[0025] The same is true for the subscriber identity means 8, which may comprise more than the three connections shown in figure 1 or figure 2, such as an additional connection for supplying a variable supply voltage, as e.g. a programming voltage or the like.

[0026] The subscriber identity means 8 and the memory control means 6 do not necessarily need the same number and kind of clock signals, so that the terminal control means 2 may supply the respectively necessary clock signals via the clock signal connections SCLK depending on which of the two units is addressed. The same is true for the bus state signal supplied from the terminal control means 2 via the bus state signal connections, which may be varied depending on how the setting of the switch means 9 is. For the removable memory module 5 according to the first embodiment shown in figure 1, the terminal control means 2 directly controls and changes the settings of the first, second and third switch means 9 by a control signal supplied via the reserved connections RES. Here, the setting of the first, second and third switch means 9 as directly

IPR2025-00645 Page 00144

changed upon the reception of a control signal from the terminal control means 2.

[0027] Figure 2 shows a schematic diagram of a removable memory module 12 according to the second embodiment of the present invention. The essential features and units of the removable memory module 12 correspond to the ones shown for and explained in relation to the removable memory module 5 shown in figure 1. The main difference is that the reserve connection RES of the interface 4 is not necessary to supply a control signal for changing the settings of the switch means 13 and 14 connecting respective connections of the interface 4, the subscriber identity means 8 and the memory control means 6. In the removable memory module 12 according to the second embodiment shown in figure 2, the clock signal connection SCLK of the memory module 12 is directly and steadily connected to the clock signal connection CLK of the subscriber identity means 8 and the clock signal connection CLK of the memory control means 6. A first switch means 13 is connected between the bus state signal connection BS of the memory module 12, the reset signal connection RST of the subscriber identity means 8 and the bus state signal connection of the memory control means 6. A second switch means 14 is connected between the data input/output connection DIE of the memory module 12, the data input/output connection IO of the subscriber identity means 8 and the data input/output connection of the memory control means 6. The first switch means 13 and the second switch means 14 are respectively connected to and controlled via a switch control signal connection SWCTL of the memory control means 6. Thereby, the first switch means 13 is a three-state output controlled switch means like the first, second and third switch means 9 of the memory module 5 shown in figure 1, whereas the second switch means 15 of the memory module 12 only is a two-state output controlled switch. In other words, the first switch means 13 selectively switches the bus state signal connection BS between the respective connections or terminals of the subscriber identity means 8 and the memory control means 6. On the other hand, the data input/output connection DIO of the memory module 12 is constantly and directly connected to the data input/output connection IO of the memory control means 6. The second switch means 15 is selectively connecting the data input/output connection DIO of the memory module 12 and the data input/output connection IO of the memory control means 6 with the data input/output connection IO of the subscriber identity means 8. Thus, even during the terminal control means 2 is accessing the subscriber identity means 8, the data exchange is being monitored by the memory control means 6. When the terminal control means 2 of the mobile terminal 1 first addresses the removable memory module 12, it sends a first command to the memory control means 6, e.g. via the bus state signal connection BS. The first switch means 13 is thus normally switched to the memory control means 6 and the second switch means 14 is open (disconnected). In case that the terminal control means 2 wants to address the memory control means 6 and the memory means 7, the setting of the first switch 13 and the second switch 14 remains unchanged. In case that the terminal control means 2 wants to access the subscriber identity means 8, the memory control means 6, after the reception of a respective command, outputs a control signal via its switch control connection SWCTL which simultaneously switches the first switch means 13 and the second switch means 14 so that the subscriber identity means 8 can be addressed. While the terminal control means 2 accesses the subscriber identity means 8, the data exchange is monitored by the memory control means 6. When the memory control means 6 recognizes the end of the data transfer between the terminal control means 2 and the subscriber identity means 8, e.g. after detecting that a certain time period has passed without any data having been sent, the memory control means 6 automatically outputs another control signal via the switch control connection SWCTL which switches the first switch means 13 and the second switch means 14 back to their original position.

[0028] Thus, the memory module 12 according to the second embodiment has, compared to the memory module 5 according to the first embodiment, the advantage that one connection less is required for controlling the setting of the switches. On the other hand, the required processing is more complex.

[0029] As shown enlarged in figure 2, the second switch means 14 may comprise a diode 15. A control signal CTL supplied from the switch control connection tap SWCTL of the memory control means 6 is supplied as an inverted signal to the diode 15 in order to selectively connect or disconnect the data input/output connection tap IO of the subscriber identity means 8. The configuration of the first switch means 13 of the memory module 12 can e.g. correspond to the configuration of the switch means 9 shown enlarged in figure 1. The other functionalities and configurations of the subscriber identity means 8, the memory control means 6, the memory means 7 and the several connection taps of the memory module 15 correspond identically to the functionalities and configurations respectively explained in relation to the memory module 5 shown in figure 1.

Claims

1. Mobile terminal (1) for a wireless telecommunication system, with

   a terminal control means (2) for controlling the functions of the mobile terminal, and a removable memory module (5, 12) comprising a memory means (7) and a memory control means (6) for controlling the memory means (7),

IPR2025-00645 Page 00145

said memory module (5, 12) being removably connected to the terminal control means (2) by an interface (4) having several connections for exchanging information between said terminal control means (2) and said memory control means (6),

whereby said memory module (5, 12) further comprises a subscriber identity means (8) for providing subscriber identity information to said terminal control module (2) via at least one of said several connections of said interface (4).

2. Mobile terminal according to claim 1, **characterized in, that** said subscriber identity means (8) comprises a connector means for connecting a removable subscriber identity module card.

3. Mobile terminal according to claim 1, **characterized in, that** said subscriber identity means (8) comprises a subscriber memory means for storing subscriber identity information.

4. Mobile terminal according to claim 1, 2 or 3, **characterized in, that** said subscriber identity means (8) is connected via respective switch means (9, 13, 14) to said at least one of said several connections of said interface (4).

5. Mobile terminal according to claim 4, **characterized in, that** said respective switch means (9, 13, 14) selectively switch a respective connection of said interface (4) between said memory control means (6) and said subscriber identity means (8).

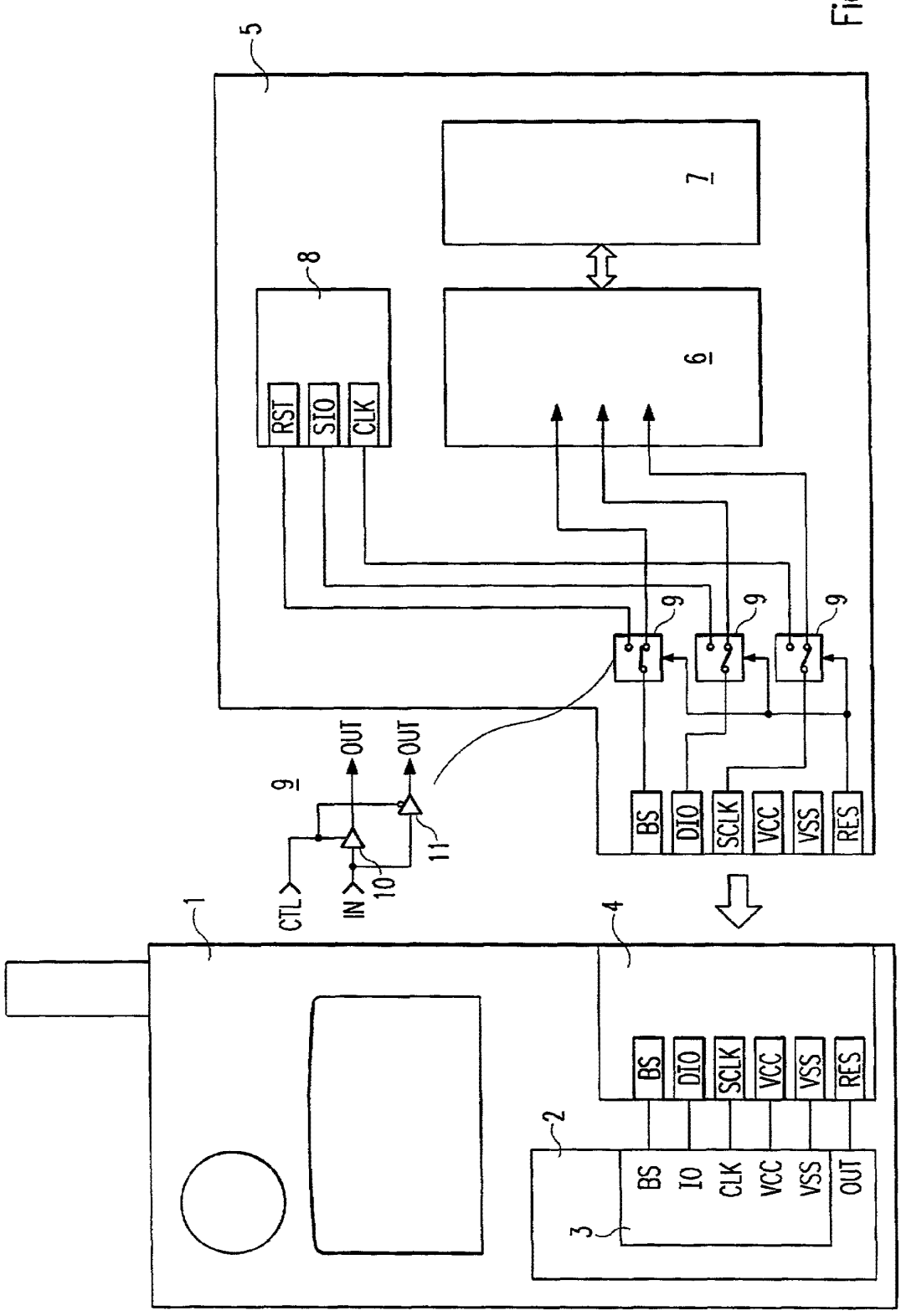
6. Mobile terminal according to claim 4 or 5, **characterized in**, said at least one connection selectively connected to said subscriber identity means (8) and said memory control means (6) is a data in/out connection.

7. Mobile terminal according to claim 4, 5 or 6, **characterized in, that** said respective switch means (5) is controlled by said terminal control means (2).

8. Mobile terminal according to claim 4, 5 or 6, **characterized in, that** said respective switch means (13, 14) is controlled by said memory control means (6).

IPR2025-00645 Page 00146

Fig. 1



IPR2025-00645 Page 00147

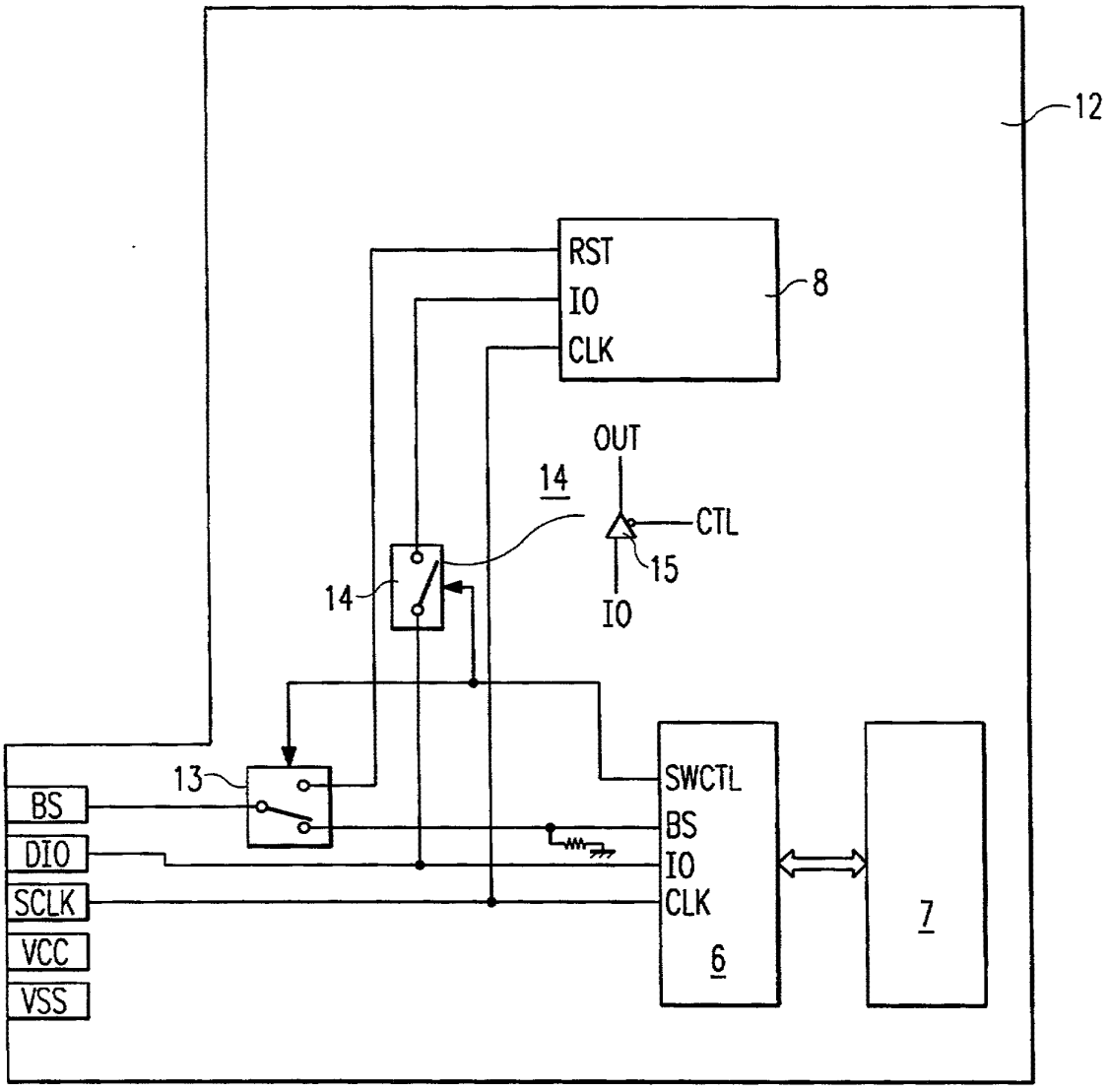


Fig. 2

IPR2025-00645 Page 00148

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 0475

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 633 484 A (SPITULNIK DAVID B ET AL) 27 May 1997 (1997-05-27) * column 2, line 37 - column 3, line 30 * * column 5, line 22 - column 6, line 38 * * abstract; claims 1-44 *	1-8	H04Q7/32
X	FR 2 748 834 A (GEMPLUS CARD INT) 21 November 1997 (1997-11-21) * page 1, line 1 - page 3, line 18 * * abstract * * figures 1,3A,3B,4,10 *	1-8	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04Q
G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	9 March 2001	Coppieters, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

IPR2025-00645 Page 00149

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 12 0475

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-03-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5633484 A	27-05-1997	CA 2165278 A,C	30-06-1996
		CN 1132874 A	09-10-1996
		DE 19548393 A	11-07-1996
		ES 2112198 A	16-03-1998
		FR 2729038 A	05-07-1996
		GB 2296584 A,B	03-07-1996
		IT RM950854 A	01-07-1996
		JP 8255033 A	01-10-1996
		US 5814798 A	29-09-1998
FR 2748834 A	21-11-1997	AU 718446 B	13-04-2000
		AU 3035797 A	09-12-1997
		CA 2255593 A	27-11-1997
		EP 0906603 A	07-04-1999
		FR 2748880 A	21-11-1997
		WO 9744762 A	27-11-1997
		JP 2000510977 T	22-08-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

IPR2025-00645 Page 00150

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 291 748 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.03.2003 Bulletin 2003/11

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **02018821.5**

(22) Date of filing: **23.08.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **11.09.2001 US 952003**

(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventors:
- **Stevens, Gilman R.**
Fairview, TX 75069 (US)
- **Mani, Babu V.**
Plano, TX 75025 (US)

(74) Representative: **Schäfer, Wolfgang, Dipl.-Ing.**
Dreiss, Fuhlendorf, Steimle & Becker
Postfach 10 37 62
70032 Stuttgart (DE)

(54) Electronic device capable of wirelessly transmitting a password that can be used to unlock/lock a password protected electronic device

(57) An electronic device is described which can be used by a user to unlock a locked password protected electronic device (e.g., PDA, wireless phone, laptop computer, personal computer...). To unlock the locked password protected electronic device, the user activates the electronic device to wirelessly transmit a password (e.g., electronic key) towards the locked password protected electronic device. The locked password protected electronic device uses the received password to unlock itself so that the user does not have to remember the password and also does not have to physically input the password into the locked password protected electronic device in order to unlock and use the password protected electronic device. The electronic device can also be used by the user to lock an unlocked password protected electronic device. Moreover, the electronic device can be incorporated within an article that the user generally has in his/her possession including a ring or a watch.

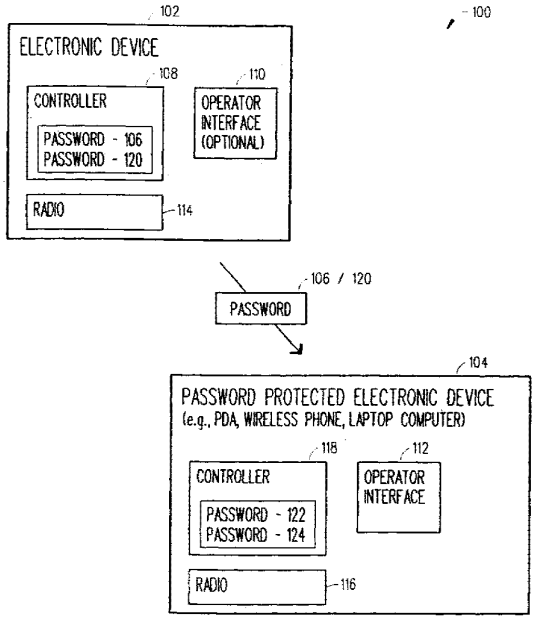


FIG. 1

EP 1 291 748 A2

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates in general to an electronic device capable of using wireless technology to transmit a password that can be used to unlock/lock a password protected electronic device.

Description of Related Art

[0002] Today personal digital assistants (PDAs), laptop computers, wireless phones, personal computers and other electronic devices often have a password protection feature that prevents an unauthorized user from using the password protected electronic device. The traditional password protection feature requires a user to physically enter a password into the password protected electronic device before they can use the password protected electronic device. One problem with the traditional password protection feature is that the user can easily forget the password needed to unlock the password protected electronic device. Of course, if the user forgets the password they cannot unlock and use the password protected electronic device. It is easy for the user to forget the password, because they can simply confuse this password with all the other passwords they need to remember in order to access things such as ATM machines, Internet sites and other password protected electronic devices.

[0003] Another problem with the traditional password protection feature is that it can be physically difficult for the user to enter the password into the password protected electronic device. For instance, the user of a PDA must use a small pen to enter a password into the PDA which is difficult because there is a good chance the user will make a mistake by hitting a wrong key. In other words, it is just plain hard and time consuming for a user to unlock a PDA using a small pen. Accordingly, there has been a need for an electronic device that helps a user to unlock a password protected electronic device. This need and other needs are satisfied by the electronic device of the present invention.

BRIEF DESCRIPTION OF THE INVENTION

[0004] The present invention includes an electronic device that can be used by a user to unlock a locked password protected electronic device (e.g., PDA, wireless phone, laptop computer, personal computer...). To unlock the locked password protected electronic device, the user activates the electronic device to wirelessly transmit a password (e.g., electronic key) towards the locked password protected electronic device. The locked password protected electronic device uses the received password to unlock itself so that the user does not have to remember the password and also does not have to physically input the password into the locked password protected electronic device in order to unlock and use the locked password protected electronic device. The electronic device can also be used by the user to lock an unlocked password protected electronic device. Moreover, the electronic device can be incorporated within an article that the user generally has in his possession including a ring or a watch.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] A more complete understanding of the present invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

FIGURE 1 is a block diagram illustrating the basic components of a system in accordance with the present invention;
FIGURE 2 is a block diagram illustrating in greater detail a first embodiment of an electronic device of the system shown in FIGURE 1;
FIGURES 3A and 3B are block diagrams illustrating in greater detail a second embodiment of the electronic device of the system shown in FIGURE 1;
FIGURE 4 is a block diagram illustrating in greater detail a third embodiment of the electronic device of the system shown in FIGURE 1;
FIGURE 5 is a block diagram illustrating in greater detail a fourth embodiment of the electronic device of the system shown in FIGURE 1; and
FIGURE 6 is a flowchart illustrating the basic steps of a preferred method in accordance with the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0006] Referring to FIGURE 1, there is a block diagram illustrating the basic components of the preferred system 100 in accordance with the present invention. The system 100 includes an electronic device 102 and a password protected electronic device 104. Basically, the user can activate the electronic device 102 (e.g., wireless electronic key transmitter, electronic key device) to wirelessly transmit a password 106 (e.g., electronic key) to a locked password protected electronic device 104. The locked password protected electronic device 104 uses the received password 106 to unlock itself so that the user does not have to remember the password 106 and also does not have to physically input the password 106 into the password protected electronic device 104 in order to unlock and use the password protected electronic device 104. The password protected electronic device 104 can be any type of electrical device including, for example, a personal digital assistant (PDA), a laptop computer, a wireless phone and a personal computer. The electronic device 102 can be incor-

IPR2025-00645 Page 00152

porated within an article that the user generally has in his possession including, for example, a ring or a watch.

[0007] The electronic device 102 includes a controller 108 that stores the password 106. There are several different ways in which a user or a manufacturer can select the password 106 and to input the selected password 106 into the controller 108. For example in the first embodiment, the user can interact with an operator interface 110 on the electronic device 102 to select the password 106 and to input the selected password 106 into the electronic device 102 (see FIGURE 2). In the second embodiment, the user can interact with an operator interface 112 on the password protected electronic device 104 to select the password 106 and direct the password protected electronic device 104 to transmit the selected electronic key 106 to the electronic device 102 (see FIGURES 3A and 3B). In the third embodiment, a manufacturer of the electronic device 102 and the password protected electronic device 104 can select the password 106 and input the password 106 into the electronic device 102 and the password protected electronic device 104 (see FIGURE 4).

[0008] To unlock a locked password protected electronic device 104, the user activates the electronic device 102 to wirelessly transmit the password 106 towards the locked password protected electronic device 104. In particular, the electronic device 102 includes a radio 114 (e.g., transmitter and receiver) that wirelessly transmits the password 106 towards the password protected electronic device 104.

[0009] The password protected electronic device 104 includes a radio 116 (e.g., transmitter and receiver) which receives the password 106 transmitted from the radio 114. The password protected electronic device 104 also includes a controller 118 that has stored therein a password 122 which is compared to the password 106 received from the electronic device 102. If there is a match, then the password protected electronic device 104 unlocks itself so that the user is able to use the password protected electronic device 104. Otherwise, if there is not a match, then the password protected electronic device 104 does not unlock itself and the user is not able to use the password protected electronic device 104.

[0010] Typically, the user activates the electronic device 102 to transmit the password 106 when the electronic device 102 is located relatively near the locked password protected electronic device 104. Preferably, the electronic device 102 uses a short-range radio frequency communication technology to transmit the password 106 towards the locked password protected electronic device 104. As such, the electronic device 102 can transmit the password 106 towards the locked password protected electronic device 104 using any one of a wide array of wireless technologies including, for example, Bluetooth technology and Infra Red technology.

[0011] In addition the user can use the electronic device 102 to lock an unlocked password protected electronic device 104, to do this the user activates the electronic device 102 to wirelessly transmit a second password 120 (e.g., electronic key) towards the unlocked password protected electronic device 104. In particular, the user activates the radio 114 (e.g., transmitter and receiver) to wirelessly transmits the second password 120 towards the password protected electronic device 104. The radio 116 within the password protected electronic device 104 receives the second password 120 transmitted from the radio 114 within the electronic device 102. The controller 118 within the password protected electronic device 104 has stored therein another password 124 which is compared to the second password 120 received from the electronic device 102. If there is a match, then the password protected electronic device 104 locks itself so that the user is not able to use the password protected electronic device 104. Otherwise, if there is not a match, then the password protected electronic device 104 does not lock itself and the user is still able to use the password protected electronic device 104. It should be understood that the first password 106 and the second password 120 can be the same such that if the password protected electronic device 104 receives the first password 106 its state can change from locked-to-unlocked or unlocked-to-locked.

[0012] This way of unlocking/locking a password protected electronic device 104 is an improvement over the state-of-the-art because the user can use the electronic device 102 to unlock/lock the password protected electronic device 104 instead of having to remember password(s) and without having to physically input the password(s) into the password protected electronic device 104 in order to unlock/lock the password protected electronic device 104.

[0013] It should also be noted that certain details associated with the radios 114 and 116 and the controllers 108 and 118 are known in the industry and as such need not be described in detail herein. Therefore, for clarity, the description provided herein in relation to the radios 114 and 116 and the controllers 108 and 118 omits some components not necessary to understand the invention. However, detailed descriptions about the different embodiments of the electrical device 102 are provided below with respect to FIGURES 2-5.

[0014] Referring to FIGURE 2, there is a block diagram illustrating in greater detail a first embodiment of the electronic device 102a. In this embodiment, the user interacts with the operator interface 110a to select the password 106a and to input the selected password 106a into the electronic device 102a (shown incorporated within a watch 202).

[0015] The operator interface 110a can display a set of alphanumerics from which the user by pushing a button 204 or moving a knob (not shown) can select any one and any number of the alphanumerics to create the password 106a (e.g., password "HOME246"). The user can then push another button 206 or move the knob in a predetermined way to store the selected password

IPR2025-00645 Page 00153

106a (e.g., password "HOME246") in the controller 108a. The user would also interact with the operator interface 112a on the password protected electronic device 104a (shown as a personal computer) to input and store therein the password 122a (e.g., password "HOME246").

[0016] Thereafter, when the user wants to use the locked password protected electronic device 104a, they would press another button 208 or move a knob in a certain way such that the electronic device 102a is activated to wirelessly transmit the password 106a (e.g., password "HOME246") towards the locked password protected electronic device 104a. As mentioned above, the electronic device 102a preferably uses a short-range radio frequency communication technology (e.g., Bluetooth technology, Infra Red technology) to transmit the password 106a (e.g., password "HOME246") to the locked password protected electronic device 104a. The controller 118a within the locked password protected electronic device 104a compares the received password 106a (e.g., password "HOME246") to the stored password 122a (e.g., password "HOME246"). If there is a match, then the password protected electronic device 104a unlocks itself so that the user is able to use the password protected electronic device 104a. Otherwise, if there is not a match, then the password protected electronic device 104a does not unlock itself and the user is not able to use the password protected electronic device 104a.

[0017] It should also be noted that the user can also use the electronic device 102a to transmit a second password (not shown) in a similar manner to lock the unlocked password protected electronic device 104a when they are done using the unlocked password protected electronic device 104a.

[0018] Referring to FIGURES 3A and 3B, there are respectively shown two block diagrams illustrating in greater detail a second embodiment of the electronic device 102b. In this embodiment, the user interacts with the operator interface 112b on the password protected electronic device 104b (shown as a wireless phone) to select the password 106b (e.g., password "TIGERS"). The user then directs the password protected electronic device 104b to transmit the selected electronic key 106b (e.g., password "TIGERS") to the electronic device 102b (shown incorporated in a watch 302) (see FIGURE 3A). At this point, the controllers 108b and 118b respectively have stored therein the password 106b and 122b.

[0019] Thereafter, when the user wants to use the locked password protected electronic device 104b, they would press a button (not shown) or move a knob 304b in a certain way (e.g., clock-wise direction) such that the radio 114b in the electronic device 102b is activated to wirelessly transmit the password 106b (e.g., password "TIGERS") towards the radio 116b within the password protected electronic device 104b (see FIGURE 3B). Again, the electronic device 102b preferably uses a short-range radio frequency communication technology (e.g., Bluetooth technology, Infra Red technology) to transmit the password 106b (e.g., password "TIGERS") to the locked password protected electronic device 104b. The controller 118b within the locked password protected electronic device 104b compares the received password 106b (e.g., password "TIGERS") to the stored password 122b (e.g., password "TIGERS"). If there is a match, then the password protected electronic device 104b unlocks itself so that the user is able to use the password protected electronic device 104b. Otherwise, if there is not a match, then the password protected electronic device 104b does not unlock itself and the user is not able to use the password protected electronic device 104b.

[0020] It should be noted that the electronic device 102b (or any other embodiments of the electronic devices 102) could be set in a locked mode to prevent accidental transmittal of the password towards password protected electronic devices 104.

[0021] It should also be noted that the user can also use the electronic device 102b to transmit a second password (not shown) in a similar manner to lock the unlocked password protected electronic device 104b when they are done using the unlocked password protected electronic device 104b.

[0022] Compared to the first embodiment of the electronic device 102a, the electronic device 102b may not require an operator interface (not shown). Because, the electronic device 102b only needs to be able to receive and store a password and then enable the user to activate the electronic device 102b so that the radio 114b transmits the password when they want to unlock/lock the password protected electronic device 104b.

[0023] Referring to FIGURE 4, there is shown a block diagram illustrating in greater detail a third embodiment of the electronic device 102c. In this embodiment, the user need not select the password 106c or input the password 106c into the electronic device 102c (shown incorporated within a ring 402). Instead, a manufacturer of the electronic device 102c and the password protected electronic device 104c (shown as a personal computer) can pre-program the password 106c (e.g., password "120de0C") into each device 102c and 104c. The manufacturer could sell the electronic device 102c and the password protected electronic device 104c as a pair to the user.

[0024] Thereafter, when the user wants to use the locked password protected electronic device 104c, they only need to move a knob 404 (shown as a rock) on the electronic device 102c in a certain way (i.e., clock-wise direction) such that the electronic device 102c is activated to wirelessly transmit the password 106c (e.g., password "120de0C") towards the password protected electronic device 104c. Again, the electronic device 102c preferably uses a short-range radio frequency communication technology (e.g., Bluetooth technology, Infra Red technology) to transmit the password 106c (e.g., password "120d ") to the locked password protected

IPR2025-00645 Page 00154

electronic device 104c. The controller 118c within the locked password protected electronic device 104c compares the received password 106c (e.g., password "120de0C ") to the stored password 106c (e.g., password "120de0C "). If there is a match, then the password protected electronic device 104c unlocks itself so that the user is able to use the password protected electronic device 104c. Otherwise, if there is not a match, then the password protected electronic device 104c does not unlock itself and the user is not able to use the password protected electronic device 104c.

[0025] It should also be noted that the user can also use the electronic device 102c to transmit a second password (not shown) in a similar manner to lock the unlocked password protected electronic device 104c when they are done using the unlocked password protected electronic device 104c.

[0026] Like the second embodiment of the electronic device 102b, the electronic device 102c does not require the operator interface (not shown). Because, the electronic device 102c only needs a knob or button of some sort to enable the user to activate the electronic device 102c so that it transmits a password when they want to unlock/lock the password protected electronic device 104c.

[0027] Following is an example of one possible application of the present invention, a PDA (e.g., password protected electronic device) and "special" watch (e.g., electronic device) can be sold as a pair to a person. The "special" watch can be programmed by the manufacturer (or person) to wirelessly transmit a particular password when a button is pushed by the person such that the transmitted password can be received by the password protected PDA. Upon receiving the password, the PDA can be unlocked and used by the person without having to physically input the password into the PDA. Of course, the PDA would have to be physically close to the "special" watch when the password is transmitted.

[0028] Referring to FIGURE 5, there is shown a block diagram illustrating in greater detail a fourth embodiment of the electronic device 102d. In this embodiment, the user can use the electronic device 102d (shown incorporated within a watch 502) to unlock/lock more than one password protected device 104d (shown are laptop computer 502, PDA 504 and wireless phone 506).

[0029] The user interacts with the operator interface 110d to select one or more passwords 106d, 106d' and 106d" (only three shown) and to input the selected passwords 106d, 106d' and 106d" into the controller 108d of the electronic device 102d. It should be noted that any of the other ways described above with respect to the second and third embodiments of the electronic device 102b and 102c can also be used to select and input the passwords 106d, 106d' and 106d" into the electronic device 102d. Each password protected electronic device 104d and controller 118d is programmed to store their own password 106d, 106d' and 106d".

[0030] Thereafter, when the user wants to use one of the locked password protected electronic devices 104d, they only need to press a button 508 or move a knob (not shown) in a certain way such that the electronic device 102d (e.g., radio 114d) is activated to wirelessly transmit one of the passwords 106d, 106d' and 106d" towards one of the password protected electronic devices 104d. For instance, the user can activate the electronic device 102d so that it only transmits password 106d' towards the PDA 504 (as shown). Again, the electronic device 102d preferably uses a short-range radio frequency communication technology (e.g., Bluetooth technology, Infra Red technology) to transmit the password 106d' to the locked PDA 504. The controller 118d within the locked PDA 504 compares the received password 106d' to the stored password 122d'. If there is a match, then the PDA 504 unlocks itself so that the user is able to use the PDA 504. Otherwise, if there is not a match, then the PDA 504 does not unlock itself and the user is still not able to use the PDA 504.

[0031] It should be understood that the electronic device 102d could be programmed to store only one electronic key 106d that can be used to unlock/lock any number of password protected electronic devices 104d.

[0032] Referring to FIGURE 6, there is a flowchart illustrating the basic steps of a preferred method 600 in accordance with the present invention. Basically, the user can activate the electronic device 102 to wirelessly transmit a password 106 (e.g., electronic key) to a locked password protected electronic device 104. The locked password protected electronic device 104 uses the received password 106 to unlock itself so that the user does not have to remember the password 106 and also does not have to physically input the password 106 into the password protected electronic device 104 in order to unlock and use the password protected electronic device 104. Again, the password protected electronic device 104 can be any type of electrical device including, for example, a personal digital assistant (PDA), a laptop computer, a wireless phone and a personal computer. The electronic device 102 can be incorporated within an article that the user generally has in their possession including, for example, a ring or a watch.

[0033] Beginning at step 602, the electronic device 102 is programmed to store the password 106. There are several ways in which a user or a manufacturer can select the password 106 and input the selected password 106 into the electronic device 102. For example, the user can interact with the operator interface 110 on the electronic device 102 to select the password 106 and to input the selected electronic key 106 into the electronic device 102 (see FIGURE 2). Alternatively, the user can interact with the operator interface 112 on the password protected electronic device 104 to select the password 106 and direct the password protected electronic device 104 to transmit the selected password 106 to the electronic device 102 (see FIGURES 3A and 3B). Or, a manufacturer of the electronic device 102 and the password protected electronic device 104 can select the

IPR2025-00645 Page 00155

password 106 and input the selected password 106 into the electronic device 102 and the password protected electronic device (see FIGURE 4).

[0034] At step 604, the user activates the electronic device 102 to wirelessly transmit the password 106 towards the locked password protected electronic device 104. In particular, the user may push a button or move a knob in a certain direction to activate the electronic device 102 so that it transmits the password 106. Typically, the user activates the electronic device 102 to transmit the password 106 when the electronic device 102 is located relatively near the locked password protected electronic device 104. Preferably, the electronic device 102 uses a short-range radio frequency communication technology to transmit the password 106 towards the locked password protected electronic device 104. As such, the electronic device 102 can transmit the password 106 towards the locked password protected electronic device 104 using any one of a wide array of wireless technologies including, for example, Bluetooth technology and Infra Red technology.

[0035] At step 606, the locked password protected electronic device 104 compares the received password 106 to a stored password. If there is not a match, then at step 608, the password protected electronic device 104 does not unlock itself and the user is not able to use the password protected electronic device 104. If there is a match, then at step 610, the password protected electronic device 104 unlocks itself so that the user is able to use the password protected electronic device 104.

[0036] This way of unlocking the password protected electronic device 104 is an improvement over the state-of-the-art because the user can use the electronic device 102 to unlock the password protected electronic device 104 instead of having to remember a password and then having to physically input the password into the password protected electronic device 104 in order to unlock and use the password protected electronic device 104.

[0037] At step 612, the electronic device 102 is programmed to store the second password 120. Like described above, there are several ways in which the user or the manufacturer can select the second password 120 and input the selected second password 120 into the electronic device 102. For example, the user can interact with the operator interface 110 on the electronic device 102 to select the second password 120 and to input the selected password 106 into the electronic device 102 (see FIGURE 2). Alternatively, the user can interact with the operator interface 112 on the password protected electronic device 104 to select the second password 120 and direct the password protected electronic device 104 to transmit the selected second password 120 to the electronic device 102 (see FIGURES 3A and 3B). Or, a manufacturer of the electronic device 102 and the password protected electronic device 104 can select the second password 120 and input the selected second password 120 into the electronic device 102 and the password protected electronic device (see FIGURE 4).

[0038] At step 614, the user activates the electronic device 102 to wirelessly transmit the second password 120 towards the unlocked password protected electronic device 104. In particular, the user may push a button or move a knob in a certain direction to activate the electronic device 102 so that it transmits the second password 120. Like above, the user activates the electronic device 102 to transmit the second password 120 when the electronic device 102 is located relatively near the locked password protected electronic device 104. Preferably, the electronic device 102 uses a short-range radio frequency communication technology to transmit the second password 120 towards the unlocked password protected electronic device 104. As such, the electronic device 102 can transmit the second password 120 towards the unlocked password protected electronic device 104 using any one of a wide array of wireless technologies including, for example, Bluetooth technology and Infra Red technology.

[0039] At step 616, the unlocked password protected electronic device 104 compares the received second password 120 to a stored second password. If there is not a match, then at step 618, the password protected electronic device 104 does not lock itself and the user is still able to use the password protected electronic device 104. If there is a match, then at step 620, the password protected electronic device 104 locks itself so that the user is not able to use the password protected electronic device 104.

[0040] This way of locking the password protected electronic device 104 is an improvement over the state-of-the-art because the user can use the electronic device 102 to lock the password protected electronic device 104 instead of having to remember a password and then having to physically input the password into the password protected electronic device 104 in order to lock the password protected electronic device 104.

[0041] It should be understood that steps 602-610 are associated with a user trying to unlock a locked password protected electronic device 104, and steps 612-620 are associated with a user attempting to lock an unlocked password protected electronic device 104. The user may still physically enter the password(s) into the password protected electronic device 104 to unlock/lock the password protected electronic device 104.

[0042] It should also be understood that the first password 106 and the second password 120 can be one in the same. If this is the case, the password protected electronic device 104 would alternatively unlock and lock itself upon receiving a correct password.

[0043] Following are some other advantages, features and capabilities of the present invention:

- To provide additional security, the electronic device can encrypt the first password and the second pass-

IPR2025-00645 Page 00156

word.

- Security can be further enhanced by using more than one password (e.g., electronic key); for instance, transmitting multiple passwords in a special sequence that can be chosen by the user.
- The user can select the mode by pressing a button or by moving a knob to a certain position and then pressing another button to transmit the password.
- The user can program the electronic device 102 to have separate key sequence for different password protected electronic devices. Here, the actual password is only known to the password protected electronic device being turned on (the target device) and the electronic device that is used to send the key (password) is just capable of generating the right keys. Again, security can be enhanced by programming the electronic device only to generate the programmed keys, i.e., the electronic device cannot be used to generate other passwords or keys.
- The user can physically input the password(s) into the password protected electronic device in the event the electronic device is not available (e.g., lost, misplaced) or not functioning (e.g., battery ran out).
- People that need to unlock/lock password protected electronic devices would have an easy, inexpensive way to do this without having to remember and physically input a password into the electronic device.
- The present invention is more convenient and cost effective for businesses to use when compared to a hard token which is used to send a password to a central location for access to corporate networks.
- The password entered directly into the password protected device could be different from the one stored in the electronic key device. This directly entered password can also be treated as a master password, which can be used to enable/disable the use of an electronic key device; this is useful in case, the electronic key device is lost or stolen.
- Programmability: some electronic devices can have permanent passwords (factory installed forever) while other electronic devices are programmable in that passwords can be changed as desired. In the latter case, the user decides the password and nobody else knows the password.
- Password(s) can be transmitted by a single keypress or a sequence of key-presses (with a fixed interval, or at different angles, or two separate keys...).
- If the password protected electronic device is capable of exchanging information with the electronic device used to transmit the password, then the device ID of the electronic device can also be transmitted upon request from the password protected electronic device or it can be transmitted along with the password. One possible scenario is provided below:

  First, the electronic key device transmits its ID to the password protected device.
  Second, the password protected device queries the electronic key device for a password; it also transmits its ID.
  Thirdly, the electronic key device selects the password for the identified device and transmits that password.
  Finally, the password protected device compares the received password with the stored password and then unlocks the password protected device (if they match).

[0044] An advantage of this scenario is that the user does not have to remember which way to turn, press or open a particular device. And, each device can have a different password since exchange of information is automatic, i.e., the user does not have to be aware of this.

[0045] Although several embodiments of the present invention has been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it should be understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

Claims

1. An electronic device, comprising:

   a controller for storing a first password; and
   a radio for transmitting the stored first password towards a password protected electronic device, wherein the password protected electronic device uses the received first password to unlock itself such that a user does not have to physically input the first password into the password protected electronic device to unlock and use the password protected electronic device.

2. The electronic device of Claim 1, further comprising an operator interface used by the user to activate said radio to transmit the first password towards the password protected electronic device.

3. The electronic device of Claim 1, further comprising an operator interface used by the user to select the first password and to store the selected first password into said controller.

4. The electronic device of Claim 1, wherein the user interacts with the password protected electronic device to select the first password and transmit the selected first password to said radio for storage in said controller.

IPR2025-00645 Page 00157

5. The electronic device of Claim 1, wherein a manufacturer of the electronic device and the password protected electronic device selects the first password and stores the selected first password In said controller and said password protected electronic device.

6. The electronic device of Claim 1, wherein:

said controller is further capable of storing a second password; and
said radio is further capable of transmitting the second password towards the password protected electronic device, wherein the password protected electronic device uses the received second password to lock itself such that the user does not have to physically input the second password into the password protected electronic device to lock the password protected electronic device.

7. The electronic device of Claim 1, wherein said electronic device is incorporated within a ring.

8. The electronic device of Claim 1, wherein said electronic device is incorporated within a watch.

9. The electronic device of Claim 1, wherein said password protected electronic device is a personal digital assistant.

10. The electronic device of Claim 1, wherein said password protected electronic device is a personal computer.

11. The electronic device of Claim 1, wherein said password protected electronic device is a wireless phone.

12. A method for using wireless technology to unlock a password protected electronic device, said method comprising the steps of:

storing a first password in an electronic device; and
activating the electronic device to wirelessly transmit the first password towards the password protected electronic device, wherein the password protected electronic device uses the received first password to unlock itself such that a user does not have to physically input the first password into the password protected electronic device to unlock and use the password protected electronic device.

13. The method of Claim 12, further comprising the step of encrypting the transmitted first password.

14. The method of Claim 12, wherein said step of storing further includes enabling the user to select the first password and to input the selected first password into the electronic device.

15. The method of Claim 12, wherein said step of storing further includes enabling the user to interact with the password protected electronic device to select the first password and to transmit the selected first password to the electronic device.

16. The method of Claim 12, wherein said step of storing further includes enabling a manufacturer to select the first password and to input the selected first password into the electronic device and the password protected electronic device.

17. The method of Claim 12, further comprising the steps of:

storing a second password in the electronic device; and
activating the electronic device to wirelessly transmit the second password towards the password protected electronic device, wherein the password protected electronic device uses the received second password to lock itself such that the user does not have to physically input the second password into the password protected electronic device to lock the password protected electronic device.

18. The method of Claim 12, wherein said first electronic device is incorporated within an article that the user generally has in their possession including a ring or a watch.

19. The method of Claim 12, wherein said password protected electronic device is a personal digital assistant.

20. The method of Claim 12, wherein said password protected electronic device is a personal computer.

21. The method of Claim 12, wherein said password protected electronic device is a wireless phone.

22. The method of Claim 12, wherein said wireless technology is Infra Red technology.

23. The method of Claim 11, wherein said wireless technology is Bluetooth technology.

24. A password protected electronic device, comprising:

a radio capable of receiving a password wirelessly transmitted from an electronic device;

IPR2025-00645 Page 00158

and

a controller capable of using the received password to unlock the password protected electronic device such that a user does not have to physically input the password into the password protected electronic device to unlock and use the password protected electronic device.

25. The password protected electronic device of Claim 24, wherein said electronic device is incorporated within a ring.

26. The password protected electronic device of Claim 24, wherein said electronic device is incorporated within a watch.

27. The password protected electronic device of Claim 24, wherein said password protected electronic device is a personal digital assistant.

28. The password protected electronic device of Claim 24, wherein said password protected electronic device is a personal computer.

29. The password protected electronic device of Claim 24, wherein said password protected electronic device is a wireless phone.

30. A system, comprising:

a first electronic device including:

a controller capable of storing a password; and

a radio capable of transmitting the password when activated by a user; and

a second electronic device including:

a controller capable of storing a password;

a radio capable of receiving the password from the first electronic device; and

said controller capable of determining whether the stored password matches the received password;

if there is a match, then the second device unlocks itself so that the user can use the second device;

if there is not a match, then the second device remains locked and the user can not use the second device.

31. The system of Claim 30, wherein said first electronic device further includes an operator interface used by the user to activate said radio to transmit the password towards the second electronic device

32. The system of Claim 30, wherein said first electronic device further includes an operator interface used by the user to select the password and to input the selected password into the first electronic device.

33. The system of Claim 30, wherein said second electronic device further includes an operator interface used by the user to select the password and to transmit the selected password to the first electronic device.

34. The system of Claim 30, wherein a manufacturer of the first electronic device and the second electronic device selects and inputs the password into the first electronic device and the second electronic device.

35. The system of Claim 30, wherein said first electronic device is incorporated within an article that the user generally has in their possession including a ring or a watch.

36. The system of Claim 30, wherein said second electronic device is a personal digital assistant, a personal computer, a laptop computer or a wireless phone.

37. A device, comprising:

a radio capable of transmitting at least one electronic key towards at least one electronic device, wherein each electronic key includes a password used to unlock or lock one of the electronic devices such that a user does not have to remember the password and does not have to physically input the password into the at least one electronic device to unlock or lock the at least one electronic device.

38. The device of Claim 37, wherein said electronic key is an encrypted electronic key.

39. The device of Claim 37, wherein said device is incorporated within an article that the user generally has in their possession including a ring or a watch.

40. The device of Claim 37, wherein said electronic device is a personal digital assistant, a personal computer or a wireless phone.

IPR2025-00645 Page 00159

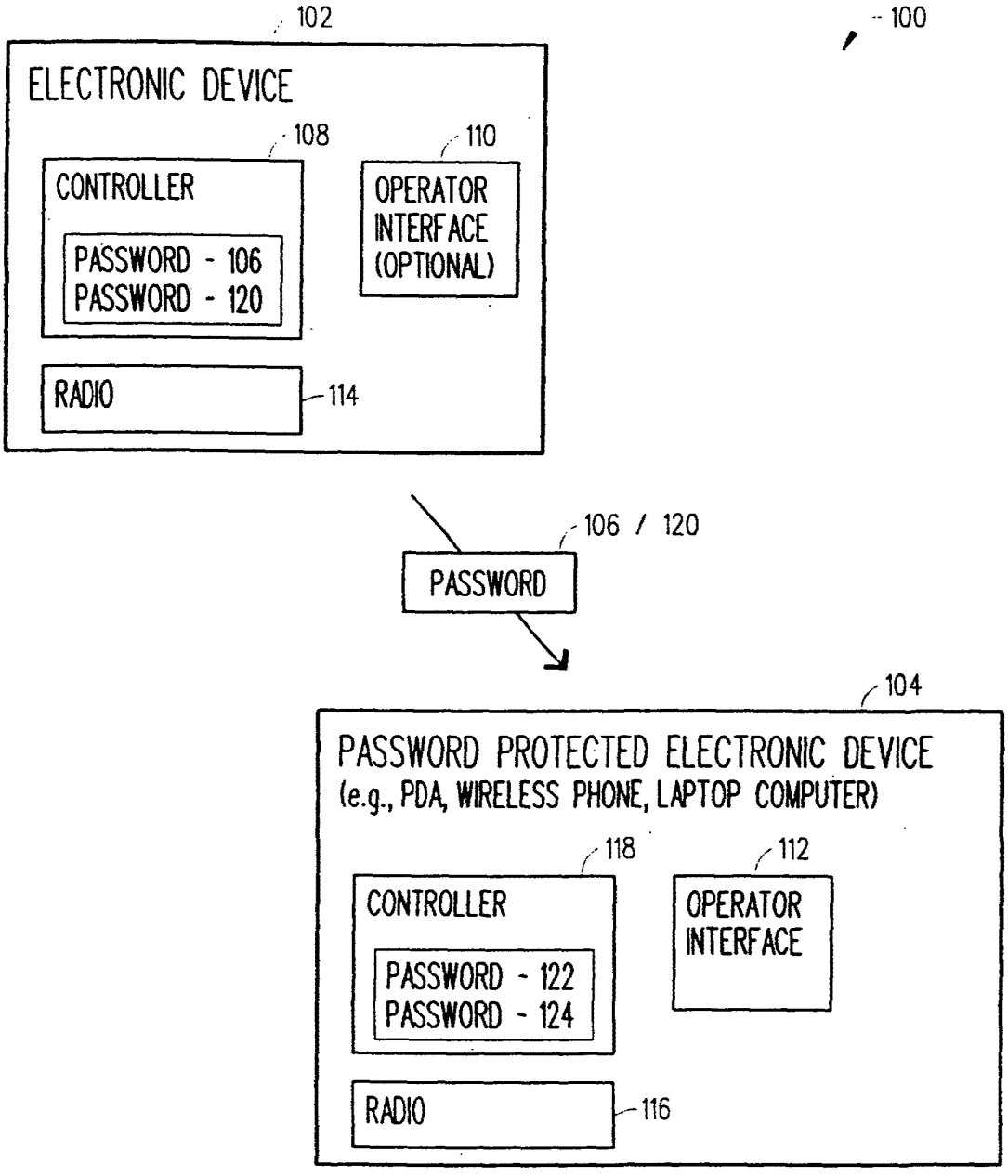


FIG. 1

IPR2025-00645 Page 00160

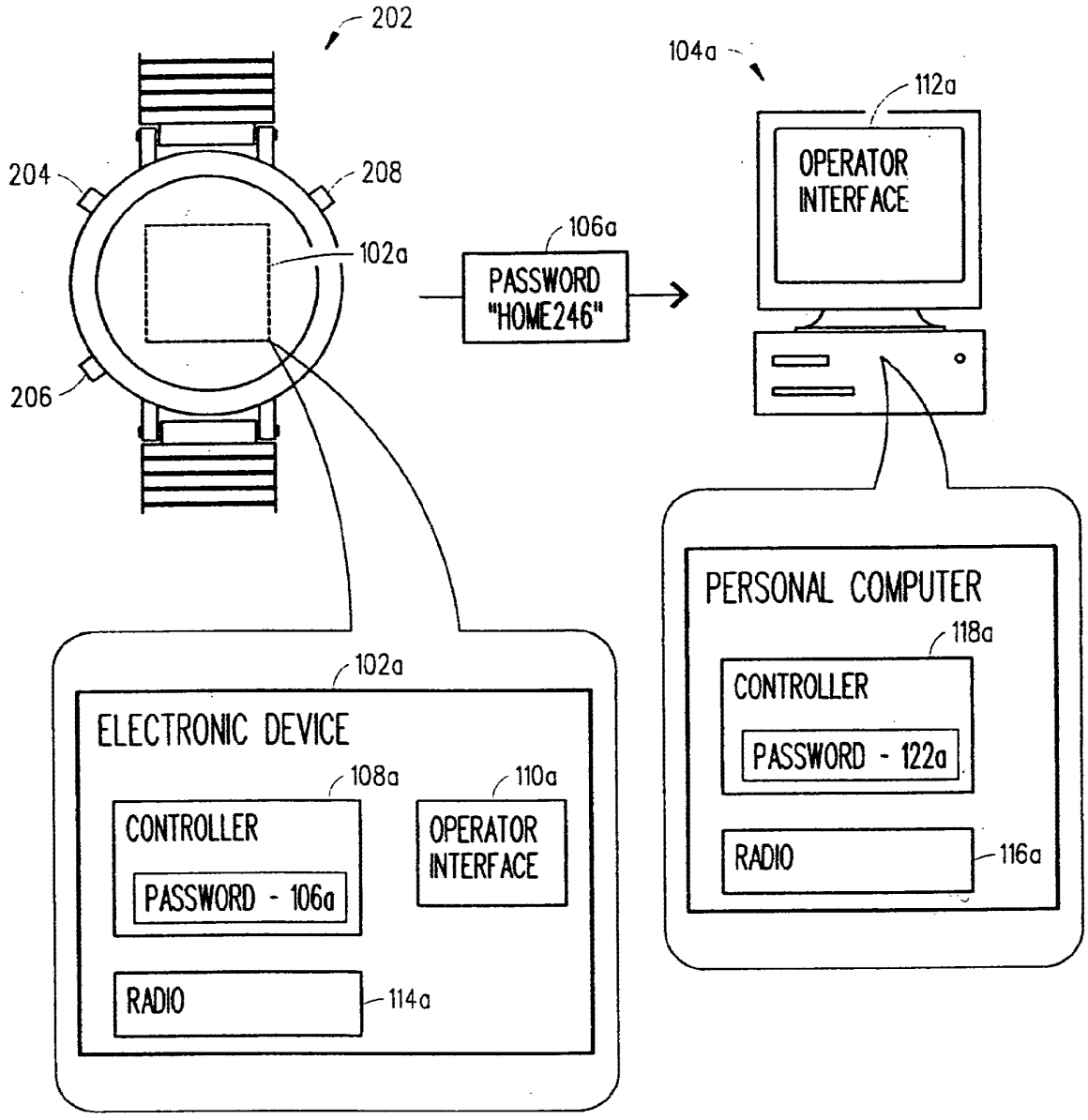


FIG. 2

IPR2025-00645 Page 00161

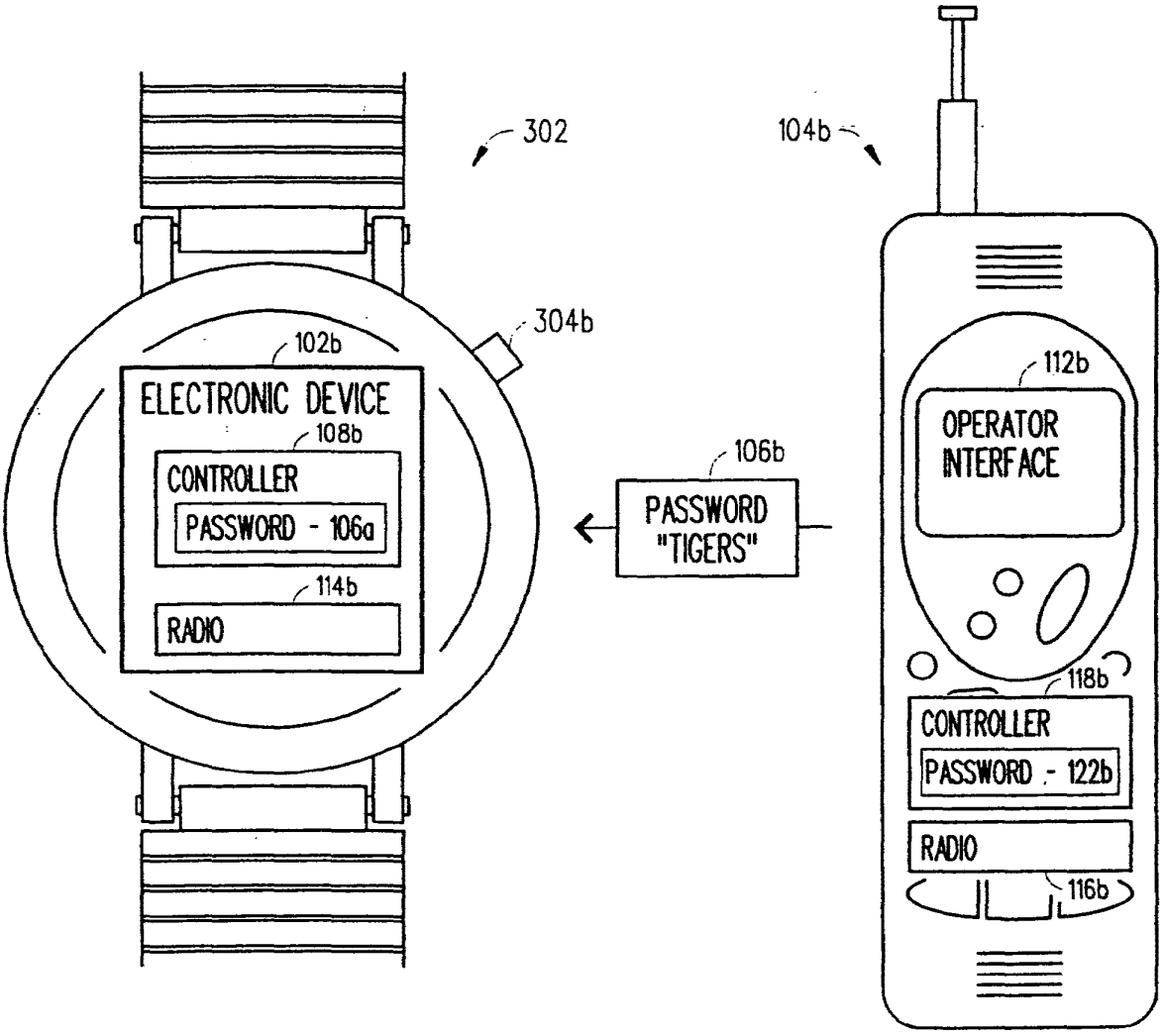


FIG. 3A

IPR2025-00645 Page 00162

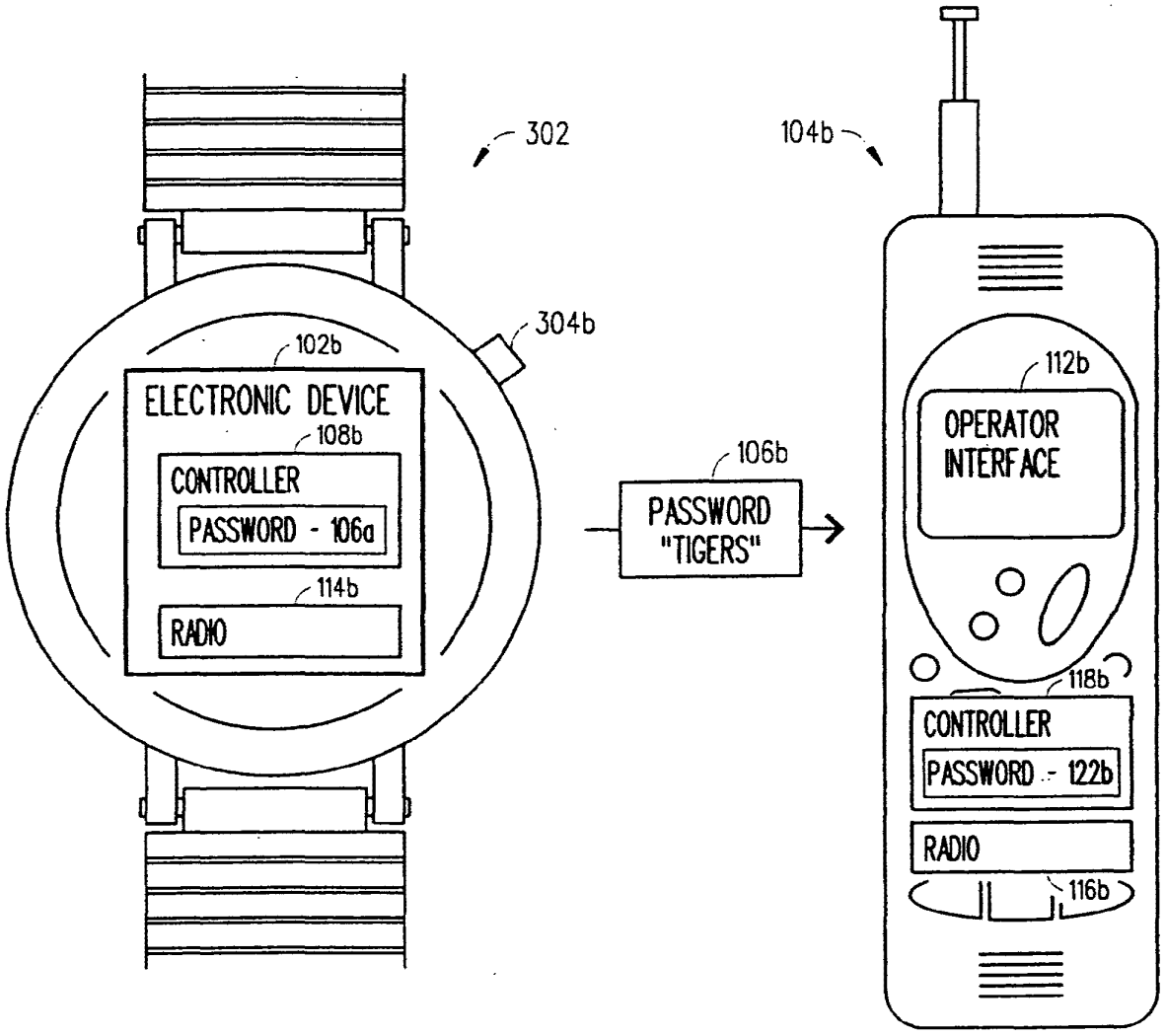


FIG. 3B

IPR2025-00645 Page 00163

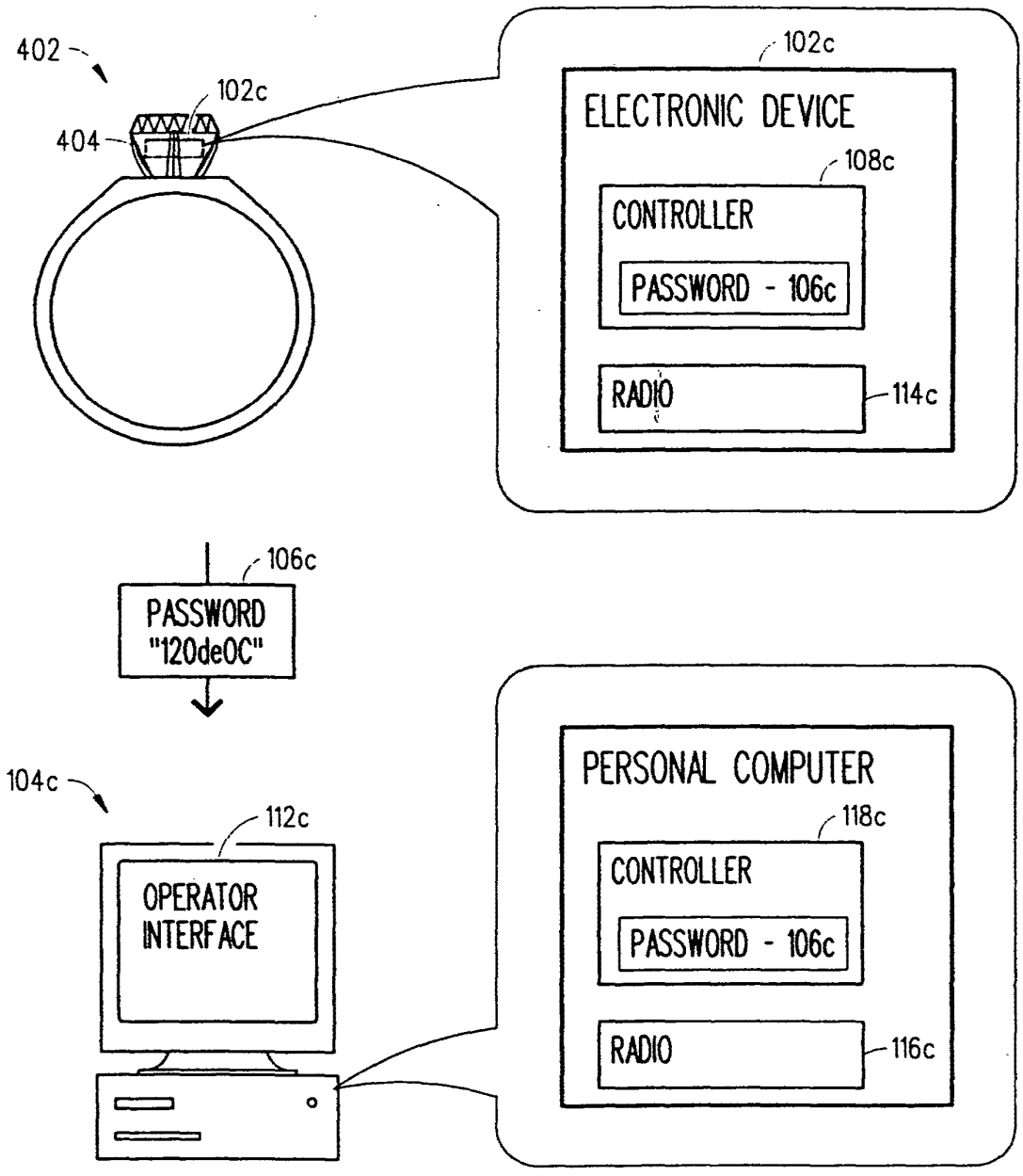


FIG. 4

IPR2025-00645 Page 00164

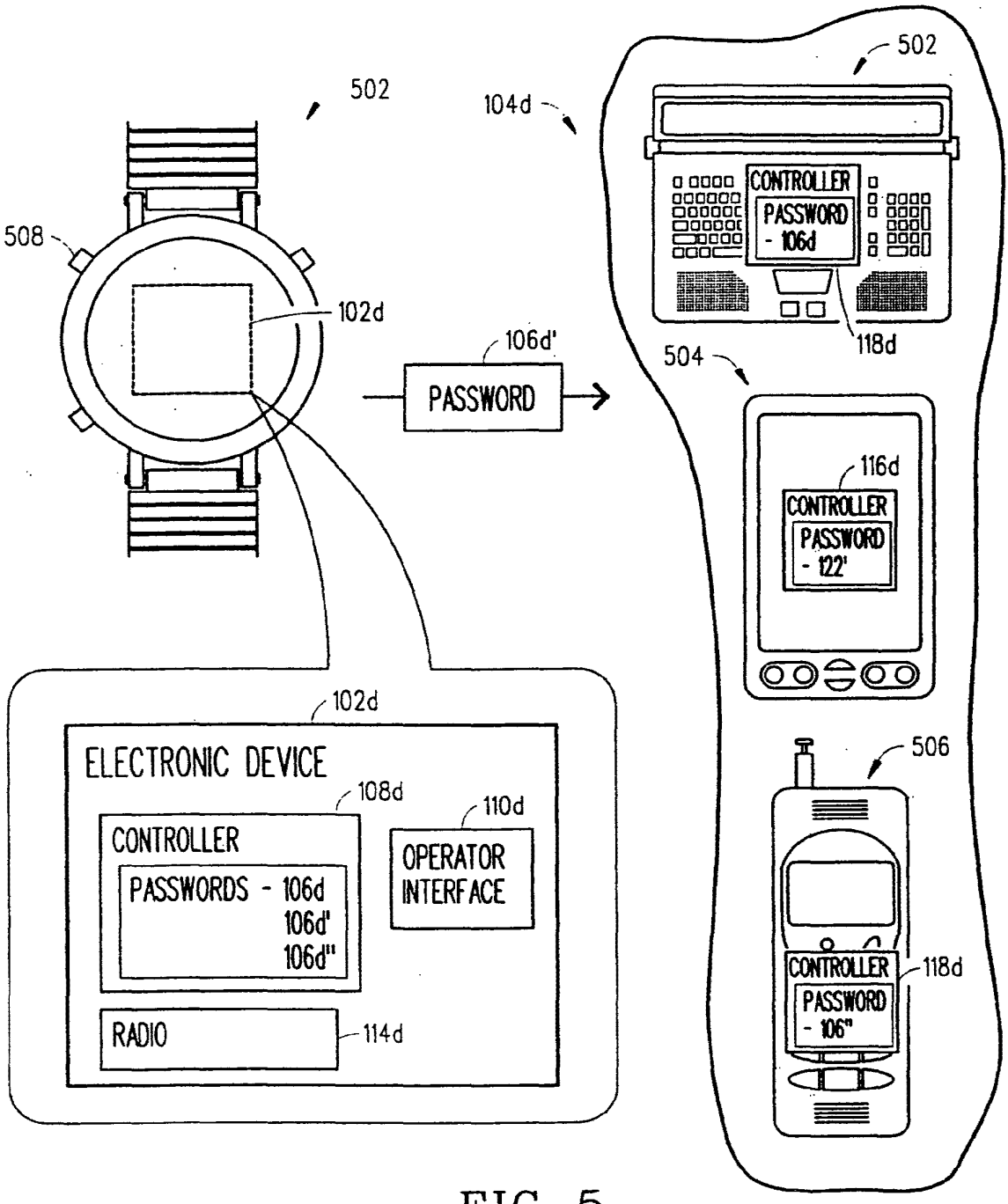


FIG. 5

IPR2025-00645 Page 00165

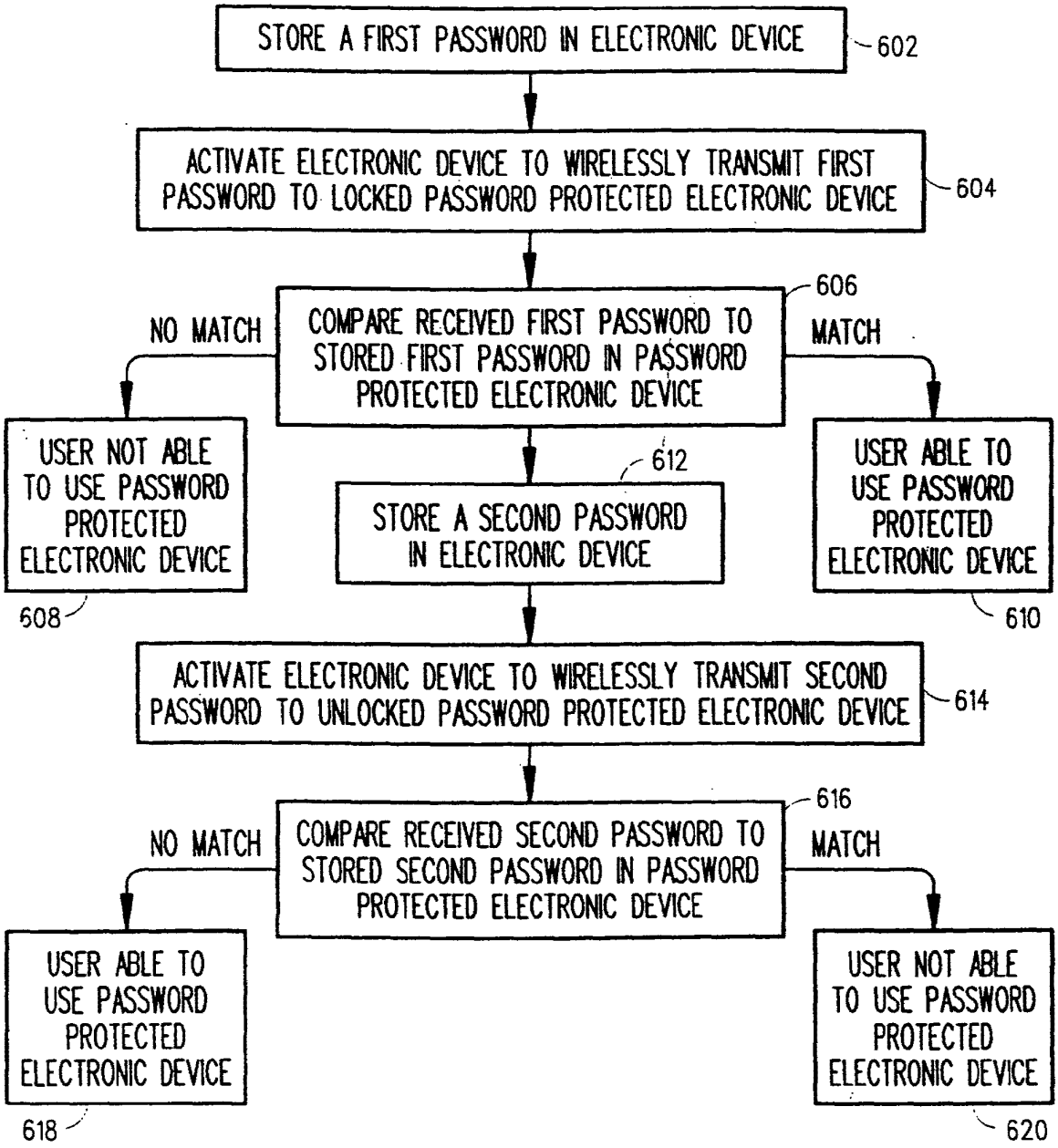


FIG. 6

IPR2025-00645 Page 00166

(12) UK Patent Application (19) GB (11) 2 316 908 (13) A

(43) Date of A Publication 11.03.1998

(21) Application No 9618647.3

(22) Date of Filing 06.09.1996

(71) Applicant(s)
John Cowling
2 De Burgh Park, BANSTEAD VILLAGE, Surrey, SM7 2PP, United Kingdom

(72) Inventor(s)
John Cowling

(74) Agent and/or Address for Service
Haseltine Lake & Co
Imperial House, 15-19 Kingsway, LONDON, WC2B 6UD, United Kingdom

(51) INT CL[6]
G06K 19/07 , G07C 9/00

(52) UK CL (Edition P)
B6A AC91 AK
U1S S2271

(56) Documents Cited
GB 2173970 A EP 0638880 A1 FR 002606188 A
NL 009200876 A US 5432864 A US 5386103 A
US 5321751 A

(58) Field of Search
UK CL (Edition O) B6A AK
INT CL[6] G07C 9/00
Online databases: WPI

(54) **Memory card with digitally encoded image of user**

(57) The card 10, eg a credit card, comprises a film mounted ROM 12 containing a non-erasable digitally encoded image of the card user. When the card is inserted into a card reader, the digital image is read, and transferred to a screen which displays the image of the user so that the identity of the user can be verified by the cashier before the transaction is authorised. The ROM 12 may contain other information relating to the user which is also displayed on the screen when the card is swiped. A second ROM 14 holds variable information. The card may also include a magnetic stripe 16.

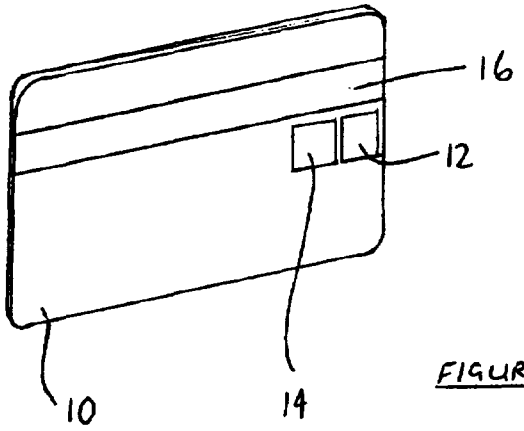


FIGURE 1

GB 2 316 908 A

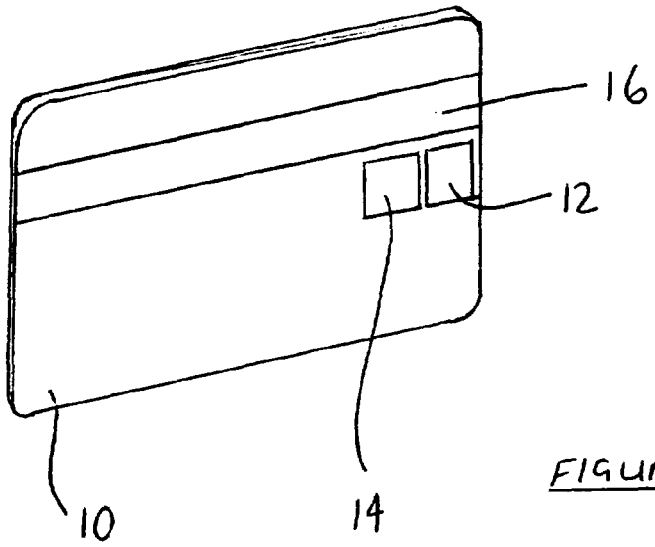


FIGURE 1

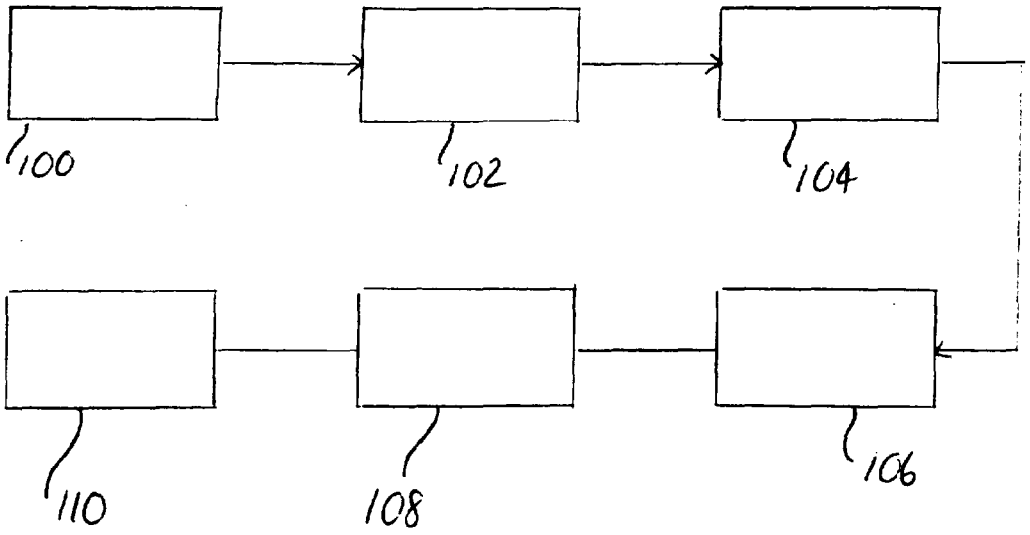


FIGURE 2

2316908

Card Security

This invention relates to credit cards and the like, and more particularly to a security arrangement for plastic cards, such as credit cards and the like, which is intended to prevent fraud and other misuse of such cards from occurring.

The use of credit cards and other types of payment cards is becoming more and more widespread in the U.K. and worldwide. Unfortunately, with this increased an increased level of fraud has also occurred, with frequent use of stolen and counterfeit cards resulting in losses of £100 - £165 million every year.

In some European countries, such as France, some credit cards and payment cards include a photograph of the authorised user of the card on one surface, usually the front, of the card. Thus, when the card is presented for payment, the cashier can compare the user shown in the photograph with the customer in order to verfy that he or she is an authorised user. However, such cards are not secure enough, and it has been found that it is possible to produce counterfeit credit cards and payment cards having fraudulent photographs on the front.

In view of the fact that 4 billion plastic card transactions are forecast in the year 2000, a completely 'instant' and totally secure method of card protection is necessary if increased losses due to fraud are to be avoided.

Thus, in accordance with a first aspect of the present invention, there is provided a card comprising memory means containing a digitally encoded image of an authorised user of the card.

In accordance with a second aspect of the present invention, there is provided apparatus for reading a card comprising memory means containing a digitally encoded image of an authorised user of the card, the apparatus comprising a digital reader unit for reading the digitally encoded image from the memory, and a display means for displaying the image of the authorised user.

Thus, when a card, for example a credit card, according to the first aspect of the present invention is presented for payment, the cashier inserts the card into the apparatus according to the second aspect of the present invention. The digital reader unit reads the digitally encoded image information. The information is then decoded and the image of an authorised user of the credit card is displayed on the screen. Fraudulent use is thus prevented.

The memory means may also include other information relating to the authorised user, for example, birth date, address, mother's maiden name, etc. for additional security checks.

The memory means preferably comprises a 2 Mb flash ROM which is mounted on a film before being embodied within the card. The card of the present invention preferably comprises a second memory means, for example a 1 Mb flash ROM, for storing variable data, such as transactions, account balances, credit limits, etc. The card may also include a magnetic stripe in order to ensure compatibility with reader systems not equipped with means for reading ROMs. A user's identify photograph is transferred onto the 2 Mb flash ROM (already mounted on the card). Therefore, the image is totally secure and non-visible.

The digitally encoded image stored in the memory means preferably includes a digital watermark for added security.

Also according to the present invention there is provided with a method of manufacturing a card, comprising the steps of producing a digitally encoded image of

an authorised user of the card, storing said digitally encoded image in memory means, and mounting said memory means on a card.

The memory is preferably a 2 Mb flash ROM which is mounted on a film before being mounted on the card. The method of manufacture may include further steps of storing variable data in second memory means, for example a 1Mb flash ROM, and mounting the second memory means on the card.

The card may be a credit card, any other type of payment card, an identification card, a railway season ticket or photocard, a passport, etc.

An embodiment of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which:

Figure 1 is a perspective rear view of a credit card according to an embodiment of the present invention; and

Figure 2 is a schematic flow diagram showing the steps involved in manufacturing a card according to one embodiment of the present invention.

A credit card according to one embodiment of the present invention is shown in Figure 1 of the drawings. The rear surface of the card 10 is provided with a first, non-erasable flash Read Only Memory (ROM) 12 and a second flash ROM 14. The first ROM 12 consists of a 2 Mb non-erasable microchip which has been mounted on a film, before being embodied within the credit card. The second ROM 14 consists of a 1Mb microchip.

The first ROM 12 contains a compressed digitally encoded image of the authorised user of the card. The ROM may also hold other information about the authorised user, for example, name, date-of-birth, mother's maiden name (for security purposes) etc. so as

to further ensure total security of the card, and prevent fraud. None of the information contained on the first flash ROM 12 can be changed or erased.

The second flash ROM 14 holds variable data such as, for example, transactions, account balance, credit limit, and similar. The card may also include a conventional magnetic strip 16 for compatibility with existing card reading systems.

In use, when the card is presented for payment, it is inserted into a card reader (not shown). The reader reads the digital information held in the first ROM 12, decompresses and decodes it, and then displays the image of the authorised user on an LCD screen together with any other information about the authorised user which is held on the ROM. The cashier can verify that the user is in fact the authorised user by comparing the user with the image displayed on the screen. If there is any doubt, the cashier may ask the user for further verification of the user's identity, for example, his mother's maiden name.

Referring to the flow diagram shown in Figure 2 of the drawings, a convenient method of manufacture of the credit card shown in Figure 1 will now be described. Firstly, at step 100, a photograph of the authorised user is taken using a QV-based imaging system. The image of the authorised user is composed on a QV type screen, and other personal details such as birth date, name, address, account, card number, expiration date, etc. can be entered. To make duplication even more difficult, the backdrop of the photo booth in which the photograph is taken may include details of the issuing branch of the card, the sort code, the address, or other unique information relating to the issuing body of the card.

At step 102, the image is compressed to a cam file, having a compression ration of 10:1, and a digital watermark is added which prevents duplication or forging of the image. Personal details can be added at this stage, as shown in step 104, via an on-line communications link, a local PC or direct connect keyboard into the QV card system. In other words, data relating to personal details of the authorised user can be transferred

to the cam file via a keyboard connected directly to the QV card system. Alternatively, the data can be entered on a personal computer and then transferred to the QV card system. If an account already exists for any particular authorised user, the data can be transferred from the main computer to the QV card system via a network or modem.

Text details are added to the cam file at step 106, the details being encrypted using a unique seed code. The encryption seed code may be based upon the authorised user's Personal Identity Number (PIN) or other personal number, such as date-of-birth.

At step 108, all of the information held in the cam file is loaded onto a non-erasable 2 Mb ROM which has been film mounted and embodied within a plastic strip. Thus, once the information has been loaded from the cam file onto the ROM, it cannot be changed or rewritten. A second flash ROM (1 Mb), containing variable data such as transactions, account balance, credit limit, and so on, is also mounted on the card.

Finally, at step 110, text is written to the front surface of the card, giving the card number, name of the authorised user, and other relevant information, as on a conventional credit card. The card surface is usually laminated and hologram protected. It may also be necessary to include a conventional magnetic stripe on some cards in order to ensure compatibility of the cards with reader systems not equipped with a QV card reader.

Cards according to the present invention are not limited to credit cards or payment cards. In fact, there are a number of different types of cards in which such security arrangements are desirable, for example, railway season tickets , identification cards, passports, and so on.

Furthermore, in the light of this disclosure, modifications of the described embodiment, as well as other embodiments, all within the scope of the present invention as defined by the appended claims, will now be apparent to persons skilled in the art.

CLAIMS:

1. A card comprising memory means containing a digitally encoded image of an authorised user of the card.

2. A card according to claim 1, wherein the memory means further contains personal data relating to the authorised user of the card.

3. A card according to any preceding claim, wherein the memory comprises a flash ROM.

4. A card according to claim 3, wherein the memory comprises a 2 Mb flash ROM.

5. A card according to any preceding claim, wherein the card further comprises a second memory means containing variable data.

6. A card according to claim 5, wherein the second memory means comprises a flash ROM.

7. A card according to claim 6, wherein the second memory means comprises a 1 Mb flash ROM.

8. A card according to any preceding claim, wherein the or each memory means is mounted on the rear surface of the card.

9. A card according to any preceding claim, comprising a magnetic strip.

10. A card according to any preceding claim, wherein the digitally encoded image of the authorised user includes a digital watermark.

11. A card according to any preceding claim, wherein the card is a payment card.

12. A card according to any of claims 1 to 10, wherein the card is a credit card.

13. A card according to any of claims 1 to 10, wherein the card is an identification card or passport.

14. A card according to any of claims 1 to 10, wherein the card is a railway season ticket.

15. A card substantially as herein described with reference to the accompanying drawings.

16. A method of manufacturing a card, comprising the steps of producing a digitally encoded image of an authorised user of the card, storing the digitally encoded image in memory means, and mounting said memory means on a card.

17. A method according to claim 16, wherein the digitally encoded image is compressed to a cam file prior to storage thereof in the memory means.

18. A method according to claim 17, wherein the compression ration is 10:1.

19. A method according to any of claims 16 to 18, wherein a digital watermark is added to the digitally encoded image prior to storage thereof in the memory means.

20. A method according to any of claims 16 to 19, further comprising the step of storing personal details relating to an authorised user of the card in the memory means.

21. A method according to any of claims 16 to 20, further comprising the step of storing variable data in a second memory means and mounting the second memory means on the card.

22. A method of manufacturing a card substantially as herein described with reference to the accompanying drawings.

23. Apparatus for reading a card comprising memory means containing a digitally encoded image of an authorised user of the card, the apparatus comprising a digital reader for reading the digitally encoded image from the memory means, and display means for displaying the image of the authorised user.

The Patent Office

9

Application No: GB 9618647.3 **Examiner:** Graham Russell
Claims searched: 1-23 **Date of search:** 29 October 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): B6A (AK)

Int Cl (Ed.6): G07C 9/00

Other: Online: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2173970 A	(MATSUSHITA) see page 2 lines 25-30	1,16,23 (at least)
X	EP 638880 A1	(DIGITAL IMAGING) see page 4 lines 31-37	1,16,23 (at least)
X	FR 2606188 A	(CORNILLE) see WPI abstract Acc No: 88-169640/25	1,16,23 (at least)
X	NL 9200876 A	(FACIES) see WPI abstract Acc No: 94-014084/02	1,16,23 (at least)
X	US 5432864	(DAOZHENG) see column 1 lines 24-27 & column 10 lines 27-40	1,16,23 (at least)
X	US 5386103	(NEURNETICS) see whole document	1,16,23 (at least)
X	US 5321751	(KODAK) see column 2 lines 26-35	1,16,23 (at least)

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-010668
(43)Date of publication of application : 14.01.2000

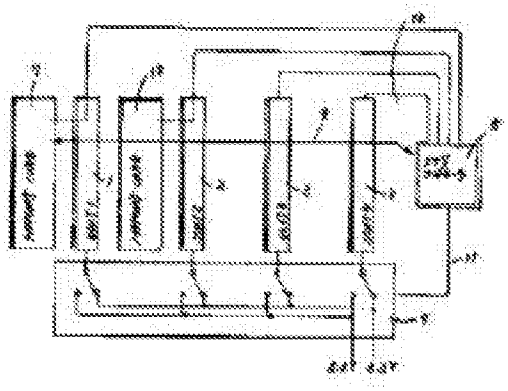
(51)Int.Cl. G06F 1/26
G06K 17/00

(21)Application number : 10-170770
(22)Date of filing : 18.06.1998

(71)Applicant : HITACHI LTD
HITACHI INFORMATION TECHNOLOGY CO LTD
(72)Inventor : FUNATSU JUNICHI

(54) MEMORY CARD SUPPLY VOLTAGE CONTROL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a memory card power supply voltage control system realizing control even when plural memory cards whose power supply voltages are different are loaded on arbitrary slots.
SOLUTION: 3.3 V is normally supplied from a power supply voltage variably setting part 9 to memory slots 1-4. When a memory card 7 is loaded on the memory slot, memory test of the memory card is operated. When the operating power supply voltage of the memory card 7 is 3.3 V, the test is normally ended, and the present power supply voltage is maintained. When the operating power supply voltage of the memory card 7 is 5 V, an error is generated, and the test is not normally ended. In this case, this system judges that a power supply voltage to be supplied is different, the power supply voltage setting part 9 switches the power supply voltage to be supplied to the memory slot 1 from 3.3 V to 5 V. After the switching, the test is operated again, and when still the test is not normally ended, it is judged that a DRAM is defective, and an error is produced. This operation is executed for each slot unit, and the co-existing loading of the memory cards with different kinds of power supply voltages can be attained.



(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2000－10668
（P2000－10668A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/26		Ｃ０６Ｆ　1/00	３３０Ｅ	５Ｂ０１１
Ｇ０６Ｋ　17/00		Ｃ０６Ｋ　17/00	Ｂ	５Ｂ０５８
		Ｇ０６Ｆ　1/00	３３０Ｆ	

審査請求　未請求　請求項の数５　ＯＬ　（全　７　頁）

(21)出願番号　特願平10－170770

(22)出願日　平成10年６月18日(1998.6.18)

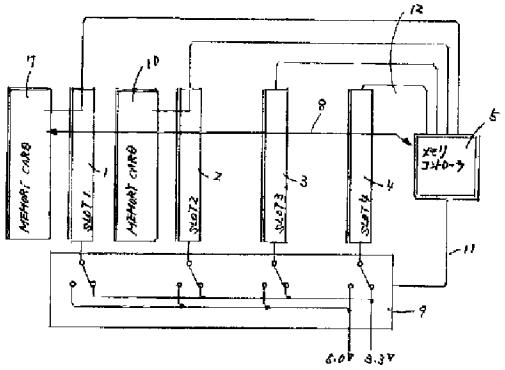
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000153454
株式会社日立インフォメーションテクノロジー
神奈川県足柄上郡中井町境456番地
(72)発明者　船津　淳一
神奈川県秦野市堀山下１番地　株式会社日立インフォメーションテクノロジー内
(74)代理人　100068504
弁理士　小川　勝男

Ｆターム(参考)　5B011 EA06 GG17 LL02
5B058 CA13 CA22 KA28 YA20

(54)【発明の名称】　メモリカード供給電圧制御方式

(57)【要約】
【課題】メモリカードを搭載する情報処理装置において、メモリカードの電源電圧が、その装置仕様で決められた単一のものであり、この電源電圧と異なるメモリカードの搭載では動作できなかった。
【解決手段】メモリスロット１から４には、電源電圧可変設定部９から通常３．３Ｖが供給される。メモリカード７がメモリスロット６に搭載されているため、このメモリカードに対してメモリテストを実施する。もし、７の動作電源電圧が３．３Ｖであれば、テストは正常終了するため、現電源電圧を維持する。７の動作電源電圧が５Ｖであれば、エラーとなり正常終了せず、システムは供給する電源電圧が異なっていると判断し、９は　1に供給する電源電圧を３．３Ｖから５Ｖに切り替える。切り替え後、再度テストを実施し、これでも正常終了しない場合には、ＤＲＡＭの不良と判断しエラーとする。以上の動作をスロット単位に実施し、異種電源電圧メモリカードの混在搭載を可能にする。

図1



【特許請求の範囲】
【請求項１】メモリカードを搭載する情報処理機器において、異種電圧で動作するメモリカードを混在して搭載した場合でも、初期テスト時に実施するメモリテストの合否によって自動的に各メモリカードの動作電源電圧を認識する手段と、上記認識結果から、各スロット毎に供給する第１の電源電圧と第２の電源電圧のうち、その当該スロットに搭載されたメモリカードが動作するために適した電源電圧に自動的に設定できる電源電圧変更手段を有することを特徴とするメモリカード電源電圧制御方式。
【請求項２】請求項１に関し、装置電源投入時におこなう初めのメモリテスト時にメモリカードに供給する電源電圧を第１及び第２の電源電圧のうち、低電圧である第１の電源電圧とすることを特徴とし、メモリテストにエラーがある場合に第２の電源電圧に変更するメモリカード電源電圧制御手段。
【請求項３】請求項１、２に関して、メモリテストの結果からエラーとなったアドレス数によって、電源電圧の相違かメモリカード自身のエラーかを判別する手段を有することを特徴とするメモリカード電源電圧制御手段。
【請求項４】請求項２に関し、メモリカードに装置電源投入時に供給する第１の電源電圧よりも低い電源電圧を持つ第３の電源電圧を有し、この第３の電源電圧を第１の電源電圧に変わり装置電源投入時にメモリカードに供給し、メモリテストをすることで、第１の電源電圧を動作電源電圧に持つメモリカードは正常動作するが、第２の電源電圧を動作電源電圧に持つメモリカードでは確実に動作できず、よりメモリカードの電源電圧の認識を効果的に実現することを特徴とするメモリカード電源電圧制御方式。
【請求項５】上記請求項のメモリカード電源電圧制御方式を実装することを特徴とする情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、パーソナルコンピュータやワークステーション等の情報処理機器において、メモリカードを搭載する構成を持つ場合のメモリカード電源電圧制御方式に関する。
【０００２】
【従来の技術】従来の技術では、ある情報処理装置でのメモリカードの動作電圧は、製品仕様として決定されていた。
【０００３】メモリカードを搭載する情報処理装置のＨ／Ｗとして、メモリカードに供給する電源電圧は、固定的で不可変的なものである。また、メモリカードにしても、そのカードに搭載されたＤＲＡＭ素子の動作電源電圧が、５Ｖ、３．３Ｖと決まっている。
【０００４】また、特開平０６－３３２５８０のようにメモリカードから出力される信号を感知し、そのメモリバスを制御するドライバの電源特性を変化させるものもある。
【０００５】
【発明が解決しようとする課題】かかる従来の方法には、次のような問題がある。
【０００６】もし異種電源電圧のメモリカードを混在させた場合、情報処理機器の仕様以外のメモリカードは動作しないというものである。これは、メモリカードを搭載するスロットが、そのＨ／Ｗとして供給される電源電圧が固定であることが原因である。
【０００７】例えば、情報処理機器仕様が５Ｖであるのに３．３Ｖのメモリカードを搭載した場合、メモリカードに搭載されたＤＲＡＭ素子の最大動作電源電圧以上に印可されてしまい、最悪ではＤＲＡＭ破壊に至る場合もある。これでは、パーソナルコンピュータ等を新しく購入した場合、以前所有していた装置とのメモリカードの動作電源電圧に相違があれば、そのメモリカードは、新しい装置への搭載は不可能になるという問題があった。
【０００８】例えば、特開平０６－３３２５８０もこの点を解決する発明である。しかし次の課題をもっている。特開平０６－３３２５８０は、メモリカードから出力される電源電圧情報信号を感知し、その信号によってメモリバスを制御するドライバの電源特性を変化させるものもあるが、この場合、メモリバスを制御するドライバの電源を変化させるために、メモリカードスロットに供給される電源電圧は一つの電位に決まり、電源電圧の異なる複数のメモリスロットを動作させることはできない。つまり、メモリバス上に複数のメモリカードを搭載する場合、搭載されたメモリカードすべてが同一の電源電位で動作する必要がある。搭載また、メモリカード自身に電源電圧情報信号を必要とすることで、バス以外の個別信号の増加につながり、搭載されるメモリカード数が多ければ、それも顕著となる。例えば、メモリカード個別に電源電圧の認識信号等を持つようにする場合、メモリカードのＳＩＭＭ、ＤＩＭＭ等のインタフェースが決まっている今日において、メモリカードの汎用性は無くなり、これも、違うインタフェースを持つ他の装置での動作ができなくなるという問題もある。
【０００９】このため、従来のメモリカードを搭載する場合の制御方法では、どのメモリカードスロットに、どの動作電源電圧を持つメモリカードが搭載されたかの認識及び、その電源電圧の自動的な設定が困難であった。
【００１０】本発明は、電源電圧が異なる複数のメモリカードを任意のスロットに搭載した場合であっても制御可能なメモリカード電源電圧制御方式の提供である。
【００１１】
【課題を解決するための手段】本発明では、メモリカードを搭載することで構成されるインタフェース制御回路において、このメモリバス上にメモリカードを搭載するスロットである各々のコネクタに対し、第１電源電圧と

第２電源電圧のうち一方を供給でき、また他方への切り替えができる電源電圧変換手段を有し、また、各々のコネクタにどの電源電圧動作するメモリカードが搭載されているかを判断し、その結果から、電源電圧変更手段に対して電源電圧の維持、または可変を指示する機能を有する制御手段を有す。また、この制御手段には、メモリバスコントローラとしての機能である、記憶データの読み出し、書き込み、ＥＣＣやパリティチェックといったエラー検出等の制御手段を持っても良い。

【００１２】本機能において、全てのメモリカードには第１電源電圧がデフォルトで供給され、初期テストにおいて、各々のスロットに対し、メモリカードの搭載可否を調査する。そして、メモリカードが搭載されているスロットに対し、個々にメモリテストを実施する。このテストでエラーになったスロットには、そのコネクタに供給する電圧を第１電源電圧から第２電源電圧に変更する。そして、再び各々のスロットに対して、メモリカードの搭載可否を確認することで、第２電源電圧で動作するメモリカードが搭載されたスロットでは、メモリカードの搭載を認識できることになる。これでも認識できないスロットでは、メモリカードが未搭載として判断する。この場合、メモリカードに搭載されたＤＲＡＭの破壊等を防止するためにも、第１電源電圧の方が第２電源電圧よりも低い電圧を持つようにすると良い。

【００１３】このように、メモリカードの電源電圧の認識を、そのスロットでメモリカードの搭載を認識できるかによって判断し、認識できないスロットに対してのみ、そのコネクタに供給する電源電圧を可変させることが可能になる。

【００１４】

【発明の実施の形態】以下に本発明の一実施例を詳細に説明する。

【００１５】図１は、本発明におけるメモリバス周辺のブロック図の一実施例である。本実施例は、メモリに対し、そのメモリインタフェースに対応したデータ読み出し及び書き込みを実施するメモリバスコントローラ５が、コネクタ６に搭載されたメモリカード７及び１０に対して、データの記憶または、記憶データの読み出しをメモリバス８を伝送路として行うものである。メモリバス８は、本実施例においては、信号レベルを３．３Ｖのインタフェース信号で伝送する。３．３Ｖインタフェースにおいては、信号のＨｉｇｈレベルが基本的には３．３Ｖであり、３．３Ｖの電源電圧で動作するメモリカードは、同一インタフェースであり問題はなく、また、５Ｖの電源電圧を持つメモリカードであってもＶｏｈの最小は２Ｖ程度であり、その信号を認識することは容易である。この場合、コネクタ１から４をメモリスロットと呼び、本図においては、メモリスロット１から４までの４個にて構成されている。また、メモリスロット１から４に対して、そのメモリスロットに搭載されたメモリカードが必要とする電源電圧を設定し供給する電源電圧可変供給部９を備えている。尚、本図においてメモリスロットは４個であるが、これはその装置任意であり、これ以上でも以下でも可能である。

【００１６】また、メモリインタフェースに関しても、ファーストページ、ＥＤＯ等のインタフェースを限定したものではない。

【００１７】この電源電圧可変供給部９について説明する。電源電圧可変供給部９は、各メモリスロット１から４に対し、スロットに搭載されたメモリカード７及び１０が必要とする電源電圧を個別に可変供給を可能にする。電源電圧可変供給部９は、本図において一例として３．３Ｖまたは５Ｖの電源電圧を規定している。現状、市販されているメモリカードの動作電源電圧はこの２種類が主であるが、本発明はこの電圧に限定したものではない。本実施例において、メモリスロット１から４には、３．３Ｖまたは５Ｖの電源電圧で動作するメモリカードが搭載される。電源電圧可変供給部９は、デフォルトで３．３Ｖの電源電圧を供給している。これは、デフォルトで５Ｖを供給すると、もし３．３Ｖの動作電源電圧を持つメモリカードが搭載された場合、動作電源電圧以上の高電位が印可され、最悪、メモリカードに搭載されたＤＲＡＭの素子破壊となる恐れがあるためである。つまり、電源電圧可変供給部９において、デフォルトは電源電圧可変供給部９で供給する複数の電圧のうち、最も電位の低いものを供給する。電源電圧可変供給部９の電源可変は、メモリコントローラ５の指示で行われる。信号１１は、このメモリコントローラ５から電源電圧可変供給部９に対する電源電圧可変制御信号である。つまり、電源電圧可変供給部９はこの信号１１に従い、内部ロジックにて、各スロット単位に電源電圧を３．３Ｖのまま維持するか、５Ｖに切り替えを実施するかのいずれかを行う。

【００１８】信号１２は、メモリスロット１から４にメモリカード搭載の有無を知らせる信号である。例えば、７２ピンＳＩＭＭのメモリーカードであれば、　Ｐｒｅｓｅｎｃｅ　Ｄｅｔｅｃｔ信号（ＰＤ０からＰＤ３）を用いる。ちなみに本信号は、そのメモリカード自信が、動作速度やメモリ容量を知らせる信号であり、４ｂｉｔのＨｉｇｈ、Ｌｏｗの組み合わせで設定されている。通常、システム側で本信号群は、プルアップされており、メモリカード側で認識に必要なｂｉｔがＧＮＤに接続され、他はフローティングである。メモリカードがメモリスロットに搭載されることで、この４ｂｉｔのうちメモリカードでＧＮＤに直結されたｂｉｔのみがＬｏｗレベルへと遷移し、他のｂｉｔはＨｉｇｈを維持する。メモリコントローラ５は、装置電源投入後に、信号１２の状態を監視する。この信号１２が認識できないメモリスロット、本図においては、スロット３及び４は、メモリカードが搭載されていないと判断する。メモリスロット１

及び２には、動作電源電圧はまだ不明であるが、メモリカード７及び１０が搭載されているため、信号１２は認識でき、メモリコントローラ５は、メモリカード７及び１０の存在とそのメモリカード７及び１０個々のメモリ容量を感知できる。信号１２は、メモリカード上のＤＲＡＭが動作電源電圧の違いで動作できなくとも、ＤＲＡＭとは関係のない部分で実施しているレベル固定処理のため、認識することは容易である。

【００１９】図２は、メモリカードの動作電源電圧を認識し、その電源電圧に可変するまでの制御の一実施例を示すフローチャート図である。図２と図１を用いて、本発明の動作を説明する。図２の最初のステータス１３では、各メモリスロットに供給する電源電圧を３．３Ｖに設定する。ステータス１４では、本動作に関係するパラメータをセットする。ｘは、メモリスロットの数である。図１においては、メモリスロット１から４と４つのスロットがあるため、初期値としてここでは、ｘ＝４とセットされる。また、ｙはメモリスロット番号である。図１では、メモリスロット１から４として存在している。初期値はｙ＝１である。この数値は、そのシステムによって適切な値をセットすれば良く、メモリスロットが６個あるシステムにおいては、ｘ＝６にセットすることになる。次のステータス１５において、各メモリスロットにメモリカードが搭載されているかを判定する。ｙの初期値がｙ＝１であるため、まずメモリスロット１からメモリカードの有無を調査する。図１において、メモリスロット１にはメモリカード７が搭載されているため、ステータス１５の分岐はＹＥＳとなる。次のステータス１６で、このメモリスロット１に搭載されたメモリカード７に対して、メモリテストを実施する。テスト内容は、メモリカードのメモリ容量が、図１の信号１２で既知であるため、全容量に対してデータの書き込み、読み出し、コンペアテストを行う。また、全容量のデータの書き込み、読み出し、コンペアテストでは、テスト時間がかかってしまうため、例えば３２ＭＢのメモリカードであるなら、最初の４ＭＢと最後の４ＭＢのデータの書き込み、読み出し、コンペアテストのみとすれば、テスト時間の短縮も可能である。ステータス１７では、このメモリテストの結果を正常終了かどうかで判定する。図１のメモリカード７が、３．３Ｖの動作電源電圧で動作する仕様のカードならば、ステータス１６のテストは、正常に終了するため、ＹＥＳに分岐することになる。その後、次のステータス１８では、セットしていたパラメータｘ、ｙの設定をシフトする。メモリスロット数を示すｘから１減算し、メモリスロット番号を示すｙに１加算することで、次のメモリスロットにテスト対象を移行する。メモリスロット１が終了したこの段階では、ｘ＝３、ｙ＝２とパラメータは変化する。ステータス１９では、ｘのパラメータを見ることで、全メモリスロットのテストは終了したかを判定している。ｘ＝０であれば全メモリスロットのテストが終了したことになる。前述した段階では、ｘ＝３のため、ステータス１９の分岐はＮＯであり、ステータス１５にジャンプすることになる。

【００２０】ｙ＝２であることから、次にメモリスロット２のテストである。図１のメモリスロット２にはメモリカード１０が搭載されているため、ステータス１５、１６、１７とメモリスロット１同様にステータスは進む。メモリカード１０が、５Ｖの動作電源電圧で動作する仕様のカードである場合、システムとして供給している電源電圧が３．３Ｖであるため、ステータス１７でのメモリテスト判定は、正常終了せず、ＮＯに分岐する。ＮＯ分岐後の次のステータス２０では、このメモリスロット２に供給する電源電圧を３．３Ｖから５Ｖに可変させる。図１において、メモリテストがＮＧであった結果が、ＣＰＵからメモリコントローラ５に通知され、メモリコントローラ５は電源電圧可変設定部９に対し、信号１１を用いて、メモリスロット２の電源電圧を変更するように通知する。これに従い、電源電圧可変設定部９は、メモリスロット２の電源電圧を５Ｖに切り替える。この切り替えが終了した後に、ステータス２１で再びメモリスロット２に対し、ステータス１６と同様の方法でメモリテストを実施する。そして、ステータス２２でそのテスト結果の判定を行う。メモリカード１０が、動作電源電圧５Ｖの仕様であるため、本メモリテストは正常終了し、判定はＹＥＳに分岐する。その場合、ステータス１８に戻り、パラメータｘ、ｙの更新となり、次のメモリスロットにテストは移行される。もし、ステータス２２で、メモリテストが正常終了しない場合、判定はＮＯに分岐する。この場合、システムが供給する電源電圧を３．３Ｖにしても５Ｖにしても、テスト結果はＮＧであるため、メモリカード自身に異常があると判定し、メモリエラーとして処理する。

【００２１】次はメモリスロット３のテストとなる。図１において、メモリスロット３にはメモリカードは搭載されていない。よって、ステータス１５での判定はＮＯであり、ステータス１８にジャンプする。続くメモリスロット４においても同様である。メモリスロット４が終了し、ステータス１８の処理を実行するとｘ＝０となる。よって、ステータス１９では判定がＹＥＳとなり、メモリカードの電源電圧自動認識、自動変換の制御は終了する。

【００２２】以上までに述べたように、本実施例では、メモリテストの結果を元にし、正常ならば現在の電源電圧が適正、異常であれば他の電源電圧に変更して再び確認といった手段によってメモリカードが動作するのに適した電源電圧を認識し、変更するものである。

【００２３】本実施例は、図２で示したフローチャートに限定するものではない。図３は、図２のステータス１７の判定部近傍を抜粋し、機能を追加したものである。

図２のステータス１７でＮＯに分岐した場合、図３ではもう一つの判定ステータス２４を実行する。ステータス２４では、メモリテストのエラー状態がテストした全アドレスか、またはそうでないかを判定する。もし動作電源電圧の違いでエラーになっている場合は、メモリカードに搭載されたＤＲＡＭがまったく動作していないはずである。つまり、テストする全アドレスにおいて、どのアドレスでもエラーになる。この場合、電源電圧を切り替えるため、ステータス２４ではＹＥＳに分岐し、図２のステータス２０以下と同じ処理を続ける。逆にテストしたアドレスの一部でのみエラーが発生した場合、ステータス２４ではＮＯに分岐することとなる。この場合、電源電圧の仕様が異なるメモリカードが搭載されているというよりはむしろ、そのメモリカード自身に異常があると判定し、ステータス２５にてメモリエラーと判断する。このように、ステータス２４を設けることで、３．３Ｖの電源電圧供給時においての、３．３Ｖ電源電圧を仕様とするメモリカードのメモリカード異常を見つけることが可能となる。図２の場合は、３．３Ｖの電源供給でテストＮＧなら、全て電源電圧を５Ｖに切り替えるため、本当は３．３Ｖ電源電圧仕様のメモリカード上の一個のＤＲＡＭが壊れていたとしても、図２のステータス１７でＮＯに分岐後、ステータス２０で電源電圧を５Ｖに切り替えることで、メモリカード上の全てのＤＲＡＭに過電圧がかかり、すべてのＤＲＡＭ破壊につながる。図３は、これを防止するためには、良い方法である。

【００２４】また、デフォルトで供給している電源電圧を本実施例において、３．３Ｖから第３の電源電圧である２．８Ｖ程度に変更しても良い。これは、５Ｖの電源電圧仕様のメモリカードが、３．３Ｖの電源電圧で、そのＤＲＡＭの実力で動作できる可能性を完全に絶つためには良い方法である。この方法では、２．８Ｖでテストののちに、３．３Ｖや５Ｖに切り替えを実施することになる。

【００２５】尚、一度設定した各メモリスロットの電源電圧は、そのメモリカードの構成が変更にならない限り、それを初期状態として供給するようにしても良い。こうすれば、構成が変更にならない限り、メモリテストが各メモリカード共、供給電源電圧の違いで失敗することはなく、テスト時間をより短縮するには有効な手段である。

【００２６】

【発明の効果】本発明はメモリカードが搭載されるメモリスロットに対し、そのメモリカードが動作するに適した電源電圧に各メモリスロット単位で個々に自動的に設定する。したがって、電源電圧の異なるメモリカードを混在させての搭載を可能にし、メモリカードの電源電圧によらない汎用性のある制御手段を実現している。電源電圧の認識方法としても、メモリテストという通常のシステム立ち上げ時に一般的に実施しているものを利用しており、簡便な構成が実現できる。

【００２７】また、電源電圧仕様が異なったためだけに使用できなかったメモリカードも、本発明により、スロットの電源キーが共通化されることで使用可能になり、リサイクルの観点からも効果的なものである。

【図面の簡単な説明】

【図１】本発明に係るメモリカード電源電圧自動変換方式が適用されたメモリバス周辺の一実施例を示したブロック図。

【図２】本発明に係るメモリカードの電源電圧を自動的に認識する手段の一実施例を示したフローチャート図。

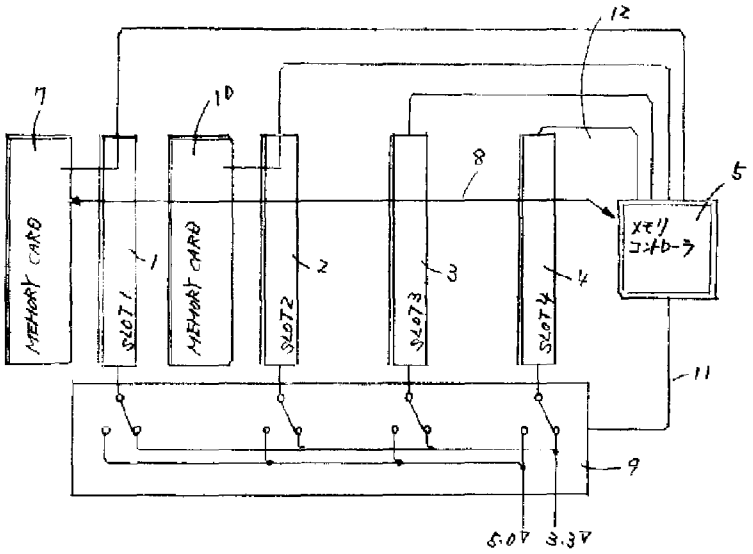
【図３】本発明に係る一実施例である図２に対し、機能を追加した他の実施例を示したフローチャート図の部分的抜粋。

【符号の説明】

１，２，３，４・・・メモリスロット
５・・・メモリコントローラ
６・・・コネクタ
７・・・３．３Ｖの電源電圧仕様のメモリカード
８・・・メモリバス
９・・・電源電圧可変供給部
１０・・・５Ｖの電源電圧仕様のメモリカード
１１・・・電源電圧可変制御信号
１２・・・メモリカードのメモリ容量、動作速度認識信号
１３・・・メモリカードに３．３Ｖを供給するステータス
１４・・・パラメータセットステータス
１５・・・メモリカード搭載確認ステータス
１６・・・電源電圧３．３Ｖでのメモリテストステータス
１７・・・メモリテスト結果判定ステータス
１８・・・パラメータ更新ステータス
１９・・・テスト終了判定ステータス
２０・・・メモリカードに５Ｖを供給するステータス
２１・・・電源電圧５Ｖでのメモリテストステータス
２２・・・メモリテスト結果判定ステータス
２３・・・メモリエラーステータス
２４・・・エラー内容判定ステータス
２５・・・メモリエラーステータス

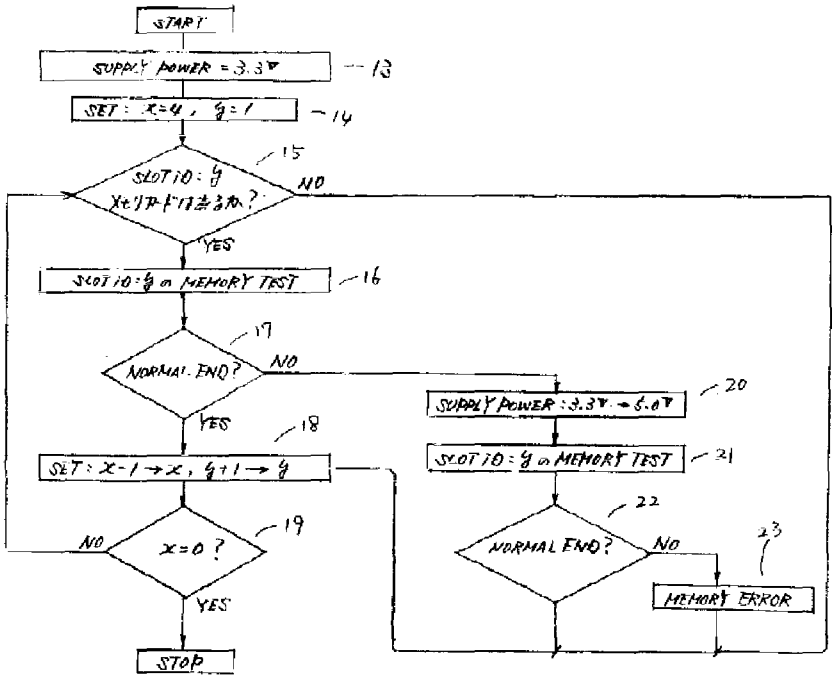
【図1】

図1


MEMORY CARD
SLOT 1
MEMORY CARD
SLOT 2
SLOT 3
SLOT 4
メモリコントローラ
5.0V
3.3V

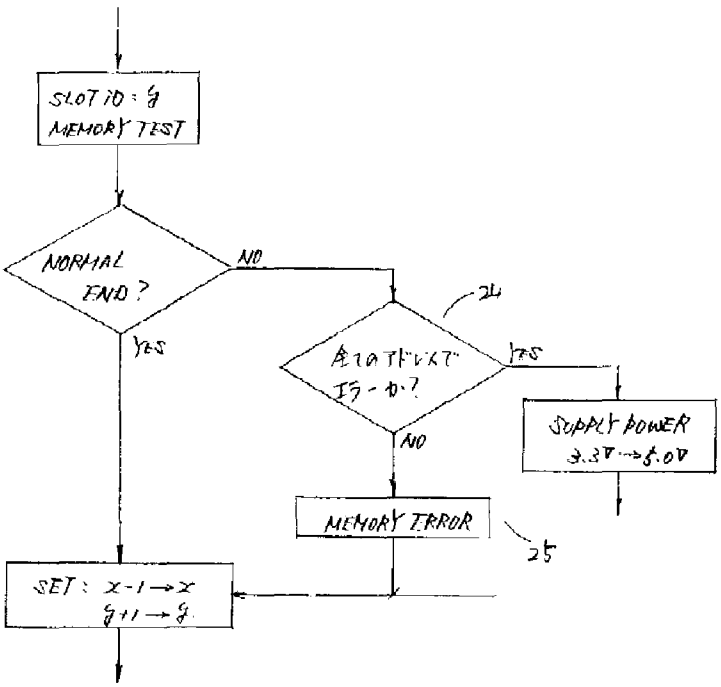
【図2】

図2


START
SUPPLY POWER = 3.3V
SET : x=4, y=1
SLOT iO : y メモリカードは差されたか?
NO
YES
SLOT iO : y の MEMORY TEST
NORMAL END?
NO
YES
SET : x-1→x, y+1→y
x=0 ?
NO
YES
STOP
SUPPLY POWER : 3.3V → 5.0V
SLOT iO : y の MEMORY TEST
NORMAL END?
NO
MEMORY ERROR

【図3】

図3


SLOT ID = y
MEMORY TEST
NORMAL END ?
NO
YES
24
全てのアドレスで エラー か ?
YES
NO
SUPPLY POWER 3.3V → 5.0V
MEMORY ERROR
25
SET : x-1 → x
y+1 → y

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-018671
(43)Date of publication of application : 20.01.2005

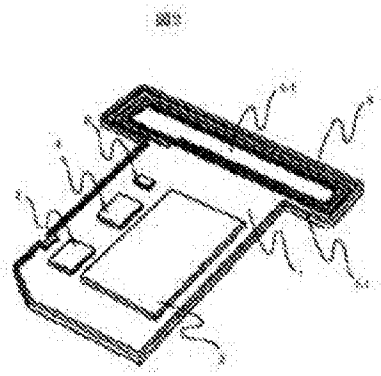
(51)Int.Cl. G06K 19/077
G06K 19/07
H01Q 1/24
H01Q 7/04
H04B 5/02
H04M 1/02

(21)Application number : 2003-186101
(22)Date of filing : 30.06.2003

(71)Applicant : HITACHI LTD
(72)Inventor : OKAWA TAKEHIRO
YOSHIKI HIROSHI
KUWANA TOSHIYUKI
SATO YUTAKA

(54) MEMORY CARD AND CELLULAR PHONE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a productive memory card with RFID function capable of ensuring a communication distance without impairing portability.
SOLUTION: The arrangement position of an antenna coil 5 is set to the outside of portable information equipment to extend the communication distance of an RFID to be integrated. A resonance capacitor is connected to both ends of the antenna coil.



(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2005-18671
(P2005-18671A)
(43)公開日　平成17年1月20日(2005.1.20)

(51)Int.Cl.[7]		F I			テーマコード（参考）
G06K	19/077	G06K	19/00	K	5B035
G06K	19/07	H01Q	1/24	C	5J047
H01Q	1/24	H01Q	7/04		5K012
H01Q	7/04	H04B	5/02		5K023
H04B	5/02	H04M	1/02	C	

審査請求 未請求　請求項の数 8　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願2003-186101(P2003-186101)
(22)出願日　平成15年6月30日(2003.6.30)

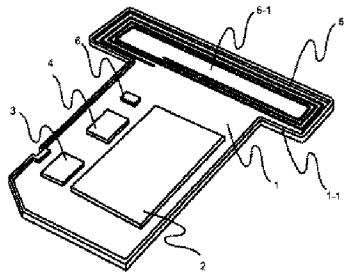
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　大川　武宏
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
(72)発明者　吉木　宏
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
(72)発明者　桑名　利幸
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所情報・通信グループ内

最終頁に続く

(54)【発明の名称】メモリカード及び携帯電話

(57)【要約】
【課題】生産性が良く、かつ、携帯性を損なうことなく通信距離を確保したＲＦＩＤ機能を搭載するメモリカードを提供する。
【解決手段】アンテナコイル５の設置場所を携帯情報機器の外側にして、組み込むＲＦＩＤの通信距離を伸ばす。アンテナコイルの両端に共振用コンデンサを接続する。
【選択図】　図２

図2



【特許請求の範囲】
【請求項1】
携帯情報機器に挿入されるメモリカードであって、
外部機器とデータ通信を行うアンテナコイルを有し、
前記携帯情報機器の前記メモリカードの挿入口の外側に前記ＲＦＩＤのアンテナコイルが配置される構造となっていることを特徴とするメモリカード。
【請求項2】
請求項１に記載のメモリカードに於いて、前記アンテナコイルがメモリカード本体と水平に配置されたことを特徴とするメモリカード。
【請求項3】
請求項１に記載のメモリカードに於いて、前記アンテナコイルがメモリカード本体と垂直に配置されたことを特徴とするメモリカード。
【請求項4】
請求項１に記載のメモリカードに於いて、前記アンテナコイルがメモリカード本体と可歪な導体で接続され、前記メモリカードが装着される携帯情報機器の外側に装着される構造であることを特徴とするメモリカード。
【請求項5】
請求項２～４のいずれかに記載のメモリカードにおいて、アンテナコイルに透磁率が１０以上で厚みが０．１ｍｍ以上、１ｍｍ以下の磁性体シートが重ね合わさっていることを特徴とするメモリカード。
【請求項6】
請求項４に記載のメモリカードにおいて、アンテナコイルとの逆側にクッション材を具備することを特徴とするメモリカード。
【請求項7】
請求項１～６のいずれかに記載のメモリカードにおいて、前記ＩＣが接触・非接触両用のＩＣであることを特徴とするメモリカード。
【請求項8】
アンテナと、
挿入口に挿入されるメモリカードと、
表示部とを有し、
上記メモリーカードは、外部機器とデータ通信を行うアンテナコイルと記憶部を有し、該記憶部は上記アンテナと上記アンテナコイルを介して受信したデータを格納し、
前記ＲＦＩＤのアンテナコイルは前記挿入口の外側に配置されることを特徴とする携帯電話。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はメモリカードに係り、特に外部機器と電磁界信号を介して通信するＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）を搭載したメモリカードに関する。
【０００２】
【従来の技術】
外部機器から放射される所定の周波数の電磁界を信号搬送波として使用し、外部機器との間でＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）情報及び各種データの通信を行う自動認識認識技術の一つであるＲＦＩＤを搭載した例としては、ＩＣテレホンカード、電子乗車券などのいわゆる非接触ＩＣカードがある。
【０００３】
非接触ＩＣカードの通信特性を向上させる技術としては、下記特許文献１－２にしめすようなものがある。
【０００４】

特許文献１は、アンテナコイルとその両端に接続される容量で構成される共振回路の中間タップ点（インピーダンスによっては共振回路の外側にも位置しうる）における出力インピーダンスとＬＳＩの入力インピーダンスとの整合をとる回路を開示する。

【０００５】

また、特許文献２は、通信距離を伸ばすために、外部機器からの信号搬送波の周波数に、ＲＦＩＤの受信回路の共振周波数を合わせることが行われている。例えば、非接触型ＩＣカードのＲＦＩＤでは、印刷パターンで形成した共振用微小コンデンサ列の使用数をＲＦＩＤ単体ごとにトリミングすることを開示する（特許文献２参照）。

【０００６】

【特許文献１】特開２０００－２７８１７２号公報

【特許文献２】特開平１１－３５３４４０号公報

【発明が解決しようとする課題】

近年、携帯電話機の普及は目覚しいものがあり、日常的に携帯電話機を携帯することが一般的となっている。

【０００７】

さらに携帯電話機の高機能化も進み、内蔵カメラ、音楽プレーヤーを搭載する携帯電話機も一般的となっており、それに伴い画像、音楽情報を着脱可能な記憶用のメモリカードを携帯電話機に搭載することも一般的となっている。また、携帯電話機へ音楽、着信メロディのダウンロード、路線検索、ＨＰへのアクセス、ネット決済等のデータのやり取りが可能なネットワーク接続機能を有した携帯電話機も一般的となっている。

【０００８】

また、電車等の料金チャージ機能、支払い機能を有した非接触ＩＣカード等のＲＦＩＤも一般的となっており、日本の都心において出かける際には非常に便利なものとなっている。

【０００９】

この携帯電話機にＲＦＩＤ機能を搭載することにより携帯性にすぐれる料金チャージ機能、支払い機能を有した携帯電話機とすることにより、更に利便性を高めることが可能となる。

【００１０】

この場合、携帯電話機の無線周波数と既存の非接触ＩＣカード等ＲＦＩＤが使用する無線周波数帯域は異なっているため、携帯電話機に既存のインフラとの互換性を持たせたままＲＦＩＤ機能を搭載するには、アンテナを２つ設けることが簡便である。

【００１１】

しかしながら、外部機器から放射される所定の周波数の電磁界を信号搬送波として使用するＲＦＩＤの機能を携帯電話機に搭載する場合、ＲＦＩＤに設けるアンテナコイルに必要な磁路上に携帯情報機器の回路基板上のシールドを兼ねたグランドパターンなど低インピーダンス閉回路が存在することを考慮する必要性と、電磁環境適合性（ＥＭＣ：Ｅｌｅｃｔｒｏ－Ｍａｇｎｅｔｉｃ　Ｃｏｍｐａｔｉｂｉｌｉｔｙ）対策のため携帯電話機の筐体に金属蒸着膜もしくは導電材塗装があることを考慮する必要があり、通信距離の確保のため磁路障害物影響の排除が要求される。

【００１２】

また、ＲＦＩＤの機能を携帯電話に搭載するには、携帯電話機の携帯性の面から大きさに制限があり、ＲＤＩＤのアンテナコイルの磁路開口面積を充分に大きくとれないこと等により、自由空間での通信に比べ通信距離が大幅に短くなるという問題がある。

【００１３】

しかしながら、前述した特許文献１及び２では、ＲＦＩＤが搭載される携帯端末（電話）自体が通信用アンテナを備えた電磁波の発信源として、他の電子機器に悪影響を及ぼさず、又、メモリカード等が外部ノイズにより障害を受けたりしないように筐体にＥＭＣ対策が施こされていることを考慮しておらず、従来技術をそのまま適用しても前記問題を解決することができない。

【００１４】
そこで、本発明の目的は携帯性を損なうことなく通信距離を確保したＲＦＩＤ機能を有する携帯電話機を提供することにある。
【００１５】
【課題を解決するための手段】
本願において開示される発明のうち、代表的なものの概要を説明すれば下記のとおりである。
【００１６】
本発明に係るメモリカードは、携帯情報機器に挿入されるメモリカードであって、外部機器とデータ通信を行うアンテナコイルを有し、前記携帯情報機器の前記メモリカードの挿入口の外側に前記ＲＦＩＤのアンテナコイルが配置される構造となっていることを特徴とする。
【００１７】
上記構成により、携帯性を損なうことなく通信距離を確保したＲＦＩＤを有する携帯電話機を提供することができる。
【００１８】
【発明の実施の形態】
以下、本発明に係るメモリカードの好適な実施形態につき、添付図面を参照しながら詳細に説明する。また、同一の符号を付したものは同様の機能を有するものとする。
【００１９】
なお、実施形態の説明において、基板と、この基板に印刷されるアンテナコイルと、前記アンテナコイルに接続される共振用コンデンサおよびＩＣとを組合わせたものを、“ＲＦＩＤ”と称する。
【００２０】
一般に、携帯電話機の筐体には、金属蒸着膜もしくは導電材塗装されている。そこで、上述のようにＲＦＩＤを携帯電話機に搭載する際に問題となる通信距離の確保のため磁路障害物影響の排除をするためには、携帯電話機の筐体に金属蒸着膜もしくは導電材塗装がない箇所にＲＦＩＤのアンテナを設置する必要性がある。
【００２１】
そこで本願では、ＲＦＩＤを携帯電話機のメモリカードに一体化させるとともに、ＲＦＩＤのアンテナコイル部を携帯電話機のメモリカード挿入部の外部に設けることにより、携帯性を損なうことなく通信距離を確保したＲＦＩＤを有する携帯電話機を提供することを実現した。
【００２２】
また、この構成とすることにより携帯電話機の携帯性の面から大きさに制限のあるアンテナコイルの磁路開口面積を充分に大きくとらずとも自由空間での通信距離を伸ばすことができる。
【００２３】
＜実施形態１＞
図１は本発明に係るメモリカードの第１の実施形態を示す図であり、従来のメモリカードを延長し前記メモリカードが携帯情報機器に実装された場合の携帯情報機器の外側に位置する部分にＲＦＩＤのアンテナコイルをメモリカードと水平に実装するアンテナコイル実装部１－１を装備したメモリカード１の概略外形図である。
【００２４】
図２は図１で示したメモリカード１の概略内部実装図である。
【００２５】
フラッシュメモリ２とコントローラ３でメモリカード本来の機能を持ち、フラッシュメモリ２は携帯情報機器からの接触結合による要求信号に応じコントローラ３によって制御されデータのライト・リードが行われる。
【００２６】

外部機器から放射される所定の周波数の磁束をアンテナコイル５を介して信号搬送波および電力として使用し、非接触結合で外部機器との間でＩＤ情報及び各種データの通信を行い、また、メモリを有するＩＣ４はアンテナコイル５に接続される。共振用コンデンサ６はアンテナコイル５に接続される。

【００２７】

ＩＣ４は、アンテナコイル５を介して外部機器との各種情報の通信を制御、情報の記憶を行う。なお、前記ＩＣ４が接触・非接触の両機能を有する場合は、携帯情報機器との接触結合による情報と外部機器との非接触結合による情報を共有することが出来る。図１、２で示した構成をとることにより、メモリカードとＲＦＩＤを同一基板状に構成することができ、安価にＲＦＩＤ搭載メモリカードを提供する。

【００２８】

また、メモリカード本体と水平に前記アンテナコイルを配置することで、メモリカード１搭載時における携帯情報機器の表裏にかかわらず、外部機器と通信可能であり、ＲＦＩＤの通信距離も確保することが出来る。

【００２９】

図３は図１で示したメモリカード１を携帯電話機７に適用した場合の概略実装図である。アンテナコイル部分が外部にでているために装着がしやすいという効果もある。

【００３０】

図４は図３で示したメモリカード１搭載の携帯電話機７を外部機器としての電子乗車券改札機８にかざしている図であり、携帯電話機７の下側に位置するアンテナコイル５を含むＲＦＩＤと電子乗車券改札機８との間で電磁界を使っての通信を行う。電子乗車券改札機８から発生しアンテナコイル５の開口部５－１を通過する磁束の大部分は自由空間でループを形成し、通信距離を確保することが出来る。

【００３１】

＜実施形態２＞

図５は本発明に係るメモリカードの第２の実施形態を示す図であり、従来のメモリカードを延長し前記メモリカードが携帯情報機器に実装された場合の携帯情報機器の外側に位置する部分にＲＦＩＤのアンテナコイルをメモリカードと垂直に実装するアンテナコイル実装部９－１を装備したメモリカード９の概略外形図である。

【００３２】

図６は図５で示したメモリカード９の概略内部実装図である。フラッシュメモリ２、コントローラ３、アンテナコイル５、ＩＣ４、共振用コンデンサ６の機能は図２の説明と同様である。

【００３３】

アンテナコイル５が印刷された基板５－２は磁性体シート１０を挟む形態でアンテナコイル実装部９－１に取り付けられる。

【００３４】

図５、６で示した構成をとることにより、実装される携帯情報機器からの突出を少なくしながら、外部機器からのアンテナコイル開口部５－１を通過した磁束は磁気抵抗の少ない磁性体シート１０を通過してループを形成することでＲＦＩＤの通信距離を確保することが出来る。

【００３５】

図７は図５で示したメモリカード９を携帯電話機７に適用した場合の概略実装図である。アンテナコイル実装部の突出が少ないため端末の携帯性を損なわないという効果がる。

【００３６】

図８は図７で示したメモリカード９搭載の携帯電話機７を外部機器としての電子乗車券改札機８にかざしている図であり、携帯電話機７の下側に位置するアンテナコイル５を含むＲＦＩＤと電子乗車券改札機８との間で電磁界を使っての通信を行う。電子乗車券改札機８から発生しアンテナコイル５の開口部５－１を通る磁束は、大部分が磁路抵抗の低い磁性体シート１０を通過することでループを形成し、通信距離を確保することが出来る。

【００３７】
＜実施形態３＞
図９は本発明に係るメモリカードの第３の実施形態を示す図であり、従来のメモリカードからフレキシブル基板１１－２を経由して前記メモリカードが携帯情報機器に実装された場合の携帯情報機器の外側に位置する部分にＲＦＩＤのアンテナコイルを貼り付けるためのアンテナコイル実装部１１－１を装備したメモリカード１１の概略外形図である。
【００３８】
図１０は図９で示したメモリカード１１のアンテナコイル実装部１１－１の概略構造図である。
基板５－２に印刷されたアンテナコイル５はフレキシブル基板１１－２を経由して図示は割愛しているがＲＦＩＤのＩＣ４と共振用コンデンサ６に接続される。アンテナコイル５には磁路を形成するための磁性体シート１０およびクッション材１２が具備される。
【００３９】
また、前記アンテナコイルを前記メモリカードと可歪の導体で接続する構造とし、前記磁性体シートを挟んで携帯情報機器に取り付ける構成とすることで前記アンテナコイルを大きくすることにより通信距離を伸ばすことが可能となる。
図９、１０で示したアンテナコイル実装部１１－１は携帯情報機器の外側の面積の大きい部分に取り付けられることを前提としているためアンテナコイル開口部５－１を大きくすることができ前述したごとく磁性体シート１０の働きとあいまってより長い通信距離を確保することが出来る。また、クッション材１２は携帯情報機器の破損を防止する。
【００４０】
また、前記磁性体シートは、初期透磁率が１０以上で厚みが０．１ｍｍ以上、１ｍｍ以下とすれば、外部機器との通信距離の確保に好適である。
【００４１】
図１１は図１０で示したメモリカード１１を携帯電話機７に適用し、アンテナコイル実装部１１－１を携帯電話機の底部に図示は略したが両面接着テープで貼り付けた場合の概略実装図である。なお、着脱が容易にできる面テープを使用する構成でもよい。
【００４２】
図１２は図１０で示したメモリカード１１搭載の携帯電話機７を外部機器としての電子乗車券改札機８にかざしている図であり、携帯電話機７の下側に位置するアンテナコイル５を含むＲＦＩＤと電子乗車券改札機８との間で電磁界を使っての通信を行う。電子乗車券改札機８から発生しアンテナコイル５の開口部５－１を通る磁束は、大部分が磁路抵抗の低い磁性体シート１０を通過することでループを形成する。
【００４３】
クッション材１２は携帯電話機７と電子乗車券改札機８との衝突時の衝撃を和らげることで携帯電話機７の破損を防ぐ。
【００４４】
＜実施形態４＞
本発明に係わるメモリカードにＲＦＩＤ用のＩＣ４として接触・非接触両用のＩＣを具備した場合の使用例について述べる。
【００４５】
携帯電話機に接触・非接触両用のＩＣ４を具備したメモリーカードを装着し、ＲＦＩＤの非接触通信ではメモリカードはＲＦＩＤのアンテナコイルを用いて情報の送受信を行う。一方メモリカードに設けられた接続端子介して携帯電話機との接触通信を行い携帯電話機のアンテナ１３からの電波を使って、他の電話とのデータのやりとりやホームページへのアクセス等を行う。これら２種類の接続を可能とし、かつデータを相互に共有できるようにすることで、より多くの情報を端末であつかうことが可能になる。例えば、非接触通信によって前述の電子乗車券としての通信を行い、履歴、経費などのデータをＩＣ４のメモリに格納する。さらに、携帯電話のアンテナ１３を介して電子乗車券としての金員のチャージ、電子乗車券としての金員の金融機関における決済、定期券更新、指定券予約のデー

タをメモリカードのＩＣ４に格納する。金銭の処理と改札処理をとも管理することで操作性を向上することができる。さらに、携帯電話にある表示部に、非接触及び接触によるデータ操作の操作履歴、とまり電子乗車券としての残金表示や使用経過明細を表示することでもユーザの使いやすさを向上することも可能である。

【００４６】

以上、本発明の好適な実施形態例について説明したが、本発明は上記実施形態例に限定されるものではなく、本発明の精神を逸脱しない範囲内において、種々の設計変更をなし得ることは勿論である。

【００４７】

例えば、携帯電話機以外に、通信機能を有するＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）などにも適用できる。また、用途としても電子乗車券以外に劇場入場など各種イベント入場にも適用できる。

【００４８】

また、フラッシュメモリ２、コントローラ３、ＩＣ４、コンデンサ６を別々にメモリカード１に搭載する実施例について示したが、フラッシュメモリ２、コントローラ３、ＩＣ４、コンデンサ６のいずれか２つ以上の機能の併せ持つ部品を搭載することも可能である。

【００４９】

【発明の効果】

携帯性を損なうことなく通信距離を確保したＲＦＩＤを有する携帯電話を提供することができる。

【図面の簡単な説明】

【図１】本発明に係るメモリカード。

【図２】図１で示したメモリカード１の概略内部実装図。

【図３】図１で示したメモリカード１を携帯電話機７に適用した場合の概略実装図。

【図４】図３で示したメモリカード１搭載の携帯電話機７を外部機器としての電子乗車券改札機８にかざしている図。

【図５】本発明に係る他のメモリカード。

【図６】図５で示したメモリカード９の概略内部実装図。

【図７】図５で示したメモリカード９を携帯電話機７に適用した場合の概略実装図。

【図８】図７で示したメモリカード９搭載の携帯電話機７を外部機器としての電子乗車券改札機８にかざしている図。

【図９】本発明に係る他のメモリカード。

【図１０】図９で示したメモリカード１１のアンテナコイル実装部１１－１の概略構造図。

【図１１】図９で示したメモリカード１１を携帯電話機７に適用した場合の概略実装図。

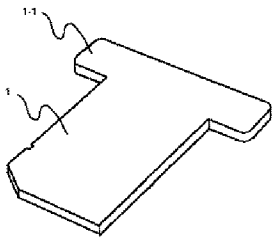
【図１２】図１１で示したメモリカード１１搭載の携帯電話機７を外部機器としての電子乗車券改札機８にかざしている図。

【符号の説明】

１…メモリカード、１－１…アンテナコイル実装部、２…フラッシュメモリ、３…コントローラ、４…ＩＣ、５…アンテナコイル、５－１…アンテナコイル開口部　５－２…基板　６…共振用コンデンサ、７…携帯電話機、８…電子乗車券改札機、９…メモリカード、９－１…アンテナコイル実装部、１０…磁性体シート、１１…メモリカード、１１－１…アンテナコイル実装部、１１－２…フレキシブル基板、１２…クッション材、１３…アンテナ。

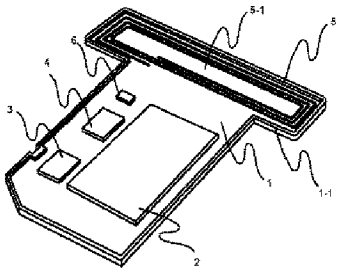
【図1】

図1



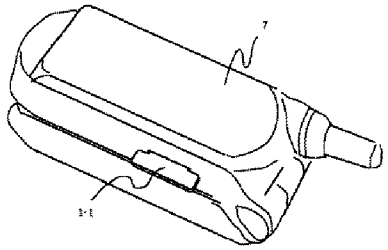
【図2】

図2



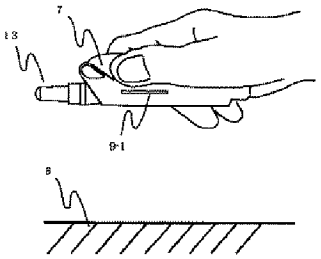
【図3】

図3



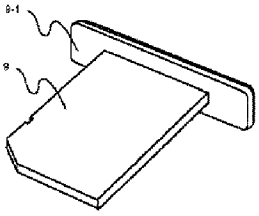
【図4】

図4



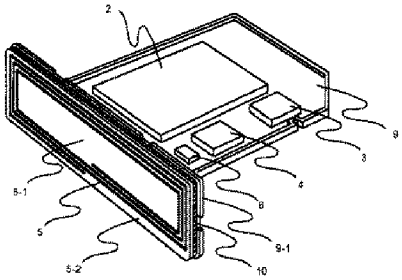
【図5】

図5



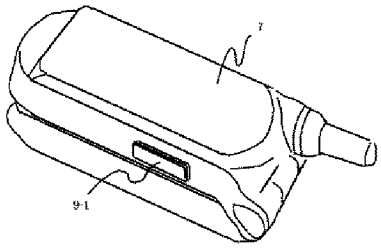
【図6】

図6



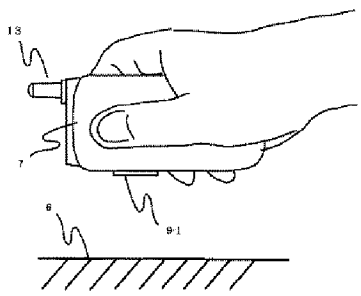
【図7】

図7



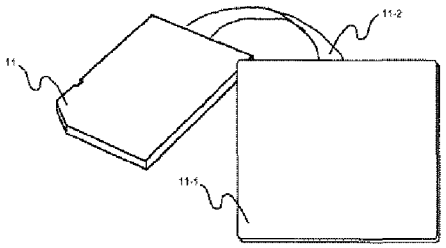
【図8】

図8



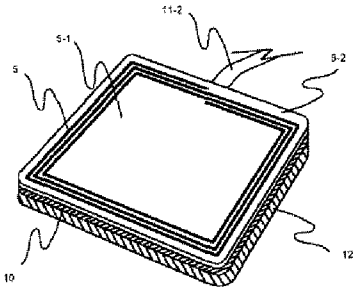
【図9】

図9



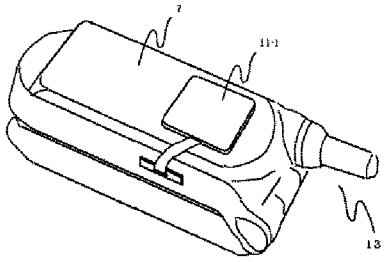
【図10】

図10



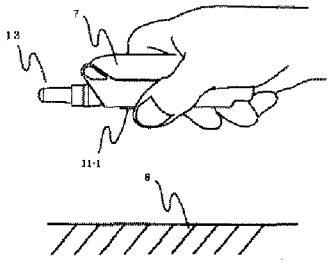
【図11】

図11



【図12】

図12



(51)Int.Cl.[7]	F I		テーマコード（参考）
Ｈ０４Ｍ　1/02	Ｇ０６Ｋ　19/00	Ｈ	

(72)発明者　佐藤　豊
神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立アドバンストデジタル内

Ｆターム(参考) 5B035 AA00 BA01 BB09 BC00 CA01 CA25
5J047 FC02 FC03 FC06
5K012 AA05 AB05 AC08 AC10 AE10 AE13 BA03
5K023 AA07 BB03 MM00 MM25 PP12

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2007-199847
(43)Date of publication of application : 09.08.2007

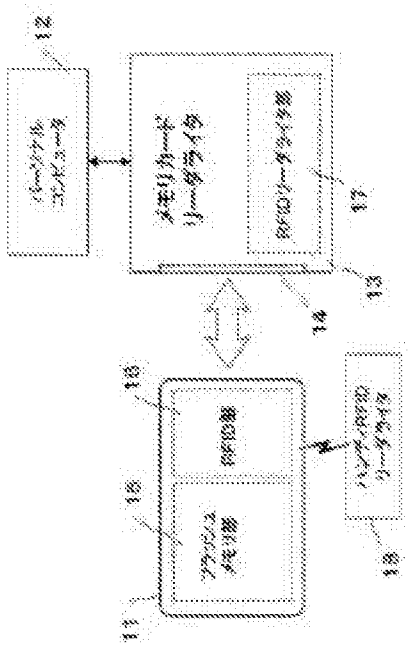
(51)Int.Cl. *G06K 19/07 (2006.01)*
G06K 17/00 (2006.01)
G06F 21/24 (2006.01)

(21)Application number : 2006-015263
(22)Date of filing : 24.01.2006

(71)Applicant : TOSHIBA CORP
TOKYO ELECTRONIC SYSTEMS CORP
(72)Inventor : NAKAO HIROSHI
UEKUSA SHINJI

(54) NONVOLATILE MEMORY MEDIUM WITH RFID FUNCTION AND ITS SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a nonvolatile memory medium with an easily controllable RFID function and a system for using the nonvolatile memory medium.
SOLUTION: The nonvolatile memory medium comprises: an RFID memory for memorizing RFID data which is transmitted and received by radio; a memory section for memorizing data except the RFID data; a memory interface connected with the memory section and RFID memory; and an RFID antenna for transmitting and receiving RFID signals. The nonvolatile memory medium also has an RFID function which has an RFID data area in the memory section, where the RFID data is memorized.



(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2007-199847
(P2007-199847A)
(43)公開日　平成19年8月9日(2007.8.9)

(51)Int.Cl.		F I		テーマコード（参考）
G06K 19/07	(2006.01)	G06K 19/00	H	5B017
G06K 17/00	(2006.01)	G06K 19/00	J	5B035
G06F 21/24	(2006.01)	G06K 17/00	F	5B058
		G06K 17/00	D	
		G06F 12/14	530C	

審査請求 未請求　請求項の数 6　OL　（全 10 頁）

(21)出願番号　特願2006-15263(P2006-15263)
(22)出願日　平成18年1月24日(2006.1.24)

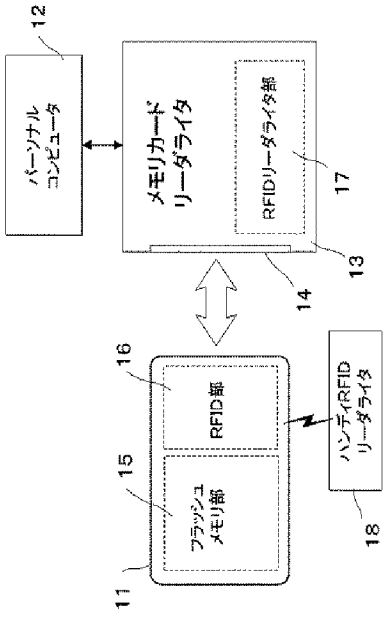
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(71)出願人　593115769
東京エレクトロニツクシステムズ株式会社
神奈川県川崎市幸区小向東芝町１番地
(74)代理人　110000235
特許業務法人　天城国際特許事務所
(72)発明者　中尾　洋
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝小向工場内
(72)発明者　植草　真二
神奈川県川崎市幸区小向東芝町１番地　東京エレクトロニツクシステムズ株式会社内

Ｆターム(参考)　5B017 AA07　BA09　CA14

最終頁に続く

(54)【発明の名称】ＲＦＩＤ機能を有する不揮発性記憶媒体及びそのシステム

(57)【要約】
【課題】容易に管理可能なＲＦＩＤ機能を有する不揮発性記憶媒体、およびそのような記憶媒体が用いられるシステムを提供すること。
【解決手段】無線により送受信可能なＲＦＩＤデータを記憶することが可能なＲＦＩＤメモリと、ＲＦＩＤデータ以外のデータを記憶することが可能なメモリ部と、このメモリ部及び前記ＲＦＩＤメモリに接続されるメモリインターフェースと、前記ＲＦＩＤの信号を送受信するＲＦＩＤ用アンテナとを備え、前記メモリ部に前記ＲＦＩＤデータを記憶可能なＲＦＩＤデータエリアを有することを特徴とするＲＦＩＤ機能を有する不揮発性記憶媒体。
【選択図】図１



【特許請求の範囲】
【請求項1】
無線により送受信可能なＲＦＩＤデータを記憶することが可能なＲＦＩＤメモリと、
ＲＦＩＤデータ以外のデータを記憶することが可能なメモリ部と、
このメモリ部及び前記ＲＦＩＤメモリに接続されるメモリインターフェースと、
前記ＲＦＩＤデータを送受信するＲＦＩＤ用アンテナとを備え、
前記メモリ部に前記ＲＦＩＤデータを記憶可能なＲＦＩＤデータエリアを有することを特徴とするＲＦＩＤ機能を有する不揮発性記憶媒体。
【請求項2】
前記ＲＦＩＤメモリには、各々ただ一つのユニークＩＤが記憶されるリードオンリメモリの領域を有することを特徴とする請求項１記載の、ＲＦＩＤ機能を有する不揮発性記憶媒体。
【請求項3】
前記ＲＦＩＤメモリ及び前記メモリ部には、各々固有のメモリアクセスのためのキーコードを有しており、このキーコードが外部から与えられたキーコードと合致したとき、前記ＲＦＩＤメモリ又は前記メモリ部にアクセス可能であるように、前記メモリインターフェースが作動することを特徴とする請求項１記載の、ＲＦＩＤ機能を有する不揮発性記憶媒体。
【請求項4】
前記メモリ部に記憶されるＲＦＩＤデータ以外のデータは、前記ＲＦＩＤメモリに記憶されるＲＦＩＤデータにより暗号化されて記憶されることを特徴とする請求項１ないし３のいずれか１に記載の、ＲＦＩＤ機能を有する不揮発性記憶媒体。
【請求項5】
コンピュータに接続されるメモリカードリーダライタ及びこのメモリカードリーダライタに着脱可能に接続される不揮発性記憶媒体とを有するシステムであって、
前記不揮発性記憶媒体は、
無線により送受信可能なＲＦＩＤデータを記憶することが可能なＲＦＩＤメモリと、
ＲＦＩＤデータ以外のデータを記憶することが可能であり、その一部に前記ＲＦＩＤデータを記憶可能なＲＦＩＤデータエリアを有するメモリ部と、
このメモリ部及び前記ＲＦＩＤメモリに接続されるメモリインターフェースと、
前記ＲＦＩＤのデータを送受信するＲＦＩＤ用アンテナとを備えることを特徴とする、ＲＦＩＤ機能を有する不揮発性記憶媒体を用いたシステム。
【請求項6】
前記メモリ部に記憶されるＲＦＩＤデータ以外のデータは、前記ＲＦＩＤメモリに記憶されるＲＦＩＤデータにより暗号化されて記憶されることを特徴とする請求項５に記載の、ＲＦＩＤ機能を有する不揮発性記憶媒体を用いたシステム。

【発明の詳細な説明】
【技術分野】
【0001】
本発明は、ＲＦＩＤ機能を有する不揮発性記憶媒体及びそのシステムに関する。
【背景技術】
【0002】
従来、フラッシュメモリなどにより構成されたＰＣカードが、パーソナルコンピュータ（パソコン）のリムーバブルディスクとして用いられる。このようなＰＣカードをいくつも使用するシステムなどではどのカードのどのような内容が記憶されているか、各々を区別する必要があり、例えばこれらのＰＣカードにＲＦＩＤを貼ることが考えられる。
【0003】
しかし、このようなＰＣカードは、パソコンのＰＣカードスロットに挿入して用いられるので、ＲＦＩＤを貼ることは、通常、困難である。
【0004】

なお、特許文献１に開示されているＲＦＩＤ機能を有するＲＦモジュールを有するメモリカードは知られている。しかし、このメモリカードはメモリカードアダプタに挿入されるものであり、これらのメモリカードを識別するものではない。
【特許文献1】特開２００５－２９３４４４号公報、図３及び明細書の段落［００３３］
【発明の開示】
【発明が解決しようとする課題】
【0005】
本発明は上記のような、複数のメモリカード（記憶媒体）を用いる場合の従来の問題点にかんがみてなされたもので、容易に管理可能なＲＦＩＤ機能を有する不揮発性記憶媒体、およびそのような記憶媒体が用いられるシステムを提供することを目的とする。
【課題を解決するための手段】
【0006】
本発明の請求項１によれば、無線により送受信可能なＲＦＩＤデータを記憶することが可能なＲＦＩＤメモリと、ＲＦＩＤデータ以外のデータを記憶することが可能なメモリ部と、このメモリ部及び前記ＲＦＩＤメモリに接続されるメモリインターフェースと、前記ＲＦＩＤデータを送受信するＲＦＩＤ用アンテナとを備え、前記メモリ部に前記ＲＦＩＤデータを記憶可能なＲＦＩＤデータエリアを有することを特徴とするＲＦＩＤ機能を有する不揮発性記憶媒体を提供する。
【0007】
本発明の請求項５によれば、コンピュータに接続されるメモリカードリーダライタ及びこのメモリカードリーダライタに着脱可能に接続される不揮発性記憶媒体とを有するシステムであって、前記不揮発性記憶媒体は、無線により送受信可能なＲＦＩＤデータを記憶することが可能なＲＦＩＤメモリと、ＲＦＩＤデータ以外のデータを記憶することが可能であり、その一部に前記ＲＦＩＤデータを記憶可能なＲＦＩＤデータエリアを有するメモリ部と、このメモリ部及び前記ＲＦＩＤメモリに接続されるメモリインターフェースと、前記ＲＦＩＤのデータを送受信するＲＦＩＤ用アンテナとを備えることを特徴とする、ＲＦＩＤ機能を有する不揮発性記憶媒体を用いたシステムを提供する。
【0008】
本発明において、ＲＦＩＤとは、信号が高周波（ＲＦ）によりデータが変調されて無線により伝送され、各々にただ一つの認識番号（ユニークＩＤ）を有する記憶媒体をいう。このＲＦＩＤとそのリーダライタ間で伝送されるデータは、ＲＦＩＤデータであり、変調された信号はＲＦＩＤデータ信号という。
【発明の効果】
【0009】
本発明によれば、ＰＣカードなど不揮発性記憶媒体にＲＦＩＤ機能を持たせることにより、各々の記憶媒体を識別することが可能になる不揮発性記憶媒体及びその記憶媒体を用いたシステムを得ることができる効果がある。
【0010】
しかも、ＲＦＩＤ機能を実現するに際して、ＲＦＩＤメモリとは異なるメモリ部にもＲＦＩＤデータエリアを設けているので、ＲＦＩＤデータを多く必要とする場合にも本発明の不揮発性記憶媒体を用いることが可能となってＲＦＩＤの用途を拡大することが可能となる。
【発明を実施するための最良の形態】
【0011】
以下、本発明の実施形態について図面を用いて説明する。図１に本発明一実施形態によるシステムの全体構成例を示す。フラッシュメモリカード１１は、メモリカードリーダライタ１３に設けられているスロット１４に挿脱可能になっている。このメモリカードリーダライタ１３はコンピュータ、例えばパーソナルコンピュータ(パソコン）１２に接続されており、パソコン１２に内蔵される場合も多い。
【0012】

フラッシュメモリカード１１は、ＰＣカードのサイズ、厚さなどの規格（TypeI、TypeII、又はTypeIII）に合致したＰＣカードであり、基本的には電子的に不揮発性のフラッシュメモリから形成され、フラッシュメモリ部１５と、ＲＦＩＤの機能を有するＲＦＩＤ部１６とを有する、一種のマルチファンクショナルカードである。フラッシュメモリカード１１がスロット１４に挿入されたとき、メモリカードリーダ１３は、パソコン１２に対して外付けのリムーバブルディスクとして機能する。また、このメモリカードリーダ１３は内部にＲＦＩＤリーダ部１７を有しており、後述するように、フラッシュメモリカード１１のＲＦＩＤ部１６と無線によりＲＦＩＤデータ信号の授受及び信号処理を行う。メモリカード１１のＲＦＩＤ部１６はまた、フラッシュメモリカード１１に近づけられるハンディＲＦＩＤリーダライタ１８とも無線によりＲＦＩＤデータ信号の授受及び信号処理を行う。

【0013】

フラッシュメモリカード１１の一実施形態の構造を図２に示す。このフラッシュメモリカード１１のフラッシュメモリ部１５は、フラッシュメモリ２１と、このフラッシュメモリ２１の情報の書き込み及び読み出しを制御するフラッシュメモリ制御部２２とを有する。

【0014】

フラッシュメモリカード１１のＲＦＩＤ部１６は、ＲＦＩＤリーダ部１７やハンディＲＦＩＤリーダライタ１８と無線信号の授受を行うＲＦＩＤ用アンテナコイル２３と、信号授受時に認証を行う認証部２４と、ＲＦＩＤデータを記憶するＲＦＩＤメモリ２５と、このＲＦＩＤメモリ２５及びフラッシュメモリ２１への信号の書き込み読み出しのインターフェースとなるメモリインターフェース２６と、このメモリインターフェース２６、認証部２４及びＲＦＩＤメモリ２５の制御を行う制御部２７とを有する。フラッシュメモリ２１の信号の書き込み及び読み出しはフラッシュメモリ制御部２２を介して行われる。

【0015】

メモリインターフェース２６と、ＲＦＩＤメモリ２５及びフラッシュメモリ制御部２２とのデータの送受、フラッシュメモリ制御部２２とフラッシュメモリ２１とのデータの送受は、パラレル伝送によりなされる。また、図示していないが、フラッシュメモリカード１１のメモリカードリーダライタ１３のスロット１４に挿入される側には、端子群２８が設けられており、これらの端子は制御部２７と接続され、ＰＣカードとして用いるときには、パソコン１２からメモリインターフェース２６、フラッシュメモリ制御部２２を介してフラッシュメモリ２１へアクセスして、ＲＦＩＤデータ以外のデータの書き込み及び読み出しが可能である。すなわち、原則としてＲＦＩＤデータは、ＲＦＩＤメモリに書き込まれ、ＲＦＩＤデータ以外のデータはフラッシュメモリ２１に記憶されるが、ＲＦＩＤデータの一部はフラッシュメモリ２１のＲＦＩＤデータエリア２９に記憶される構成となっている。

【0016】

ＲＦＩＤ部１６のＲＦＩＤメモリ２５には、そのフラッシュメモリカード１１を識別するためのユニークＩＤと、メモリアクセスのためのキーコードなどがあらかじめ記憶されているシステムエリアと、ユーザが自由に情報を記憶することが可能なユーザエリアとが設けられている。このようなフラッシュメモリカード１１において、通常、主にシステムエリアはリードオンリメモリ（ＲＯＭ）から成り、ユーザエリアはランダムアクセスメモリ（ＲＡＭ）から構成されている。ＲＦＩＤ部１６は比較的小容量であり、ＲＦＩＤメモリ２５に記憶できないＲＦＩＤデータは、フラッシュメモリ２１内の特別のＲＦＩＤデータエリア２９に記憶される。このように、ＲＦＩＤデータをフラッシュメモリ２１に記憶できると、ＲＦＩＤメモリ２５が容量的に小さくても、十分なデータを記憶させることが可能となる。

【0017】

次に本発明のこの実施形態についてフラッシュメモリカード１１がメモリカードリーダライタ１３に挿入されたときの動作を説明する。図３はメモリカードリーダライタ１３側

の動作を、また図４はフラッシュメモリカード１１側の動作を、各々示すフローチャートである。

【0018】

メモリカードリーダライタ１３は、図３のステップＳ３０１において、フラッシュメモリカード１１がスロット１４に挿入されたか否かを検知する。この検知は例えばスロット１４内で一対の光学的素子を設ける、あるいは電気的に行う。挿入が検知されると、ステップＳ３０２において、ＲＦＩＤリーダライタ部１７からフラッシュメモリカード１１にユニークＩＤを問い合わせるＩＤ質問信号を送信し、ステップＳ３０３において、フラッシュメモリカード１１からＩＤ応答信号が送られてくるのを待つ。

【0019】

一方、フラッシュメモリカード１１では、図４のステップＳ４０１においてＲＦＩＤリーダライタ部１７から送信されるＩＤ質問信号を待ち、ＩＤ質問信号がＲＦＩＤ用アンテナコイル２３において受信されると、まず、認証部２４において認証処理がされる。

【0020】

認証されると、ＩＤ質問番号は認証部２４を経由して制御部２７で解析される。ＩＤ質問信号であることが判定されると、制御部２７はＲＦＩＤメモリ２５のシステムエリアに記憶されている、このフラッシュメモリカード１１のユニークＩＤを読み出し、ステップＳ４０２において、ＲＦＩＤ用アンテナコイル２３から送信する。

【0021】

一方、このＩＤ応答信号はメモリカードリーダライタ部１３のＲＦＩＤリーダライタ部１７にて受信される（ステップＳ３０３）と、ステップＳ３０４にてメモリカード１１への制御が読み出しか書き込みか決定し、読み出しのときにはステップ３０５において、書込制御信号をメモリアクセスのためのキーコード、読出データを特定する情報と共に、当該ユニークＩＤのフラッシュメモリカード１１に送信する。この読出制御信号はフラッシュメモリカード１１のＲＦＩＤ用アンテナコイル２３により受信され、制御部２７において解析される。ステップＳ４０４で送られてきた制御信号が読み出しか書き込みか検知される。

【0022】

検知された制御信号が読出制御信号であったときには、ステップＳ４０５において、メモリインターフェース２６からＲＦＩＤメモリ２５及びフラッシュメモリ制御部２２に上記キーコードが送られる。このキーコードと、ＲＦＩＤメモリ２５のシステムエリアに記憶されているキーコードが比較回路（図示せず）で比較され、合致したときには、ＲＦＩＤメモリ２５のユーザエリアから特定のＲＦＩＤデータがメモリインターフェース２６を経由して読み出され、所定の形式で、ＲＦＩＤ用アンテナコイル２３から送信される。

【0023】

一方、上記キーコードはメモリインターフェース２６を経由してフラッシュメモリ制御部２２にも送られて、同様に比較回路で比較され、フラシュメモリ部１５のキーコードと合致するときには、フラッシュメモリ２１から特定のＲＦＩＤデータ以外の読出データがフラッシュメモリ制御部２２又は直接、メモリインターフェース２６を経由して読み出され所定の形式で、ＲＦＩＤ用アンテナコイル２３から送信される（ステップＳ４０５）。この送信された読み出しデータはステップＳ３０６で、ＲＦＩＤリーダライタ部１７において、受信される。そして、例えばステップＳ３０７で、パソコン１２の表示画面上にユニークＩＤと共に、フラッシュメモリカード１１から送信されてきたデータがファイルとして、あるいは内容自体が表示される。

【0024】

一方、フラッシュメモリカード１１への制御が、書き込み命令のときには、ステップＳ３０８で書き込み制御信号が、ＲＦＩＤリーダライタ部１７から送信され、続いてステップＳ３０９において、ユニークＩＤとメモリアクセスのためのキーコードと、書き込む内容のＲＦＩＤデータの書込データを送信する。

【0025】

ステップＳ４０４において制御部２７で、ＲＦＩＤリーダライタ部１７から送られてきた制御信号が書込制御信号であることが検知されたときには、ステップＳ４０６においてＲＦＩＤ用アンテナコイル２３によりＲＦＩＤデータの書込データを受信する。そしてステップＳ４０７において、読み出しのときと同じように、送付されてきたキーコードをそれぞれのキーコードと比較することにより、ＲＦＩＤメモリ２５への書き込みかフラッシュメモリ２１への書き込みかを判別し、それらの特定の場所に受信した書込データを記憶し終了する。内からのデータの読み出し、フラッシュメモリ２１へのデータの書き込みの対象エリアはＲＦＩＤデータエリア２９であることもある。

【0026】

このようにして、ユニークＩＤを特定し、フラッシュメモリカード１１とメモリカードリーダライタのＲＦＩＤリーダライタ部１７との間でＲＦＩＤデータの送受信が行われる。

【0027】

ここでは詳しく述べないが、フラッシュメモリカード１１はハンディＲＦＩＤリーダライタ１８とも、ＲＦＩＤデータ信号の送受信を行うことが可能である。この場合にもハンディＲＦＩＤリーダライタ１８と認証部２４との間でまず認証を行い、その後に信号の送受信を行う。

【0028】

フラッシュメモリカード１１は、メモリカードリーダライタ１３のスロットに挿入することにより、端子群２８が、メモリカードリーダライタ１３内の所定の端子と接続され、通常のＰＣカードと同じようにパソコン１２に対してリムーバブルディスクとして用いることができる。

【0029】

上記認証部２４を設けると、セキュリティの高いＲＦＩＤ機能を達成できる利点がある。しかし、本発明によるメモリカードにおいて認証部は必ずしも必要でない。

【0030】

上記実施形態の動作では、フラッシュメモリカードがメモリカードリーダライタに挿入された場合について述べたが、無線によりＲＦＩＤデータの送受が行われるので、フラッシュメモリカード１１がメモリカードリーダライタ１７の近くに置かれた場合も同様に動作させることができる。

【0031】

なお、上記ＲＦＩＤ用アンテナコイル２３の背面には、通信の妨げになるようなものは配置しない。ＲＦＩＤ用アンテナコイル２３は、特にフラッシュメモリカード１１の金属板が設けられていない部分に設けるほうが、外部との無線の送受信に好適である。また、本発明のメモリカードに内蔵されるＲＦＩＤ用のアンテナは必ずしもコイル形状をしている必要はない。

【0032】

上記実施形態では、フラッシュ型のメモリカードを用いた場合について述べたが、必ずしもフラッシュ型でなくてもよく、不揮発性のメモリカードであればよい。

【0033】

上記実施形態では、フラッシュメモリカードのＲＦＩＤ部１６にはＲＦＩＤデータを書き込み可能になっていたが、予めＲＦＩＤデータが記憶されており、外部からＲＦＩＤデータのみを読み出すことのみができるようになっていてもよい。この場合には、ＲＦＩＤリーダライタ部１７はＲＦＩＤリーダに置き換えられ、ハンディＲＦＩＤリーダライタ１８は、ハンディＲＦＩＤリーダに置き換えることができる。なお、ＲＦＩＤリーダライタ及びＲＦＩＤリーダはハンディであることは本発明において必ずしも必須ではない。

【0034】

上記実施形態によれば、管理するメモリカードが多くなった場合、ハンディＲＦＩＤリーダライタ１８やメモリカードリーダライタを用いてそれぞれのメモリカードのユニークＩＤを読み取ることによりそれらのＩＤと内容を結びつけたデータベースとの紐付けが可

能になり、容易に管理できるようになる効果がある。ＲＦＩＤの読み取りやフラッシュメモリカードは通常のＰＣ用などのメモリカードとしてもそれぞれ単独で読み取り可能なので、ＲＦＩＤリーダライタを搭載してないメモリカードリーダライタにおいて通常のフラッシュメモリとして用いることが可能である。

【0035】

ＲＦＩＤのＩＣチップが保持するメモリ容量は、通常数バイトから数百バイトであるが、フラッシュメモリの容量は、１Ｇバイト以上のものがある。ＲＦＩＤからフラッシュメモリに直接アクセスできるようすることにより、非接触で広大なメモリエリアにアクセス可能となり、ＲＦＩＤとしての用途を広げることが可能となる。

【0036】

このように、通常のフラッシュメモリカードにＲＦＩＤを搭載することによりメモリカード本体の管理が容易になると共に、書き込むデータのセキュリティに応用することが可能となる。即ち、認証などの処理によるチェックをフラッシュメモリのエリアを用いて行うことが容易にできる。更に、ＲＦＩＤからフラッシュメモリカードにアクセスできるようにすることによってＲＦＩＤとしての用途が格段に広がる。

【0037】

また、ＲＦＩＤとしてのデータをキーとしてフラッシュメモリに書き込まれるデータを暗号化すれば、ＲＦＩＤリーダを搭載していないカードリーダによりフラッシュメモリのデータを読み出すことができないようにすることが可能となり、メモリカードのセキュリティをより高めることが可能となる。

【0038】

上記実施形態では、フラッシュメモリカードについて述べたが、本発明ではこれに限られず、ＳＤメモリ、コンパクトフラッシュ(登録商標)、メモリスティックなど、一般的には不揮発性の記憶媒体であればよい。

【0039】

本発明は上記実施形態に限定されるものではなく、本発明の技術思想の範囲内で種々変形して実施可能である。

【図面の簡単な説明】

【0040】

【図1】本発明一実施形態によるシステムの全体の構成を示す図。

【図2】本発明一実施形態におけるフラッシュメモリカードの構成例を示す図。

【図3】本発明一実施形態においてメモリカードリーダライタの動作を説明するための図。

【図4】本発明一実施形態においてフラッシュメモリカードの動作を説明するための図。

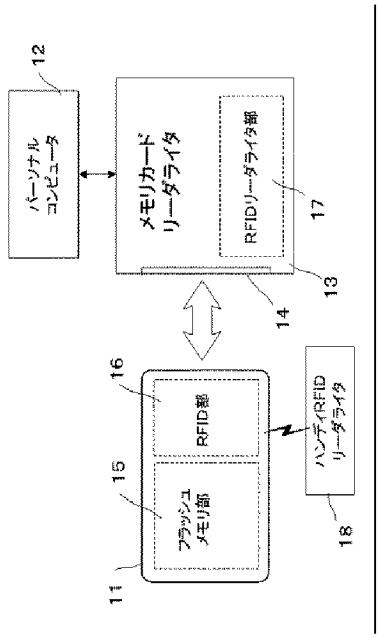
【符号の説明】

【0041】

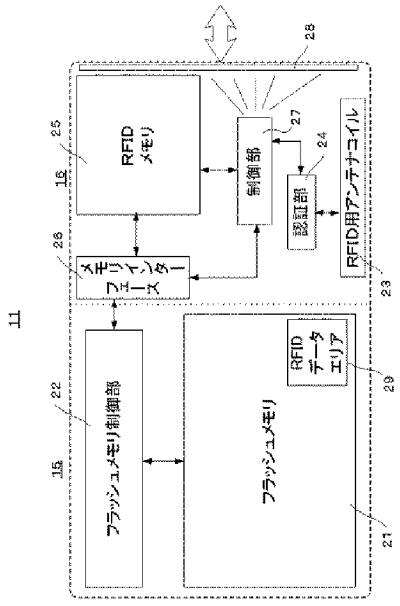
１１・・・フラッシュメモリカード、
１２・・・パーソナルコンピュータ（パソコン）、
１３・・・メモリカードリーダライタ、
１４・・・スロット、
１５・・・フラッシュメモリ部、
１６・・・ＲＦＩＤ部、
１７・・・ＲＦＩＤリーダライタ部、
１８・・・ハンディＲＦＩＤリーダライタ、
２１・・・フラッシュメモリ、
２２・・・フラッシュメモリ制御部、
２３・・・ＲＦＩＤ用アンテナコイル、
２４・・・認証部、
２５・・・ＲＦＩＤメモリ、
２６・・・メモリインターフェース、

２７・・・制御部、
２８・・・端子群、
２９・・・ＲＦＩＤデータエリア。

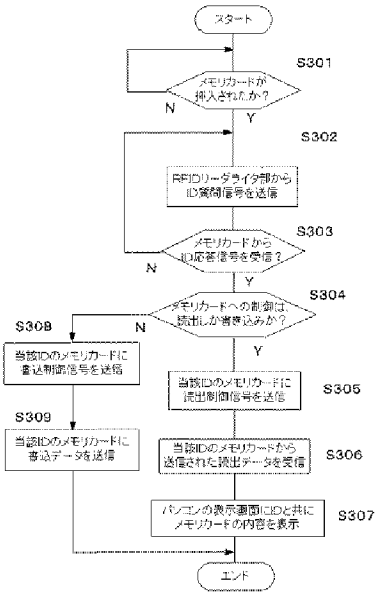
【図1】



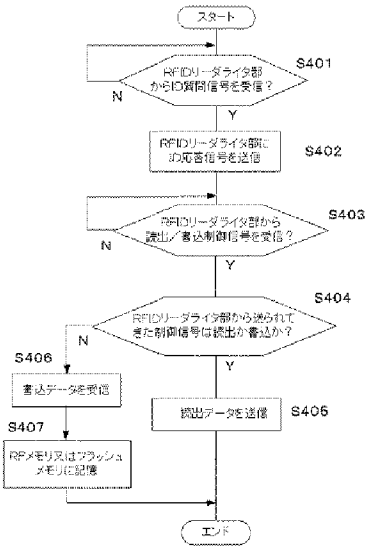
【図2】



【図3】


スタート
S301
メモリカードが挿入されたか？
N
Y
S302
RFIDリーダライタ部からID質問信号を送信
S303
メモリカードからID応答信号を受信？
N
Y
S304
メモリカードへの制御は、読出しか書込みか？
S308
N
当該IDのメモリカードに書込制御信号を送信
Y
当該IDのメモリカードに読出制御信号を送信
S305
S309
当該IDのメモリカードに書込データを送信
当該IDのメモリカードから送信された読出データを受信
S306
パソコンの表示画面にIDと共にメモリカードの内容を表示
S307
エンド

【図4】


スタート
S401
RFIDリーダライタ部からID質問信号を受信？
N
Y
RFIDリーダライタ部にID応答信号を送信
S402
S403
RFIDリーダライタ部から読出／書込制御信号を受信？
N
Y
S404
RFIDリーダライタ部から送られてきた制御信号は読出か書込か？
N
Y
S406
書込データを受信
S405
読出データを送信
S407
RFメモリ又はフラッシュメモリに記憶
エンド

Ｆターム(参考) 5B035 AA06 AA13 BB09 CA25 CA38
5B058 CA13 CA17 CA23 CA26 KA35

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2007-328689
(43)Date of publication of application : 20.12.2007

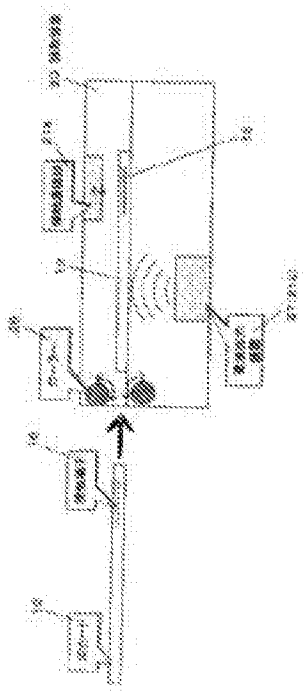
(51)Int.Cl. *G06K 19/07 (2006.01)*
G06K 17/00 (2006.01)

(21)Application number : 2006-160987
(22)Date of filing : 09.06.2006

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : YAMADA MASANARI

(54) PORTABLE INFORMATION RECORDING MEDIUM AND READER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a portable information recording medium continuously operating as it is even when power feeding becomes unstable because of a contact failure or the like, and to provide a reader.
SOLUTION: An IC card 10 is provided with a contact terminal 16 and an antenna. When the IC card 10 is inserted into the reader 20, a contact communication part 21a of the reader 20 supplies power in a contact manner, and the contact terminal 16 of the IC card 10 receives the power in a contact manner. Even when the contact terminal 16 of the IC card 10 receives the power, a radio wave output device 27 of the reader 20 emits radio waves, the IC card 10 receives the radio waves to generate power.



(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2007-328689
(P2007-328689A)
(43)公開日　平成19年12月20日(2007.12.20)

(51)Int.Cl.		F I		テーマコード（参考）
G06K 19/07	(2006.01)	G06K 19/00	J	5B035
G06K 17/00	(2006.01)	G06K 17/00	B	5B058

審査請求 未請求　請求項の数 5　ＯＬ　（全 8 頁）

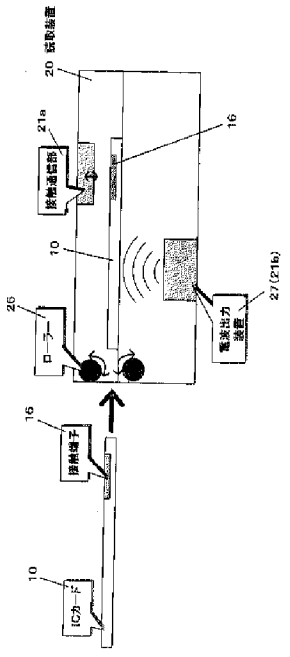
(21)出願番号　特願2006-160987 (P2006-160987)
(22)出願日　平成18年6月9日 (2006.6.9)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100092576
弁理士　鎌田　久男
(72)発明者　山田　真生
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

Ｆターム(参考)　5B035 AA11　BB09　CA12　CA25
5B058 CA13　CA17　CA22　KA40

(54)【発明の名称】携帯可能情報記録媒体及び読取装置

(57)【要約】
【課題】接点不良などによって電力の供給が不安定になった場合であっても、そのまま動作し続けることができる携帯可能情報記録媒体及び読取装置を提供する。
【解決手段】ＩＣカード１０は、接触端子１６とアンテナとを備える。読取装置２０にＩＣカード１０を挿入すると、読取装置２０の接触通信部２１ａからは、接触式で電力が供給され、ＩＣカード１０の接触端子１６は、接触式で電力を受信する。また、ＩＣカード１０の接触端子１６が電力を受信している場合であっても、読取装置２０の電波出力装置２７からは、電波が発せられ、ＩＣカード１０は、その電波をアンテナで受信して電力を発生させる。
【選択図】図３



【特許請求の範囲】
【請求項1】
接触式で電力を受信する接触式電力受信手段と、
非接触式で電波を受信して電力を発生させる非接触式電波受信手段とを備え、
前記接触式電力受信手段が電力を受信している場合であっても、前記非接触式電波受信手段に電波の受信を行わせること、
を特徴とする携帯可能情報記録媒体。
【請求項2】
接触式で電力を受信する接触式電力受信手段と、
非接触式で電波を受信して電力を発生させる非接触式電波受信手段とを備え、
前記非接触式電波受信手段が電波を受信している場合であっても、前記接触式電力受信手段に電力の受信を行わせること、
を特徴とする携帯可能情報記録媒体。
【請求項3】
請求項１又は請求項２に記載の携帯可能情報記録媒体において、
接触式で制御信号を受信する接触式制御信号受信手段と、
非接触式で制御信号を受信する非接触式制御信号受信手段とを備え、
この携帯可能情報記録媒体が接触式で動作する場合には、前記非接触式制御信号受信手段が受信した制御信号を無効とし、
この携帯可能情報記録媒体が非接触式で動作する場合には、前記接触式制御信号受信手段が受信した制御信号を無効とすること、
を特徴とする携帯可能情報記録媒体。
【請求項4】
接触式で電力を供給する接触式電力供給手段と、
非接触式で電波を供給する非接触式電波供給手段とを備え、
前記接触式電力供給手段が電力を供給している場合であっても、前記非接触式電力供給手段に電波の供給を行わせること、
を特徴とする読取装置。
【請求項5】
接触式で電力を供給する接触式電力供給手段と、
非接触式で電波を供給する非接触式電力供給手段とを備え、
前記非接触式電力供給手段が電波を供給している場合であっても、前記接触式電力供給手段に電力の供給を行わせること、
を特徴とする読取装置。

【発明の詳細な説明】
【技術分野】
【0001】
本発明は、携帯可能情報記録媒体及び読取装置に関するものである。
【背景技術】
【0002】
従来、接触式・非接触式の２つの通信手段を備えたＩＣカードは、片方の通信方式のみを使用して外部と情報を交換する。そのため、接触式で通信する場合は、接触式の接点から供給される電力を使用して動作し、非接触式で通信する場合は、電波とアンテナコイルとの電磁誘導により発生する電力を使用して動作する。
【0003】
図４は、接触式の通信手段を備えたＩＣカードを示す図である。
接触式の通信手段を備えたＩＣカード１００は、振動の多い場所に設置された場合、接点不良が生じる可能性がある。
ＩＣモジュール端子１０１のリセット信号端子２や、クロック信号端子３は、接点不良を起こしても即座に接点が復帰すれば、そのまま動作し続ける可能性が高い。また、デー

タ入出力信号端子７が接点不良を起こして通信に異常が発生しても、ＩＣカード１００と読取装置間で復帰措置が取られるような通信規約が定義されている。
しかし、回路電圧端子１が接点不良を起こした場合には、ＩＣカード１００が誤動作したり、処理中の命令が途中で止まってしまったりして故障の原因になる可能性があった。
【0004】
一方、特許文献１は、有料道路の自動料金収受システムを開示しているが、このシステムで使用されるカード型記録媒体は、車の走行中に発生する振動によって接点不良を起こし、上述したような問題が起こる可能性があった。
【特許文献1】特開平１０－２１４３８号公報
【発明の開示】
【発明が解決しようとする課題】
【0005】
本発明の課題は、接点不良などによって電力の供給が不安定になった場合であっても、そのまま動作し続けることができる携帯可能情報記録媒体及び読取装置を提供することである。
【課題を解決するための手段】
【0006】
本発明は、以下のような解決手段により、前記課題を解決する。なお、理解を容易にするために、本発明の実施例に対応する符号を付して説明するが、これに限定されるものではない。
請求項１の発明は、接触式で電力を受信する接触式電力受信手段（１１ａ）と、非接触式で電波を受信して電力を発生させる非接触式電波受信手段（１１ｂ）とを備え、前記接触式電力受信手段（１１ａ）が電力を受信している場合であっても、前記非接触式電波受信手段（１１ｂ）に電波の受信を行わせること、を特徴とする携帯可能情報記録媒体である。
請求項２の発明は、接触式で電力を受信する接触式電力受信手段（１１ａ）と、非接触式で電波を受信して電力を発生させる非接触式電波受信手段（１１ｂ）とを備え、前記非接触式電波受信手段（１１ｂ）が電波を受信している場合であっても、前記接触式電力受信手段（１１ａ）に電力の受信を行わせること、を特徴とする携帯可能情報記録媒体である。
請求項３の発明は、請求項１又は請求項２に記載の携帯可能情報記録媒体において、接触式で制御信号を受信する接触式制御信号受信手段（１１ａ）と、非接触式で制御信号を受信する非接触式制御信号受信手段（１１ｂ）とを備え、この携帯可能情報記録媒体（１０）が接触式で動作する場合には、前記非接触式制御信号受信手段（１１ｂ）が受信した制御信号を無効とし、この携帯可能情報記録媒体（１０）が非接触式で動作する場合には、前記接触式制御信号受信手段（１１ａ）が受信した制御信号を無効とすること、を特徴とする携帯可能情報記録媒体である。
請求項４の発明は、接触式で電力を供給する接触式電力供給手段（２１ａ）と、非接触式で電波を供給する非接触式電波供給手段（２１ｂ）とを備え、前記接触式電力供給手段（２１ａ）が電力を供給している場合であっても、前記非接触式電力供給手段（２１ｂ）に電波の供給を行わせること、を特徴とする読取装置である。
請求項５の発明は、接触式で電力を供給する接触式電力供給手段（２１ａ）と、非接触式で電波を供給する非接触式電力供給手段（２１ｂ）とを備え、前記非接触式電力供給手段（２１ｂ）が電波を供給している場合であっても、前記接触式電力供給手段（２１ａ）に電力の供給を行わせること、を特徴とする読取装置である。
【発明の効果】
【0007】
本発明によれば、携帯可能情報記録媒体に、接触式と非接触式の受信手段を備えさせ、両方の受信手段で電力を受信するので、一方の受信手段にトラブルが発生しても、そのまま動作し続けることができる。

また、接触式での動作や、非接触式での動作などの状況に応じて、制御信号を使い分けることよって、携帯可能情報記録媒体に誤動作を生じさせない。

一方、読取装置に、接触式と非接触式の供給手段を備えさせ、両方の供給手段で電力を供給するので、一方の電力の供給が不安定になった場合であっても、安定して電力を供給し続けることができる。

【発明を実施するための最良の形態】

【0008】

本発明は、接点不良などによって電力の供給が不安定になった場合であっても、そのまま動作し続けることができる携帯可能情報記録媒体及び読取装置を提供するという目的を、接触式で電力を受信している場合であっても、非接触式で電波を受信させて電力を発生させることにより実現する。

【実施例】

【0009】

以下、図面等を参照して、本発明の実施例について、さらに詳しく説明する。

図１は、本発明による携帯可能情報記録媒体及び読取装置の実施例を示す図である。

本実施例のＩＣカード（携帯可能情報記録媒体）１０は、通信部１１と、ＣＰＵ１２と、ＲＡＭ１３と、ＲＯＭ１４と、ＥＥＰＲＯＭ１５などとを備える。

【0010】

通信部１１は、ＣＰＵ１２及び読取装置２０間の通信を媒介する部分であり、接触通信部（接触式電力受信手段、接触式制御信号受信手段）１１ａと、非接触通信部（非接触式電波受信手段、非接触式制御信号受信手段）１１ｂとを備える。

接触通信部１１ａは、接触式で読取装置２０と通信を行う部分であり、電力や制御信号を受信する接触端子を備える。

非接触通信部１１ｂは、非接触式で読取装置２０と通信を行う部分であり、制御信号を含む電波又は制御信号を含まない電波を受信して電力を発生させる巻き線コイルなどのアンテナを備える。

【0011】

ＣＰＵ１２は、ＩＣカード１０や通信部１１を統括制御する中央処理装置であり、通信部１１を介して受信するコマンドに応じて、ＲＯＭ１４及びＥＥＰＲＯＭ１５に記憶されている実行コードを実行する部分である。

ＲＡＭ１３は、揮発性メモリであり、ＣＰＵ１２が処理を行う作業領域として使用される。

【0012】

ＲＯＭ１４は、不揮発性の読み出し専用のメモリであり、実行コードや各種パラメータなどが記憶されている。

ＥＥＰＲＯＭ１５は、随時書き換え可能な不揮発性のメモリであり、実行コードやカードの固有情報などが記憶されている。

【0013】

一方、読取装置２０は、通信部２１と、ＣＰＵ２２と、ＲＡＭ２３と、ＲＯＭ２４と、ＥＥＰＲＯＭ２５などとを備える。

通信部２１は、ＣＰＵ２２及びＩＣカード１０間の通信を媒介する部分であり、接触通信部（接触式電力供給手段）２１ａと、非接触通信部（非接触式電波供給手段）２１ｂとを備える。

接触通信部２１ａは、接触式でＩＣカード１０と通信を行う部分であり、電力を供給する接触端子を備える。

非接触通信部２１ｂは、非接触式でＩＣカード１０と通信を行う部分であり、電波を発するアンテナを備える。

【0014】

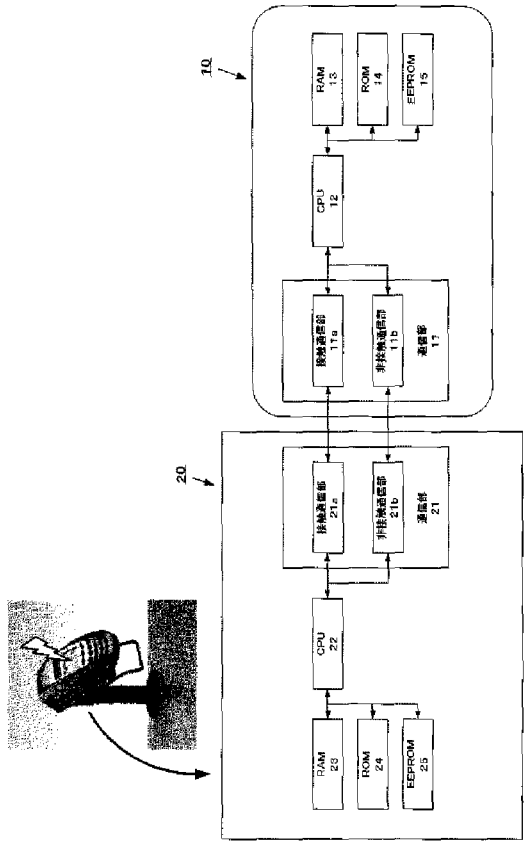
ＣＰＵ２２は、読取装置２０や通信部２１を統括制御する中央処理装置であり、タッチボタンなどからの入力情報に応じて、ＲＯＭ２４及びＥＥＰＲＯＭ２５に記憶されている

実行コードを実行する部分である。
　ＲＡＭ２３は、揮発性メモリであり、ＣＰＵ２２が処理を行う作業領域などとして使用される。
【0015】
　ＲＯＭ２４は、不揮発性の読み出し専用のメモリであり、実行コードや各種パラメータなどが記憶されている。
　ＥＥＰＲＯＭ２５は、随時書き換え可能な不揮発性のメモリであり、実行コードや固有情報などが記憶されている。
【0016】
　図２は、ＩＣカード１０の内部構造の詳細を説明する図である。
　ＩＣカード１０のＣＰＵ１２は、制御信号などを振り分けるセレクター１２１と、制御信号を解読し実行するプロセッサー１２２とを備える。なお、図２の接触電源端子３０、接触電源検知部３１、接触Ｉ／Ｏ端子３２、接触受信部３３、接触信号検知部３４は、図１の接触通信部１１ａに含まれており、図２のアンテナ４０、非接触受信部４１、変復調部４２、非接触信号検知部４３、非接触電源検知部４４は、図１の非接触通信部１１ｂに含まれている。
【0017】
　図２（Ａ）に示すように、接触電源端子３０から、接触電源検知部３１に電力が供給されると、セレクター１２１は、プロセッサー１２２に電力を供給する。
　図２（Ｂ）に示すように、接触Ｉ／Ｏ端子３２から、接触受信部３３を介して接触信号検知部３４に制御信号が送信されると、セレクター１２１は、その制御信号をプロセッサー１２２に送信する。
【0018】
　ＩＣカード１０は、接触通信部１１ａと非接触通信部１１ｂの２つの通信手段を備えているので（図１参照）、接触式で動作することも、非接触式で動作することもできる。そこで、セレクター１２１は、ＩＣカード１０が、接触式で動作する場合には、非接触式の制御信号を無効とし、非接触式で動作する場合には、接触式の制御信号を無効とする。
　接触信号検知部３４が、非接触式の制御信号よりも先に、接触式の制御信号を検知した場合には、ＣＰＵ１２は、セレクター１２１の設定を「非接触信号受信不可」に変更する。なお、これとは逆に、非接触信号検知部４３が、接触式の制御信号よりも先に、非接触式の制御信号を検知した場合には、ＣＰＵ１２は、セレクター１２１の設定を「接触信号受信不可」に変更する。
【0019】
　このように設定を変更することによって、図２（Ｃ）に示すように、アンテナ４０から、非接触受信部４１及び変復調部４２を介して、非接触信号検知部４３が制御信号を受信した場合には、セレクター１２１は、その制御信号を無効とし、プロセッサー１２２には、送信しない。
　また、図２（Ｄ）に示すように、アンテナ４０から、非接触受信部４１を介して、非接触電源検知部４４が電力を受信した場合は、セレクター１２１は、その電力をプロセッサー１２２に送信する。
【0020】
　図３は、ＩＣカード１０及び読取装置２０の動作を説明する模式図である。
　まず、利用者は、ＩＣカード１０の接触端子１６を表側かつ前側にしながら、読取装置２０にＩＣカード１０を挿入する。
　そうすると、読取装置２０のローラー２６が回転し、ＩＣカード１０が奥まで挿入される。
　そして、読取装置２０の接触通信部２１ａからは、接触式で電力が供給され、ＩＣカード１０の接触端子１６は、接触式で電力を受信する。
　また、ＩＣカード１０の接触端子１６が電力を受信している場合であっても、読取装置２０の電波出力装置２７（非接触通信部２１ｂ）からは、電波が発せられ、ＩＣカード１

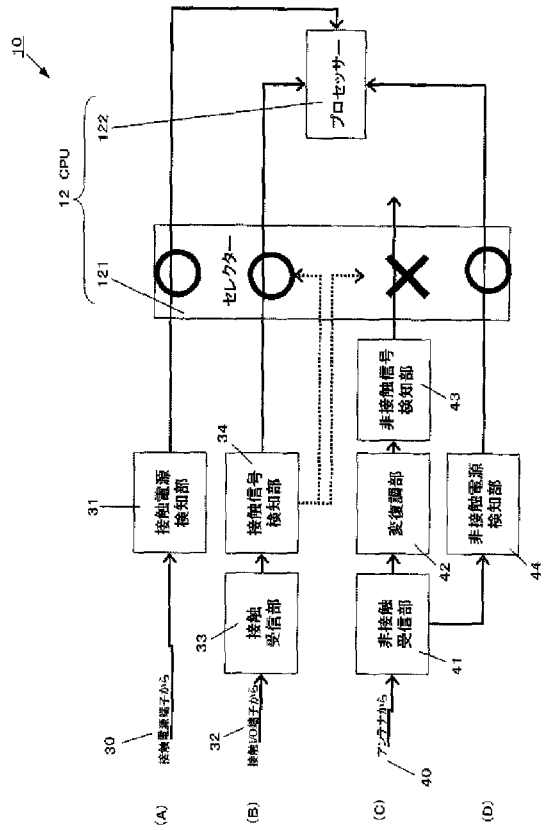
０は、その電波を受信して電力を発生させる。
【0021】
　このように、本実施例によれば、以下のような効果がある。
（１）ＩＣカード１０に、接触通信部１１ａと非接触通信部１１ｂとを備えさせ、両方の通信部で電力を受信するので、振動などによって接触端子１６が接点不良を起こしても、電波によって電力の供給を補助することができ、ＩＣカード１０が誤動作したり、処理中の命令が途中で止まってしまったりすることがない。
（２）読取装置２０は、ＩＣカード１０と接触式で通信している最中も電波を出し続け、ＩＣカード１０は、接触式で供給されている電力と、電磁誘導によって起電する電力とを区別しないで使用することができるので、ＩＣカード１０の動作が安定する。
【0022】
（３）セレクター１２１は、接触式での動作や、非接触式での動作などの状況に応じて、制御信号を振り分けるので、ＩＣカード１０に誤動作を生じさせない。
（４）例えば、ＩＣカード１０をデュアルインタフェースカードにし、ＥＴＣ（Electronic Toll Collection；登録商標）カードや、ＩＣパチンコカードとして使用すれば、振動の多い環境であっても好適に使用することができる。なお、ＥＴＣカードを装着する車載用の読取装置は、接触部分をスプリングなどによって上から押さえつけ、振動を吸収するような構造になっているが、カードを抜き差しする必要があるため、スプリングの強度をそれほど強くすることができない。そこで、本実施例の構成を採用すれば、カードをそれほど強固に押さえつけていなくても、電力の供給を安定させることができる。
【0023】
（変形例）
　以上説明した実施例に限定されることなく、種々の変形や変更が可能であって、それらも本発明の均等の範囲内である。
（１）ＩＣカード１０は、接触通信部１１ａが電力を受信している場合であっても、非接触通信部１１ｂに電波の受信を行わせる例で説明したが、これとは逆に、非接触通信部１１ｂが電波を受信している場合であっても、接触通信部１１ａに電力の受信を行わせてもよい。このようにすれば、ＩＣカード１０は、応答信号などの電波を安定して発信することができる。
（２）読取装置２０は、接触通信部１１ａが電力を供給している場合であっても、非接触通信部１１ｂに電波の供給を行わせる例で説明したが、これとは逆に、非接触通信部１１ｂが電波を供給している場合であっても、接触通信部１１ａに電力の供給を行わせてもよい。このようにすれば、ＩＣカード１０に対して、安定して電力の供給を行うことができる。
（３）接触式のＩＣカードであれば、デュアルタイプやハイブリットタイプのＩＣカードにせず、電力を起電するための専用のアンテナを設けてもよい。
【図面の簡単な説明】
【0024】
【図1】本発明による携帯可能情報記録媒体及び読取装置の実施例を示す図である。
【図2】ＩＣカード１０の内部構造の詳細を説明する図である。
【図3】ＩＣカード１０及び読取装置２０の動作を説明する模式図である。
【図4】接触式の通信手段を備えたＩＣカードを示す図である。
【符号の説明】
【0025】
１０　ＩＣカード（携帯可能情報記録媒体）
１１　通信部
１１ａ　接触通信部（接触式電力受信手段、接触式制御信号受信手段）
１１ｂ　非接触通信部（非接触式電波受信手段、非接触式制御信号受信手段）
１２　ＣＰＵ
１２１　セレクター

１２２　プロセッサー
１３　ＲＡＭ
１４　ＲＯＭ
１５　ＥＥＰＲＯＭ
１６　接触端子
２０　読取装置
２１　通信部
２１ａ　接触通信部（接触式電力供給手段）
２１ｂ　非接触通信部（非接触式電波供給手段）
２２　ＣＰＵ
２３　ＲＡＭ
２４　ＲＯＭ
２５　ＥＥＰＲＯＭ

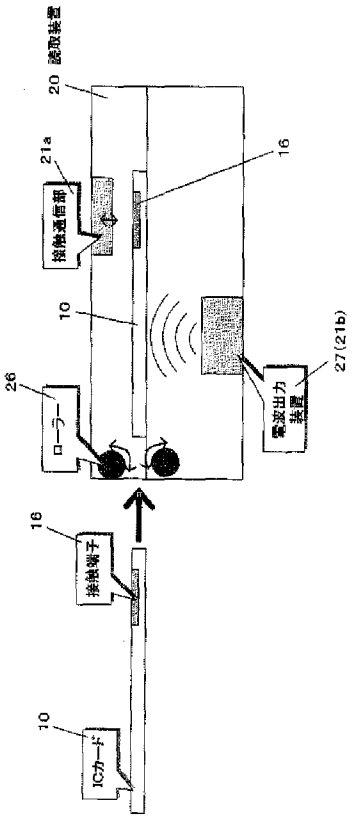
【図1】



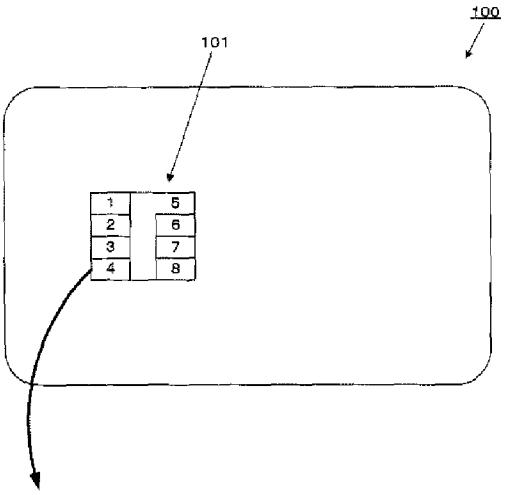
【図2】



【図3】



【図4】



ICモジュール端子の役割			
1. Vcc	:回路電圧	5. GND	:グランド
2. RST	:リセット信号	6. Vpp	:書込み供給電圧
3. CLK	:クロック信号	7. I／O	:データ入出力信号
4. RFU	:将来利用	8. RFU	:将来利用

INVENTOR-INFORMATION:

NAME COUNTRY

ASSIGNEE-INFORMATION:

PAT-NO: JP404102112A

DOCUMENT-JP 04102112 A IDENTIFIER:

TITLE: DOCUMENT EDITING DEVICE, INFORMATION PROCESSOR AND BATTERY USED FOR THE DOCUMENT EDITING DEVICE AND INFORMATION PROCESSOR

PUBN-DATE: April 3, 1992

FUKUSHIMA, MASAHITO

YAMAZAKI, ISAO

SUGANUMA, YUJI

MATSUOKA, SHIGERU

NAME COUNTRY

HITACHI LTD N/A

APPL-NO: JP02218924

APPL-DATE: August 22, 1990

INT-CL (IPC): G06F001/26 , G06F015/20 , G06F015/20

ABSTRACT:

PURPOSE: To make the main body itself of a Japanese word processorsmall in volume and

light in weight by forming a battery like a seallead battery insertable to a memory card slot, and

providing the slotwhich can supply power and insert a memory card as well.

7/20/2011, EAST Version: 3.0.0.6

CONSTITUTION: This word processor is composed of a display device1, input device 2, printer

4 and so on. In this case, a slot 12 isprovided to insert a ROM card building in a card-shaped

seal leadbattery or a program in the same shape as the memory card to berequired in the case

of carrying the main body and requiring a powersource for backup, or a RAM card to store data

such as documents orthe like. Namely, the battery like the light seal lead battery can beinserted

to the slot of the memory card so as to use the slot notonly for supplying power but also for

inserting the memory card.Thus, the main body itself of the Japanese word processor or

apersonal computer can be small in volume and light in weight.

COPYRIGHT: (C)1992,JPO&Japio

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

7/20/2011, EAST Version: 3.0.0.6

Biblio

[Print]

Patent/Publication Number	200905471
Title	Memory card hidden command protocol
Issued/Publication Date	2009/02/01
Application Date	2008/03/26
Application Number	097110873
IPC	G06F-012/00(200601)
Inventor	NARENDRA, SIVA G. US; TADEPALLI, PRABHAKAR IN; SPITZER, THOMAS N. US
Applicant	TYFONE, INC.US
Priority Number	20070330US20070920932P 20070824US20070895629
Abstract	A memory card compatible token includes non-memory components accessed using commands hidden in the data stream of a memory card access command. A mobile computing device such as a mobile phone accesses the non-memory components by writing to a specific address, including a known data value in the data stream, or both. The token may be activated using an activation code, and a subsequently chosen password may be used to authenticate the mobile computing device to the token each time a hidden command is issued.
Individual	F

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：97110873

※ 申請日期：97 年 3 月 26 日　　※IPC 分類：G06F 12/00 (2006.01)

一、發明名稱：（中文/英文）

隱藏命令協定之記憶卡

MEMORY CARD HIDDEN COMMAND PROTOCOL

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商．泰豐股份有限公司

Tyfone, Inc.

代表人：（中文/英文）

史匹哲湯瑪斯N

SPITZER, THOMAS N.

住居所或營業所地址：（中文/英文）

美國俄勒岡州波特蘭市西南馬卡丹大道 5520 號 250 室

5520 SW Macadam Ave., Suite 250 Portland, OR 97219 U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 3 人）

姓　名：（中文/英文）

1.納廉達西瓦 G/NARENDRA, SIVA G.

2.塔迪帕里波拉伯哈卡爾/TADEPALLI, PRABHAKAR

3.史匹哲湯瑪斯 N/SPITZER, THOMAS N.

IPR2025-00645 Page 00222

國　籍：(中文/英文)

1.美國/USA

2.印度/India

3.美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1.美國；2007 年 3 月 30 日；60/920,932

2.美國；2007 年 8 月 24 日；11/895,629

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

一種記憶卡相容代符(token)，包括使用隱藏在一記憶卡存取命令之資料串流中的命令而所存取的非記憶體組件。一種行動運算裝置，例如行動電話，其藉由寫入一特定位址、含括在該資料串流中一已知的資料值，或兩者皆可的方式，來存取該非記憶體組件。該代符可使用一啟動碼來啟動，且一後續選擇的密碼可用於在每次發出一隱藏命令時認證該行動運算裝置到該代符。

六、英文發明摘要：

A memory card compatible token includes non-memory components accessed using commands hidden in the data stream of a memory card access command. A mobile computing device such as a mobile phone accesses the non-memory components by writing to a specific address, including a known data value in the data stream, or both. The token may be activated using an activation code, and a subsequently chosen password may be used to authenticate the mobile computing device to the token each time a hidden command is issued.

IPR2025-00645 Page 00224

七、指定代表圖：

(一)、本案指定代表圖為：第(6)圖。

(二)、本代表圖之元件代表符號簡單說明：

無元件符號

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

IPR2025-00645 Page 00225

九、發明說明：

【發明所屬之技術領域】

本發明概言之關於通訊協定，尤指一種在行動運算裝置與附加卡之間的通訊協定。

【先前技術】

許多行動運算裝置(例如行動電話)具有記憶卡插槽來容納記憶卡。記憶卡與行動運算裝置之間的通訊協定基本上包括標準化記憶卡存取命令。標準化可增加多種型式與品牌的行動運算裝置與記憶卡之間的互運作性。

【發明內容】

本發明之一態樣，係揭示一種在一記憶卡插槽中操作一代符的方法，包含以下步驟:接收一記憶體存取命令，該記憶體存取命令包括一位址欄位及一資料欄位；比較該資料欄位之至少一部份與一預定的資料值，以決定是否有匹配；如果沒有匹配，根據該記憶體存取命令執行一記憶體存取；及如果有匹配，轉移該記憶體存取命令來進一步解譯。

本發明之另一態樣，係揭示一種具有一機器可讀取媒體之物件，其上儲存有指令，在當存取時使得一機器:將與一記憶體寫入命令一起接收的資料與一預定的資料值相比較，以決定該記憶體寫入命令是否應被解譯成一記憶體寫入命令，或該記憶體寫入命令是否應被解譯成一記憶體寫

IPR2025-00645 Page 00226

入命令之外的一命令。

本發明之另一態樣，係揭示一種具有一機器可讀取媒體之物件，其上儲存有指令，在當存取時使得一機器：將與一記憶體寫入命令一起接收的位址欄位與一預定的位址值相比較，以決定該記憶體寫入命令是否應被解譯成一記憶體寫入命令，或該記憶體寫入命令是否應被解譯成一記憶體寫入命令之外的一命令。

本發明之另一態樣，係揭示一種在一記憶卡介面上與一代符通訊的方法，包含藉由將一資料樣式置於一資料欄位的至少一第一部份的方式，而將欄位置於要被傳送到該記憶卡介面的一記憶體寫入命令中，以將該記憶體寫入命令識別為一為了一記憶體寫入之外的目的而被轉移的命令。

本發明之另一態樣，係揭示一種具有一機器可讀取媒體之物件，其上儲存有指令，在當存取時使得一行動運算裝置：藉由將一資料樣式置於一記憶卡寫入命令之一資料欄位的方式，而存取在一裝置(其耦合至該行動運算裝置之一記憶卡介面)中的一非記憶體控制功能，以將該記憶卡寫入命令識別為一為了一記憶體寫入之外的目的而被轉移的命令。

本發明之另一態樣，係揭示一種記憶卡相容裝置，包含：一主機界面，以接收記憶體寫入命令；一非記憶體控制器組件，其耦合至該主機介面，以解譯包含在該記憶體寫入命令中的資料成為非記憶體相關的命令。

本發明之另一態樣，係揭示一種記憶卡相容裝置，包含：一主機介面，其相容於一行動運算裝置之一記憶卡介面；及一記憶體命令路由組件，其基於要被寫入之資料的至少一部份來解譯記憶卡寫入命令，以決定該記憶卡寫入命令是否必須為了一記憶體寫入之外的目的而被轉移，其中該記憶體命令路由組件被耦合以自該主機介面接收該記憶卡寫入命令。

本發明之另一態樣，係揭示一種記憶卡相容裝置，包含：一主機介面，其相容於一行動運算裝置之一記憶卡介面；及一記憶體命令路由組件，其基於要被寫入之位址的至少一部份來解譯記憶卡寫入命令，以決定該記憶卡寫入命令是否必須為了一記憶體寫入之外的目的而被轉移，其中該記憶體命令路由組件被耦合以自該主機介面接收該記憶卡寫入命令。

本發明之另一態樣，係揭示一種操作一記憶卡相容裝置的方法，包含以下步驟：於該記憶卡相容裝置中一非記憶體控制組件處，接收在一記憶體寫入命令之一資料欄位中的一啟動碼；比較該啟動碼與一已知值來偵測一匹配；及如果有匹配，請求一密碼來用於對一記憶卡相容裝置中該非記憶體控制組件的後續認證。

【實施方式】

在以下的實施方式中，係參照到附屬圖式，藉由例示來顯示一發明的多種具體實施例。這些具體實施例以充份

的細節描述，以使得本技藝專業人士可實施本發明。應瞭解到本發明的多種具體實施例雖有不同，但不需要相互排斥。例如，配合一具體實施例所述的一特定特徵、結構或特性可在其它具體實施例中實施，其皆不背離本發明之精神及範疇。此外，應可瞭解到在每個揭露的具體實施例中個別元件的位置或配置皆可修正，其亦不背離本發明的精神及範疇。因此，以下的實施方式並非採用限制型式，且本發明的範疇僅由附屬申請專利範圍所定義，經過適當解譯(interpretation)，配合該等申請專利範圍所享有之完全範圍的同等者。在圖式中，類似的編號代表若干圖式當中相同或類似的功能。

第 1 圖所示為一行動運算裝置與一記憶卡插槽相容的代符。行動運算裝置 110 在第 1 圖中顯示為一行動電話，但此並非本發明的限制。例如，行動運算裝置 110 可為一個人數位助理(PDA, “Personal digital assistant”)、一智慧型電話、一行動電話、一掌上型電腦、一桌上型電腦、或任何其它能夠如此處所述來操作的裝置。

行動運算裝置 110 包括記憶卡插槽 112。記憶卡插槽 112 為一種能夠容納代符 120 之插槽。例如，記憶卡插槽 112 可具有與代符 120 相容的實體尺寸，並可具有一通訊介面，其使用與代符 120 相容的一協定來運作。在本發明一些具體實施例中，記憶卡插槽 112 為一種記憶卡插槽，其設計成容納記憶卡並與其通訊。如此處所使用者，術語“記憶卡插槽”代表能夠容納具有記憶體的卡片之任何附加

插槽，其可由一行動運算裝置存取，如第 1 圖所示。例如，一記憶卡插槽可相容於一產業標準通訊協定，或可相容於廣泛接受的通訊協定，其必需要正式建檔為一產業標準。範例包括相容於多媒體記憶卡(MMC, "Multimedia Memory Card")協定、記憶棒 DUO 協定、安全數位(SD, "Secure digital")協定、及智慧媒體協定之插槽。先前列表為示例性，並未詳盡列出。記憶卡插槽 112 可相容於除了那些在上述明確列出者外之許多記憶卡插槽協定，其皆不背離本發明的範疇。

代符 120 包括電子接點 122，其可做為一與記憶卡插槽 112 通訊之主機介面之一部份。例如，電子接點 122 可提供相容於記憶卡之通訊協定的連接性。在一些具體實施例中，代符 120 包括一"無接點"(contactless)介面，來與記憶卡插槽 112 通訊。例如，電子代符 120 可包括到記憶卡插槽 112 之一介面，其使用電場或磁場、紅外線(IR, "Infrared")光線、或任何其它適當通訊機制來通訊。

代符 120 可包括記憶體，且亦可包括額外的功能。在一些具體實施例中，代符 120 包括可由行動運算裝置 110 存取的記憶體，且亦包括額外的功能。在其它具體實施例中，代符 120 不包括可由行動運算裝置 110 存取的記憶體。代符 120 的額外功能可採取任何型式，且本發明的多種具體實施例並不限於此方面。

在本發明的多種具體實施例中，在代符 120 中額外的功能可由行動運算裝置 110 使用已經定義給用於記憶卡插

IPR2025-00645 Page 00230

槽 112 中的記憶卡存取命令來存取。因此，本發明的多種具體實施例可致能實施記憶體存取之外的代符功能，而不需要定義新的命令。在一些具體實施例中，該代符的新命令係嵌入在記憶卡讀取/寫入命令之後的資料位元當中。然後代符 120 決定該進入的資料位元是否代表一般的讀取/寫入功能或是新功能。換言之，額外的代符功能可經由該資料串流中的命令“隱藏”來存取，其可使用既有的記憶卡存取命令及功能來交換。根據本發明多種具體實施例，既有的記憶卡功能及新功能皆可不需要改變建構主控協定的方式來實施。

第 2 圖為一行動運算裝置之區塊圖。行動運算裝置 110 包括天線 240、無線電電路 230、處理器 210、記憶體 220 及記憶卡插槽 112。在某些具體實施例中，行動運算裝置 110 為一行動電話、或包括行動電話功能。例如，天線 240 及無線電電路 230 可用於與一胞狀電話網路通訊。再者，於一些具體實施例中，行動運算裝置 110 為一無線區域網路(WLAN, “Wireless local area network”)或無線廣域網路(WWAN, “Wireless wide area network”)裝置。例如，天線 240 及無線電電路 230 可用於與一無線存取點通訊。在某些具體實施例中，天線 240 及無線電電路 230 被省略，且行動運算裝置 110 並未利用無線連接性。

處理器 210 代表能夠與在行動運算裝置 110 中所示之其它區塊進行通訊的一處理器。例如，處理器 210 可為一微處理器、一數位信號處理器(DSP, “Digital signal

IPR2025-00645 Page 00231

processor")、一微控制器或類似者。再者，處理器 210 可由狀態機器或其它連續邏輯來形成。在運作上，處理器 210 可讀取來自記憶體 220 之指令，並對其回應來執行動作。例如，處理器 210 可執行程式指令，其會影響行動運算裝置 110 與耦合至記憶卡插槽 112 之一裝置之間的通訊。

記憶卡插槽 112 係參照第 1 圖做說明。記憶卡插槽 112 包括與代符 120 相容的電路。行動運算裝置 110 藉由使用一標準組合的記憶卡存取命令來與代符 120 通訊。例如，處理器 210 可使用記憶卡寫入命令來寫入到代符 120 中的記憶體，並可使用記憶卡讀取命令來讀取代符 120 中的記憶體。

行動運算裝置 110 可使用嵌入在記憶卡存取命令中的"隱藏"命令來存取代符 120 中額外的功能。例如，一記憶卡寫入命令可包括一唯一的資料字串，以將該記憶卡寫入命令辨別成要轉移之命令，其係為了一記憶體寫入之外的目的。此外，具有該記憶卡寫入命令之區段位址可被設定為一特定位址值，以進一步將該記憶卡寫入命令識別為要轉移的一命令。除了將該記憶卡存取命令識別為除了一記憶體存取之外的目的而要轉移的命令之特定位址/資料值，該記憶體存取命令可包括資料位元來進一步指定隱藏命令之種類及功能。隱藏命令的範例格式在以下進一步說明。在某些具體實施例中，一讀取命令在一寫入命令之後立即發出，以進行由該非記憶卡功能到該主機的資料流，其中該寫入命令的資料具有該隱藏命令。一記憶卡寫入命

令及一記憶卡讀取命令的組合可依此方式使用來形成一隱藏讀取命令。

第 3 圖所示為與在一行動運算裝置中一記憶卡插槽通訊之一代符的一區塊圖。代符 300 包括主機介面 310、命令路由組件 320、記憶體控制組件 340、非記憶體控制組件 330、記憶體 360、及選擇性功能 350。代符 300 可為任何型式的代符，其能夠與一行動運算裝置中一記憶卡插槽進行通訊。再者，代符 300 可採取與一記憶卡插槽相容的任何造型規格。

記憶體 360 可為任何種類的揮發性或非揮發性記憶體。例如，記憶體 360 可為揮發性記憶體，例如靜態隨機存取記憶體(SRAM, "Static random access memory")或動態隨機存取記憶體(DRAM, "Dynamic random access memory")。同時，例如，記憶體 360 可為非揮發性記憶體，例如 NOR FLASH 記憶體或 NAND FLASH 記憶體。在本發明多種具體實施例中，記憶體 360 代表由一行動運算裝置使用為此目的定義之記憶卡存取命令所存取的記憶體。

選擇性功能 350 可包括任何功能，其可被加入到代符 300。如以下的進一步說明，選擇性功能 350 可由一行動運算裝置藉由傳送在一記憶卡存取命令內的隱藏命令來存取。

主機介面 310 包括電子接點來與一記憶卡插槽介接。例如，在某些具體實施例中，主機介面 310 包括接點，例如接點 122(第 1 圖)。同時，例如，在某些具體實施例中，

主機介面 310 包括凹陷的電子接點。主機介面 310 亦可包括電路，例如驅動程式、接收器、終止點等等。

命令路由組件 320 用於按路徑繞送自主機介面 310 接收的記憶卡存取命令。命令可被按路徑繞送到記憶體存取之記憶體控制組件 340，或可被按路徑繞送(轉移)到非記憶體控制組件 330，用於除了記憶體存取之外的目的。例如，當代符 300 與一行動運算裝置中一記憶卡插槽進行通訊，該行動運算裝置可傳送一記憶卡存取命令，藉以存取記憶體 360。同時，例如，該行動運算裝置可傳送包含一隱藏命令之一記憶卡存取命令。命令路由組件 320 偵測該隱藏命令的存在性，並轉移所有或部份的記憶體存取命令到非記憶體控制組件 330。

命令路由組件 320 可用許多方式偵測該隱藏命令。例如，在某些具體實施例中，該記憶卡存取命令可包括一特定位址值或一特定資料值。命令路由組件 320 偵測包括該特定位址值或特定資料值之一或兩者的命令，並適當地按路徑繞送該命令。用於此目的之特定位址值及特定資料值在此處稱之為該隱藏命令位址值及該隱藏命令資料值。

在某些具體實施例中，命令路由組件 320 僅基於該隱藏命令位址值來轉移命令。在這些具體實施例中，命令路由組件 320 檢查包括在記憶卡存取命令中的位址值，並當其匹配該隱藏命令位址值時轉移該命令。在某些具體實施例中，命令路由組件 320 僅基於該隱藏命令資料值來轉移命令。在這些具體實施例中，命令路由組件 320 檢查包括

IPR2025-00645 Page 00234

在記憶卡存取命令中的資料值，並當其匹配該隱藏命令資料值時轉移該命令。在又其它的具體實施例中，命令路由組件 320 同時基於該隱藏命令位址值及該隱藏命令資料值來轉移命令。在這些具體實施例中，命令路由組件 320 僅在當該記憶卡存取位址及資料分別匹配該隱藏命令位址值及資料值時轉移該命令。

該隱藏命令位址值及隱藏命令資料值可用許多方式指定。例如，所有代符可利用固定數值發出。在這些具體實施例中，每次該選擇性功能被存取時，相同的隱藏命令位址及/或資料值係包括在該記憶卡存取命令中。同時，例如，不同的代符可利用唯一數值發出。在這些具體實施例中，每個代符在當查詢時可提供這些數值到一行動運算裝置。同時，例如，隱藏命令位址及/或資料值可由該行動運算裝置所指定。在又其它的具體實施例中，隱藏命令位址及資料值可為動態性。該隱藏命令位址及資料值可在每次施加電力或以一定期基礎來改變。

在本發明多種具體實施例中，命令路由組件 320、記憶體控制組件 340、及非記憶體控制組件用許多不同方式實施。例如，在一些具體實施例中，該多種組件實施在硬體中。在這些具體實施例中，該多種組件可實施成個別的積體電路，或在一組合的積體電路中。同時，例如，在某些具體實施例中，該多種組件可實施在軟體中，或為硬體及軟體之組合。在某些具體實施例中，代符 300 可包括一微處理器，且該等組件可實施成在該微處理器上執行的軟

體模組。在其它具體實施例中，代符 300 可包括多個處理器，且該等組件可實施成分佈在多個處理器上的軟體模組。

第 4 圖所示為根據本發明之多種具體實施例中的代符。代符 400 包括主機介面 310、記憶卡控制器 440、記憶體 360、次級控制器 430、程式記憶體 432、及選擇性功能 350。主機介面 310、記憶體 360 及選擇性功能 350 在上述參照第 3 圖做說明。

在第 4 圖所代表的具體實施例中，記憶卡控制器 440 與使用記憶卡存取命令之行動裝置進行通訊。記憶卡控制器 440 亦與記憶體 360 通訊。記憶卡控制器 440 決定每個命令是否應造成記憶體 360 之記憶體運作，或是否該命令應被轉移到一次級控制器 430。在某些具體實施例中，記憶卡控制器 440 執行儲存在一內部記憶體或儲存在記憶體 360 中的指令。在某些具體實施例中，記憶卡控制器 440 包括特殊目的硬體，用於決定一命令是否應被轉移。在其它具體實施例中，記憶卡控制器 440 可為一微控制器，其在所有方面中與在記憶卡中找到的一控制器相同，除了其所執行的程式之外。

次級控制器 430 接收由記憶卡控制器 440 轉移的隱藏命令。次級控制器 430 另解譯該隱藏命令，並依回應來執行動作。例如，次級控制器 430 可命令選擇性功能 350 來提供一服務。次級控制器 430 執行儲存在程式記憶體 432 中的指令。在某些具體實施例中，程式記憶體 432 係嵌入在次級控制器 430 中，且在其它具體實施例中，程式記憶

IPR2025-00645 Page 00236

體 432 為記憶體 360 的一部份。

在第 4 圖代表的具體實施例中，記憶卡控制器 440 同時包括命令路由組件 320 及記憶體控制組件 340(第 3 圖)之功能，而次級控制器 430 包括非記憶體控制組件 330 之功能(第 3 圖)。在其它具體實施例中，次級控制器 430 與主機介面 310 及記憶卡控制器 440 進行通訊，並包括該命令路由組件之功能。

第 5 圖所示為一記憶卡寫入命令之資料部份。所包括的為隱藏命令資料值 510、狀態欄位 520、密碼欄位 530、裝置 ID 532、命令索引 540、及隱藏命令相關的資料 550。在第 5 圖的範例中，該資料部份長度為 512 位元組，且此並非本發明的限制。任何數量的資料可被包括在該寫入命令中，且第 5 圖所示的每個欄位可為任何長度。

在第 5 圖的範例中，該隱藏命令資料值為 256 位元長，且其可使用任何長度，皆未背離本發明的範疇。在一些具體實施例中，隱藏命令資料值 510 係用於將一記憶體寫入命令識別為一隱藏命令。當接收一具有在前 256 位元中之資料(其匹配該隱藏命令資料值)的寫入命令時，則將該命令識別成為了除了一記憶體寫入之外的目的而要轉移的一命令。如上所述，一隱藏命令位址值可配合用於或除了一隱藏命令資料值外，以識別該記憶體寫入命令成為一隱藏命令。

當該記憶體寫入為一隱藏命令時，其餘的欄位具有意義。例如，如果前 256 位元未匹配該隱藏命令資料值(或如

IPR2025-00645 Page 00237

果該寫入位址並不匹配該隱藏命令位址值或兩者)，在該資料欄位中其餘的位元係要視為在一正常記憶體寫入命令中的資料。相反地，當該記憶體寫入為一隱藏命令時，其餘的欄位係用於進一步解譯該隱藏命令。

命令路由組件 320(第 3 圖)檢查該隱藏命令資料值 510、狀態欄位 520、及可能的密碼欄位 530 及裝置 ID 532。如果該命令被識別成一隱藏命令時，命令路由組件 320 轉送密碼 530、命令索引 540 及相關資料 550 到非記憶體控制組件 330。

狀態欄位 520 可包括關於該隱藏命令之狀態的任何資訊。例如，狀態欄位 520 可包括一個以上的位元來對命令路由組件 320 指明該主機(行動運算裝置)是否預期該非記憶體控制組件會因應於該隱藏命令來傳回資料。例如，當狀態欄位 520 指示一寫入時，命令路由組件 320 轉送密碼裝置 ID、命令索引及相關的資料，而不預期會傳回任何資料到該主機。同時，例如，當狀態欄位 520 指明一讀取時，命令路由組件 320 轉送該密碼、裝置 ID、命令索引及相關的資料，其預期非記憶體控制組件 330 將因應於一記憶卡讀取命令，而提供被傳送到該主機之資料。在一記憶卡寫入命令之後即刻跟隨著一記憶卡讀取命令之組合可用於提供“讀取”功能到該非記憶體控制組件。來自該非記憶體控制組件之讀取作業在以下參照第 8 圖進一步說明。

密碼欄位 530 包括一密碼來允許非記憶體控制組件 330 來認證該主機到該代符。在某些具體實施例中，每一

個隱藏命令包括一密碼。每次該密碼、裝置ID、命令索引、及相關資料被轉移到該非記憶體控制組件，該密碼被檢查來認證該主機到該代符。

裝置ID 532唯一地識別該主機(行動運算裝置)。該裝置ID可由該非記憶體控制組件檢查，以確保該代符被插入到其所認證的該主機中。本發明的某些具體實施例使用該裝置ID強制一唯一主機/代符配對，且其它具體實施例允許非記憶體控制功能被任何主機來存取。

命令索引540識別隱藏命令的種類。可能之隱藏命令的數目僅受限於其所配置的位元數目。任何數目的位元可被配置到命令索引540，其並未背離本發明的範疇。隱藏命令相關的資料550可對每種隱藏命令來不同地利用。任何數目的位元可用於隱藏命令相關的資料550。

第5圖所示的資料係提供為一範例，一記憶卡存取命令之資料欄位可包括比第5圖所示之那些更多或更少的資料欄位。本發明並不限於在一記憶卡存取命令中欄位的數目或內容。

第6圖所示為根據本發明之多種具體實施例中的流程圖。在一些具體實施例中，方法600可由一行動運算裝置使用，來與在一記憶卡插槽中一代符進行通訊。在某些具體實施例中，方法600或其部份由一具有一記憶卡插槽的行動運算裝置來執行，且在其它具體實施例中，方法600或其部份係由軟體執行。方法600中的各種動作可由所呈現之順序、或按不同的順序或是同時地來執行。再者，在

IPR2025-00645 Page 00239

某些具體實施例中，第 6 圖所列出的一些動作由方法 600 中省略。

方法 600 開始於 610，其中一資料樣式(data pattern)及一位址值於一記憶卡插槽中之一裝置所接收。該資料樣式對應於該隱藏命令資料值，且該位址值對應於該隱藏命令位址值。在某些具體實施例中，該行動裝置僅接收該資料值，且在其它具體實施例中，該行動裝置僅接收該位址值。在某些具體實施例中，610 的動作在當該裝置第一次插入在該記憶卡插槽中時發生一次。然後該行動運算裝置在當每次它產生一隱藏命令時可使用該位址及資料值。在其它具體實施例中，610 的動作可在當每次該裝置被插入到該記憶體插槽中時發生。在又其它的具體實施例中，610 的動作可定期地發生。每次發生動作 610 時，該資料樣式可以相同或不同，且該位址值可為相同或不同。

在 620 中，一記憶卡存取命令之一資料欄位被置入該資料樣式，以造成該命令除了一記憶體存取之外的目的而被轉移。例如，該資料樣式可被寫入到該資料欄位做為該隱藏命令資料值 510(第 5 圖)。

在 630 中，該記憶卡存取命令之一位址欄位被置入該位址值，以進一步造成該命令除了一記憶體存取之外的目的而被轉移。在某些具體實施例中，僅 620 或 630 之一被利用。在這些具體實施例中，一隱藏命令之存在性由該資料樣式單獨或該位址值單獨指明。

在 640 中，該記憶卡存取命令之資料欄位被置入一命

IPR2025-00645 Page 00240

令字串，以指定除了一記憶卡存取之外的目的。例如，該命令字串可被寫入到該資料欄位，做為該非記憶體控制組件之命令索引 540。

在 650 中，一記憶卡存取命令之資料欄位被置入一密碼，以認證存取到耦合至該記憶卡插槽之該裝置。在某些具體實施例中，一密碼被包括在每一個隱藏命令之資料欄位中。在其它具體實施例中，一密碼僅包括在一交換的開始處。

在 660 中，該記憶卡存取命令被傳送到耦合至該記憶卡插槽之裝置。例如，一行動運算裝置(第 1 圖 110)可傳送該記憶卡存取命令到一記憶卡插槽(第 1 圖 112)中一代符(第 1 圖 120)。該代符可包括一命令路由組件(第 3 圖 320)來基於在方法 600 中置入的該等資料欄位來轉移該命令。

第 7 圖所示為根據本發明之多種具體實施例中的流程圖。在某些具體實施例中，方法 700 可由在一記憶卡插槽中的代符所使用。在某些具體實施例中，方法 700 或其部份係由一代符內一命令路由組件來執行，且在其它具體實施例中，方法 700 或其部份係由軟體執行。方法 700 中的多種動作可由所呈現之順序、或按不同的順序或同時地來執行。再者，在某些具體實施例中，第 7 圖所列出的一些動作從方法 700 中省略。

方法 700 開始於 710，其中一記憶卡存取命令經由一主機介面自一行動運算裝置接收。710 的動作對應於接收一記憶卡存取命令之一行動運算裝置的一記憶卡插槽中的

一代符。

在 720 中，該代符檢查在該記憶卡存取命令中的條件，以決定是否該記憶卡存取命令應為了其它目的被轉移。該條件可為一隱藏命令資料值、一隱藏命令位址值或兩者之一或兩者。如果在 730 中有一條件可匹配，即存在一隱藏命令，且該記憶卡存取命令之至少一部份於 740 中轉移。如果沒有匹配的條件，即不存在隱藏命令，且一記憶體存取在 750 中執行。

第 8 圖所示為根據本發明之多種具體實施例中的流程圖。在某些具體實施例中，方法 800 可由在一記憶卡插槽中的代符所使用。在某些具體實施例中，方法 800 或其部份係由一代符內一命令路由組件來執行，且在其它具體實施例中，方法 800 或其部份係由軟體執行。方法 800 中的多種動作可由所呈現之順序、不同的順序或同時地來執行。再者，在某些具體實施例中，第 8 圖所列出的一些動作從方法 800 中省略。

方法 800 開始於 810，其中一記憶卡寫入命令係經由一主機介面而自一行動運算裝置接收。如果該記憶卡寫入命令被決定為一隱藏命令，程序繼續到 840；否則，一記憶體寫入在 830 中執行。

在 840 中，該隱藏命令被轉移到一非記憶體控制組件。如果在 850 中該隱藏命令被決定為一“讀取”時，程序繼續到 860；否則，該隱藏命令程序即完成。在 860 中，該命令路由組件由該非記憶體控制組件取得非記憶體資

IPR2025-00645 Page 00242

料，且於 870 中，一記憶卡讀取命令由該行動運算裝置接收。在 880 中，該非記憶體資料即傳回到該行動運算裝置。

方法 800 說明一行動運算裝置如何能夠執行自一選擇性功能或自一非記憶體控制組件的讀取。該行動運算裝置發出一具有一隱藏命令之記憶卡寫入命令，該隱藏命令包含指定一讀取之一狀態欄位，然後該行動運算裝置發出一記憶卡讀取命令。在該卡中的程序接收該隱藏命令，將其識別為一讀取，然後因應於一後續記憶卡讀取命令來傳回資料到該行動運算裝置。

第 9 圖所示為認證一行動運算裝置到一代符中一或多個功能的方法。方法 900 開始於區塊 910，其中在一代符處接收來自一行動運算裝置的一啟動碼。在 920 中，該接收的啟動碼係相較於儲存在該代符中的碼。如果該啟動碼匹配時，該代符接收來自該行動運算裝置之一密碼，如 940，並儲存該密碼在該代符中於稍後使用，如 950。如果該啟動碼並不匹配時，該代符決定是否已經超過可允許的嘗試次數，如 960。如果該可允許嘗試的數目已經超過時，則於步驟 970 接觸該代符發出者，且如果該可允許嘗試的數目並未超過時，該方法即重複，直到該啟動碼匹配，或是已經超過可允許嘗試的數目之後。

方法 900 可在當一代符被發出給一使用者時來執行。該使用者可具有一啟動碼，以“啟動”該代符。當該使用者成功地輸入該啟動碼，該使用者被提示一密碼，且該密碼即被儲存來用於未來的隱藏命令中。

IPR2025-00645 Page 00243

在某些具體實施例中，在一代符中的多種非記憶體功能使用方法 900 來認證。例如，每一個多個非記憶體功能可以具有儲存的啟動碼，且每一個被分別啟動。每一個個別啟動的功能可具有一不同的密碼，或該多個功能可共享一密碼。

【圖式簡單說明】

第 1 圖顯示一行動運算裝置與一記憶卡插槽相容的代符；

第 2 圖為一行動運算裝置之區塊圖；

第 3 圖及第 4 圖為與行動運算裝置中記憶卡插槽通訊之代符的區塊圖；

第 5 圖為一記憶卡寫入命令之資料部份；及

第 6 圖至第 9 圖為根據本發明多種具體實施例之方法的流程圖。

【主要元件符號說明】

110 行動運算裝置
112 記憶卡插槽
120 代符
122 電子接點
210 處理器
220 記憶體
230 無線電電路
240 天線
300 代符
310 主機介面
320 命令路由組件
330 非記憶體控制組件
340 記憶體控制組件
350 選擇性功能

IPR2025-00645 Page 00244

360 記憶體
400 代符
430 次級控制器
432 程式記憶體
440 記憶卡控制器
510 隱藏命令資料值
520 狀態欄位
530 密碼欄位
532 裝置識別
540 命令索引
550 隱藏命令相關資料

IPR2025-00645 Page 00245

十、申請專利範圍：

1. 一種在一記憶卡插槽中操作一代符的方法，包含以下步驟：

接收一記憶體存取命令，該記憶體存取命令包括一位址欄位及一資料欄位；

比較該資料欄位之至少一部份與一預定的資料值，以決定是否有匹配；

如果沒有匹配，根據該記憶體存取命令執行一記憶體存取；及

如果有匹配，轉移該記憶體存取命令來進一步解譯。

2. 如申請專利範圍第1項所述之方法，另包含比較該位址欄位與一預定位址值以決定是否有一位址匹配，並僅在當亦有一位址匹配時才轉移該記憶體存取命令。

3. 如申請專利範圍第1項所述之方法，其中轉移該記憶體存取命令之步驟包含傳送該資料欄位的至少一部份到一非記憶體控制器組件來進一步解譯。

4. 如申請專利範圍第3項所述之方法，另包含自該資料欄位讀取一密碼，以認證存取到該非記憶體控制器組件。

5. 一種具有一機器可讀取媒體之物件，其上儲存有指令，在當存取時使得一機器：

將與一記憶體寫入命令一起接收的資料與一預定的資料值相比較，以決定該記憶體寫入命令是否應被

IPR2025-00645 Page 00246

解譯成一記憶體寫入命令，或該記憶體寫入命令是否應被解譯成一記憶體寫入命令之外的一命令。

6. 如申請專利範圍第5項所述之物件，其中該等指令在當存取時另使得該機器在該記憶體寫入命令應被解譯成一記憶體寫入命令時，轉送該記憶體寫入命令到一記憶體控制器組件。

7. 如申請專利範圍第5項所述之物件，其中該等指令在當存取時另使得該機器在該記憶體寫入命令應被解譯成一記憶體寫入命令之外的一命令時，轉送該記憶體寫入命令到一非記憶體控制器組件。

8. 一種具有一機器可讀取媒體之物件，其上儲存有指令，在當存取時使得一機器：

將與一記憶體寫入命令一起接收的位址欄位與一預定的位址值相比較，以決定該記憶體寫入命令是否應被解譯成一記憶體寫入命令，或該記憶體寫入命令是否應被解譯成一記憶體寫入命令之外的一命令。

9. 一種在一記憶卡介面上與一代符通訊的方法，包含藉由將一資料樣式置於一資料欄位的至少一第一部份的方式，而將欄位置於要被傳送到該記憶卡介面的一記憶體寫入命令中，以將該記憶體寫入命令識別為一為了一記憶體寫入之外的目的而被轉移的命令。

10. 如申請專利範圍第9項所述之方法，另包含在置入該等欄位之前，接收來自耦合至該記憶卡介面之代符的該資料樣式的一複本。

11. 如申請專利範圍第9項所述之方法，另包含將一位址值置於一位址欄位，以另將該記憶體寫入命令識別為一為了一記憶體寫入之外的目的而被轉移的命令。

12. 如申請專利範圍第9項所述之方法，另包含將一命令索引置於該資料欄位的一第二部份，以指定除了一記憶體寫入之外的目的。

13. 如申請專利範圍第9項所述之方法，另包含將一密碼置於該資料欄位的一第二部份，以認證存取到耦合至該記憶卡介面之代符。

14. 如申請專利範圍第9項所述之方法，另包含：

在發出該記憶體寫入命令到耦合至該記憶卡介面之代符之後，接著發出一記憶體讀取命令到耦合至該記憶卡介面之代符。

15. 一種具有一機器可讀取媒體之物件，其上儲存有指令，在當存取時使得一行動運算裝置：

藉由將一資料樣式置於一記憶卡寫入命令之一資料欄位的方式，而存取在一裝置(其耦合至該行動運算裝置之一記憶卡介面)中的一非記憶體控制功能，以將該記憶卡寫入命令識別為一為了一記憶體寫入之外的目的而被轉移的命令。

16. 如申請專利範圍第15項所述之物件，其中該等指令在當存取時另使得該行動運算裝置將一密碼置於該資料欄位，以認證存取到耦合至該記憶卡介面之裝置。

17. 如申請專利範圍第15項所述之物件，其中該等指令在

當存取時另使得該行動運算裝置將一命令索引置於該資料欄位，以指定除了一記憶體寫入之外的目的。

18. 一種記憶卡相容裝置，包含：

一主機界面，以接收記憶體寫入命令；

一非記憶體控制器組件，其耦合至該主機介面，以解譯包含在該記憶體寫入命令中的資料成為非記憶體相關的命令。

19. 如申請專利範圍第 18 項所述之記憶卡相容裝置，另包含：

非揮發性記憶體；

一記憶體控制器組件，其耦合至該非揮發性記憶體；及

一記憶體命令路由組件，其耦合至該主機介面及該非記憶體控制器組件，該記憶體命令路由組件包括邏輯，其基於含括在該記憶體寫入命令中的資料，來決定是否要按路徑繞送一記憶體寫入命令到該記憶體控制器或是該非記憶體控制器。

20. 一種記憶卡相容裝置，包含：

一主機介面，其相容於一行動運算裝置之一記憶卡介面；及

一記憶體命令路由組件，其基於要被寫入之資料的至少一部份來解譯記憶卡寫入命令，以決定該記憶卡寫入命令是否必須為了一記憶體寫入之外的目的而被轉移，其中該記憶體命令路由組件被耦合以自該主

機介面接收該記憶卡寫入命令。

21. 如申請專利範圍第20項所述之記憶卡相容裝置，另包含：

一記憶體控制器組件，其被耦合以自該記憶體命令路由組件接收記憶體寫入命令。

22. 如申請專利範圍第20項所述之記憶卡相容裝置，另包含：

一非記憶體控制器組件，其被耦合以自該記憶體命令路由組件接收轉移的記憶體寫入命令。

23. 一種記憶卡相容裝置，包含：

一主機介面，其相容於一行動運算裝置之一記憶卡介面；及

一記憶體命令路由組件，其基於要被寫入之位址的至少一部份來解譯記憶卡寫入命令，以決定該記憶卡寫入命令是否必須為了一記憶體寫入之外的目的而被轉移，其中該記憶體命令路由組件被耦合以自該主機介面接收該記憶卡寫入命令。

24. 一種操作一記憶卡相容裝置的方法，包含以下步驟：

於該記憶卡相容裝置中一非記憶體控制組件處，接收在一記憶體寫入命令之一資料欄位中的一啟動碼；

比較該啟動碼與一已知值來偵測一匹配；及

如果有匹配，請求一密碼來用於對一記憶卡相容裝置中該非記憶體控制組件的後續認證。

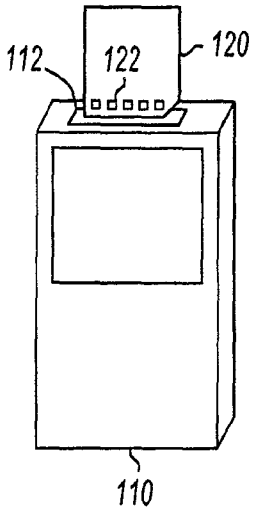
IPR2025-00645 Page 00250

25. 如申請專利範圍第24項所述之方法，另包含接收隱藏在記憶體寫入命令之資料欄位中的非記憶體相關命令，其中該等非記憶體相關命令包括該密碼。

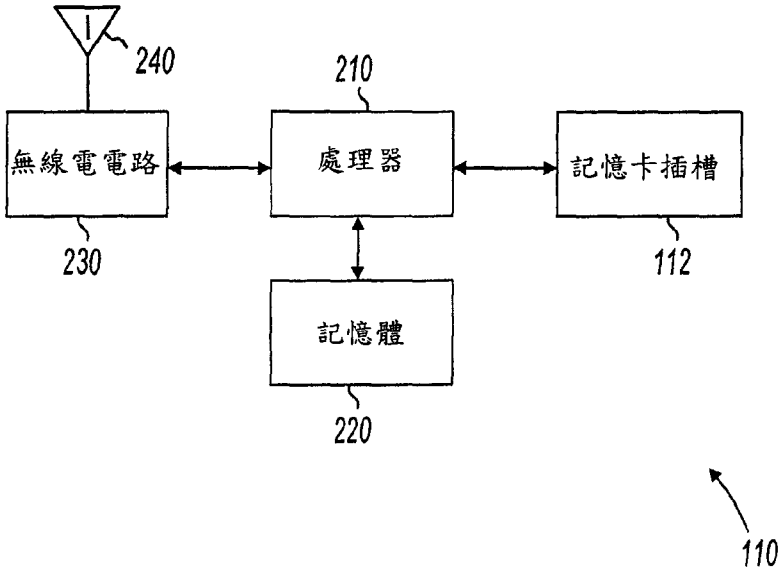
26. 如申請專利範圍第24項所述之方法，另包含接收複數個啟動碼，其中該複數啟動碼中每一個對應於在該記憶卡相容裝置中一不同非記憶體控制組件的啟動。

IPR2025-00645 Page 00251

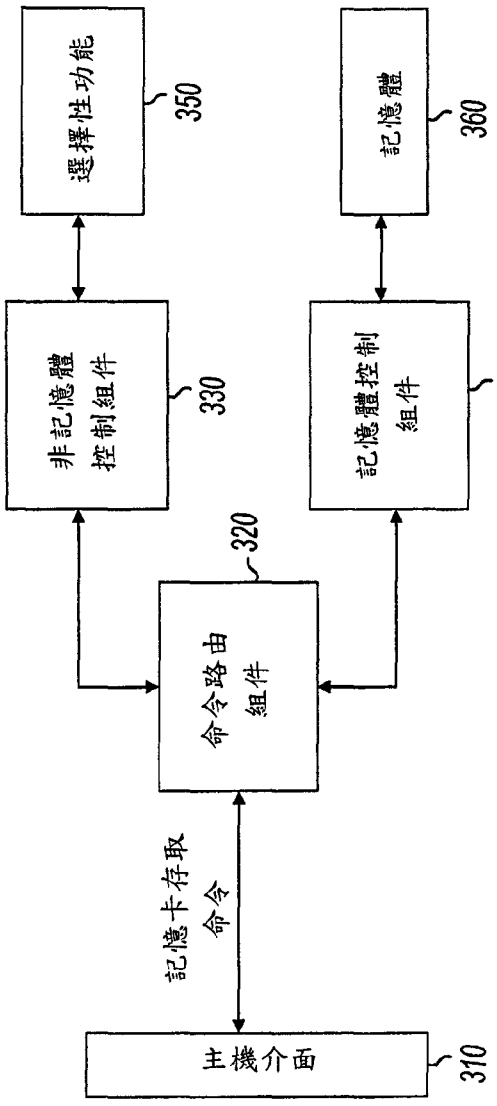
十一、圖式：



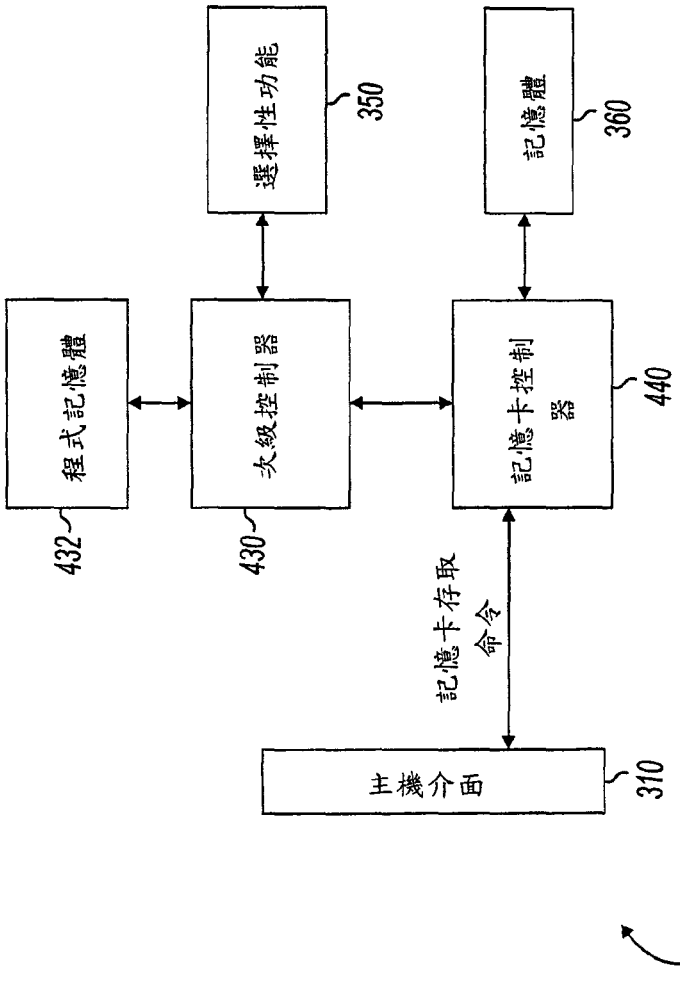
第 1 圖



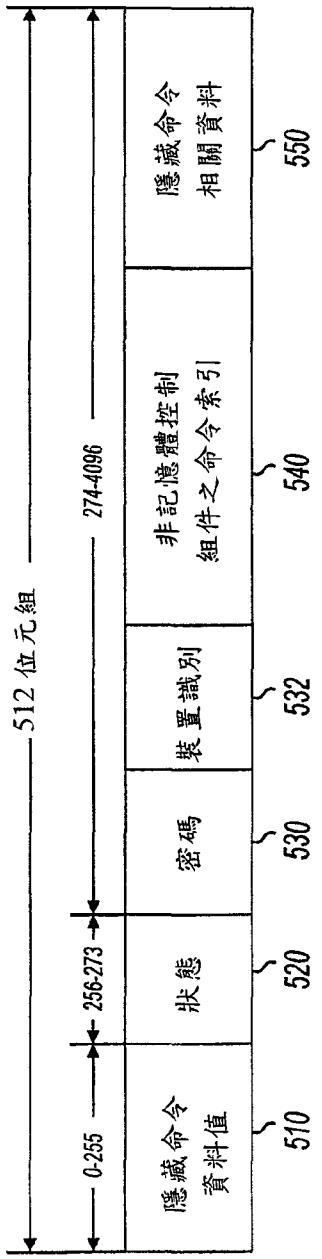
第 2 圖


主機介面
310
記憶卡存取命令
命令路由組件
320
非記憶體控制組件
330
記憶體控制組件
340
選擇性功能
350
記憶體
360
300

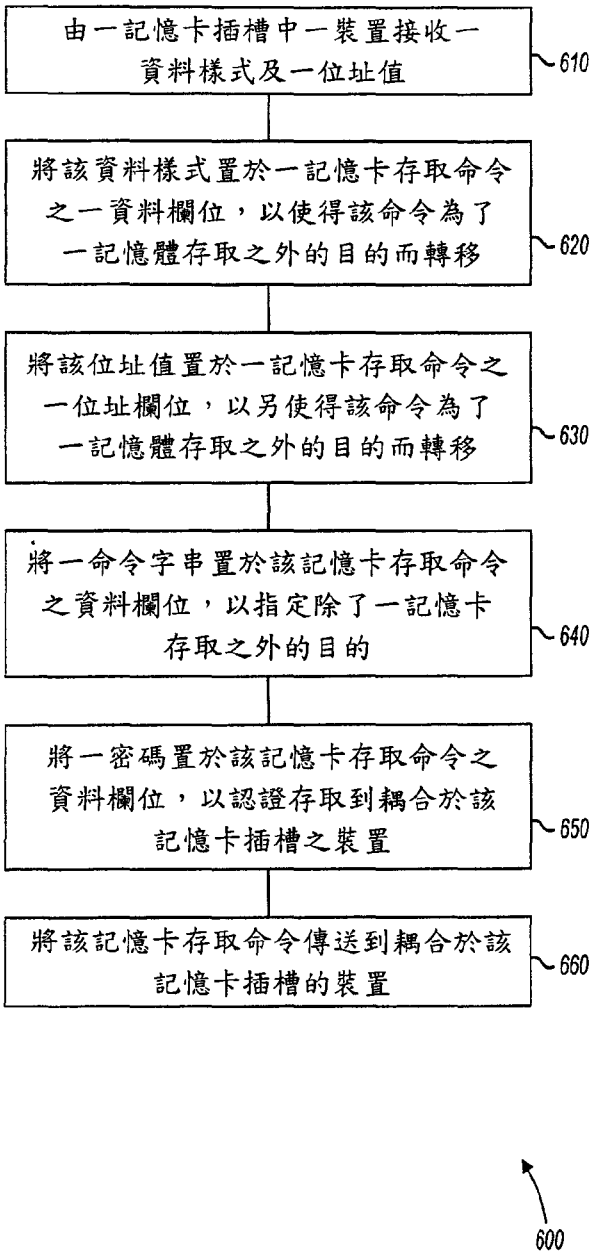
第 3 圖


選擇性功能
350
記憶體
360
程式記憶體
次級控制器
記憶卡控制器
440
432
430
記憶卡存取命令
主機介面
310
400

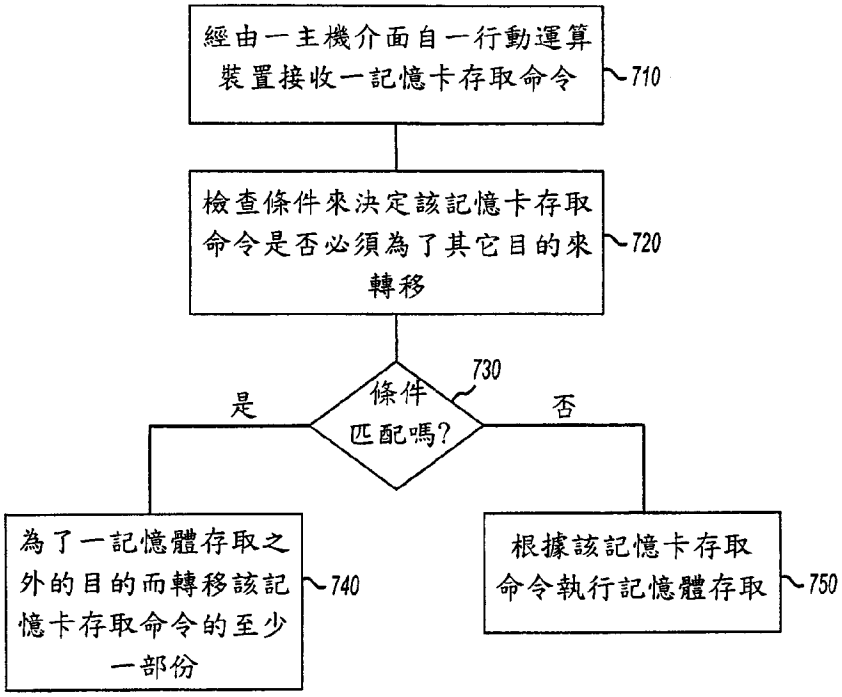
第 4 圖


512 位元組
0-255
256-273
274-4096
隱藏命令資料值
510
狀態
520
密碼
530
裝置識別
532
非記憶體控制組件之命令索引
540
隱藏命令相關資料
550

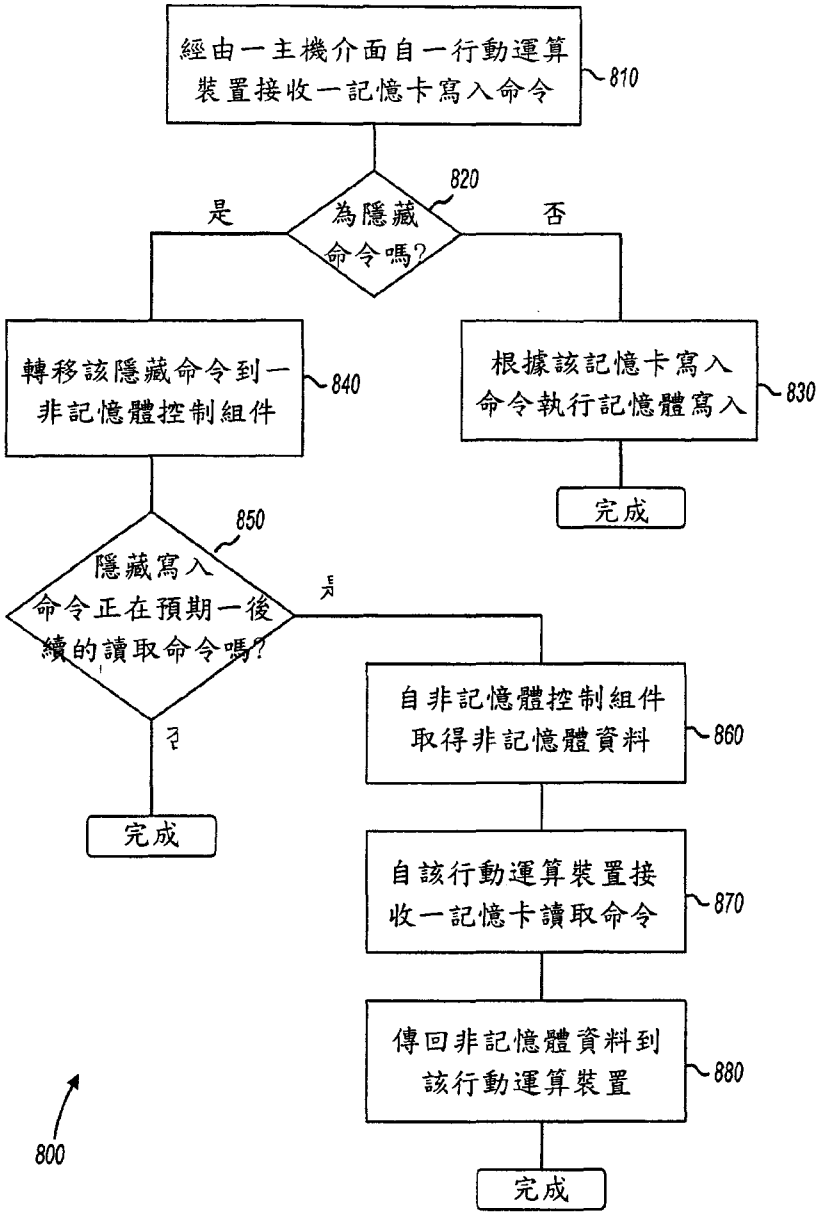
第 5 圖


由一記憶卡插槽中一裝置接收一資料樣式及一位址值
610
將該資料樣式置於一記憶卡存取命令之一資料欄位，以使得該命令為了一記憶體存取之外的目的而轉移
620
將該位址值置於一記憶卡存取命令之一位址欄位，以另使得該命令為了一記憶體存取之外的目的而轉移
630
將一命令字串置於該記憶卡存取命令之資料欄位，以指定除了一記憶卡存取之外的目的
640
將一密碼置於該記憶卡存取命令之資料欄位，以認證存取到耦合於該記憶卡插槽之裝置
650
將該記憶卡存取命令傳送到耦合於該記憶卡插槽的裝置
660
600

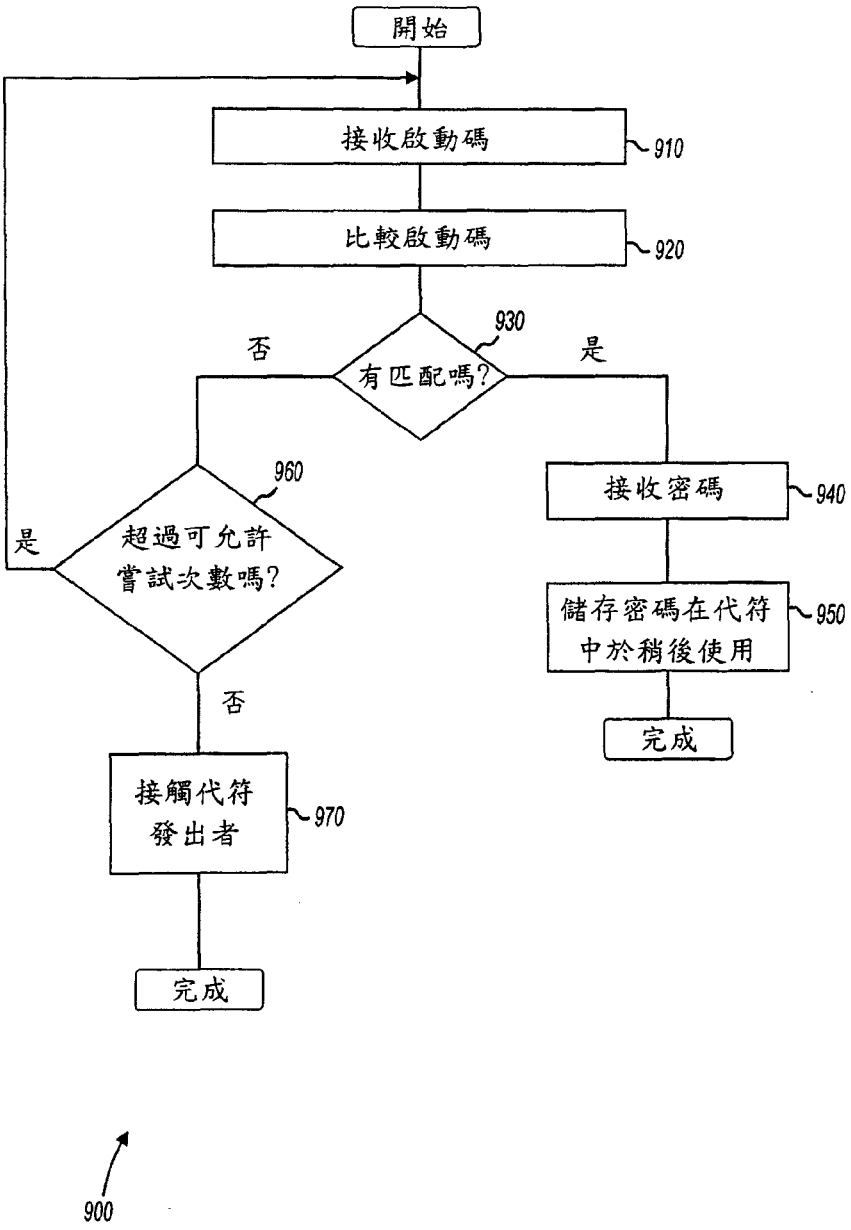
第 6 圖


經由一主機介面自一行動運算裝置接收一記憶卡存取命令
710
檢查條件來決定該記憶卡存取命令是否必須為了其它目的來轉移
720
730
條件匹配嗎?
是
否
為了一記憶體存取之外的目的而轉移該記憶卡存取命令的至少一部份
740
根據該記憶卡存取命令執行記憶體存取
750

第 7 圖


經由一主機介面自一行動運算裝置接收一記憶卡寫入命令
810
為隱藏命令嗎?
820
是
否
轉移該隱藏命令到一非記憶體控制組件
840
根據該記憶卡寫入命令執行記憶體寫入
830
完成
隱藏寫入命令正在預期一後續的讀取命令嗎?
850
是
否
自非記憶體控制組件取得非記憶體資料
860
自該行動運算裝置接收一記憶卡讀取命令
870
傳回非記憶體資料到該行動運算裝置
880
完成
800

第 8 圖


開始
接收啟動碼
910
比較啟動碼
920
930
有匹配嗎?
否
是
960
超過可允許
嘗試次數嗎?
是
否
接收密碼
940
儲存密碼在代符
中於稍後使用
950
完成
接觸代符
發出者
970
完成
900

第 9 圖

Biblio

[Print]

Patent/Publication Number	201023662
Title	Power negotiation for small RFID card
Issued/Publication Date	2010/06/16
Application Date	2009/08/06
Application Number	098126588
IPC	H04W-024/00(2009.01)
Inventor	NARENDRA, SIVA G. IN; TADEPALLI, PRABHAKAR IN; CHAKRABORTY, SAURAV IN
Applicant	TYFONE, INC.US
Priority Number	20080808US20080188382
Abstract	A memory card compatible RFID card includes a smartcard controller that receives power from a host device. The RFID card also includes a small inductive device capable of inductive coupling with an RFID reader. The small inductive device is small enough to fit in the form factor of a memory card. Commands may be sent to the RFID card to keep the RFID card powered.
Individual	F

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201023662 A1

(43)公開日： 中華民國 99 (2010) 年 06 月 16 日

(21)申請案號：098126588 (22)申請日： 中華民國 98 (2009) 年 08 月 06 日

(51)Int. Cl.： *H04W24/00 (2009.01)*

(30)優先權：2008/08/08 美國 12/188,382

(71)申請人：泰豐股份有限公司 (美國) TYFONE, INC. (US)
美國

(72)發明人：納廉達西瓦G NARENDRA, SIVA G. (IN) ；塔迪帕里波拉伯哈卡爾 TADEPALLI, PRABHAKAR (IN) ；伽拉柏堤索瑞 CHAKRABORTY, SAURAV (IN)

(74)代理人：蔡坤財；李世章

申請實體審查：有 申請專利範圍項數：19 項 圖式數：13 共 50 頁

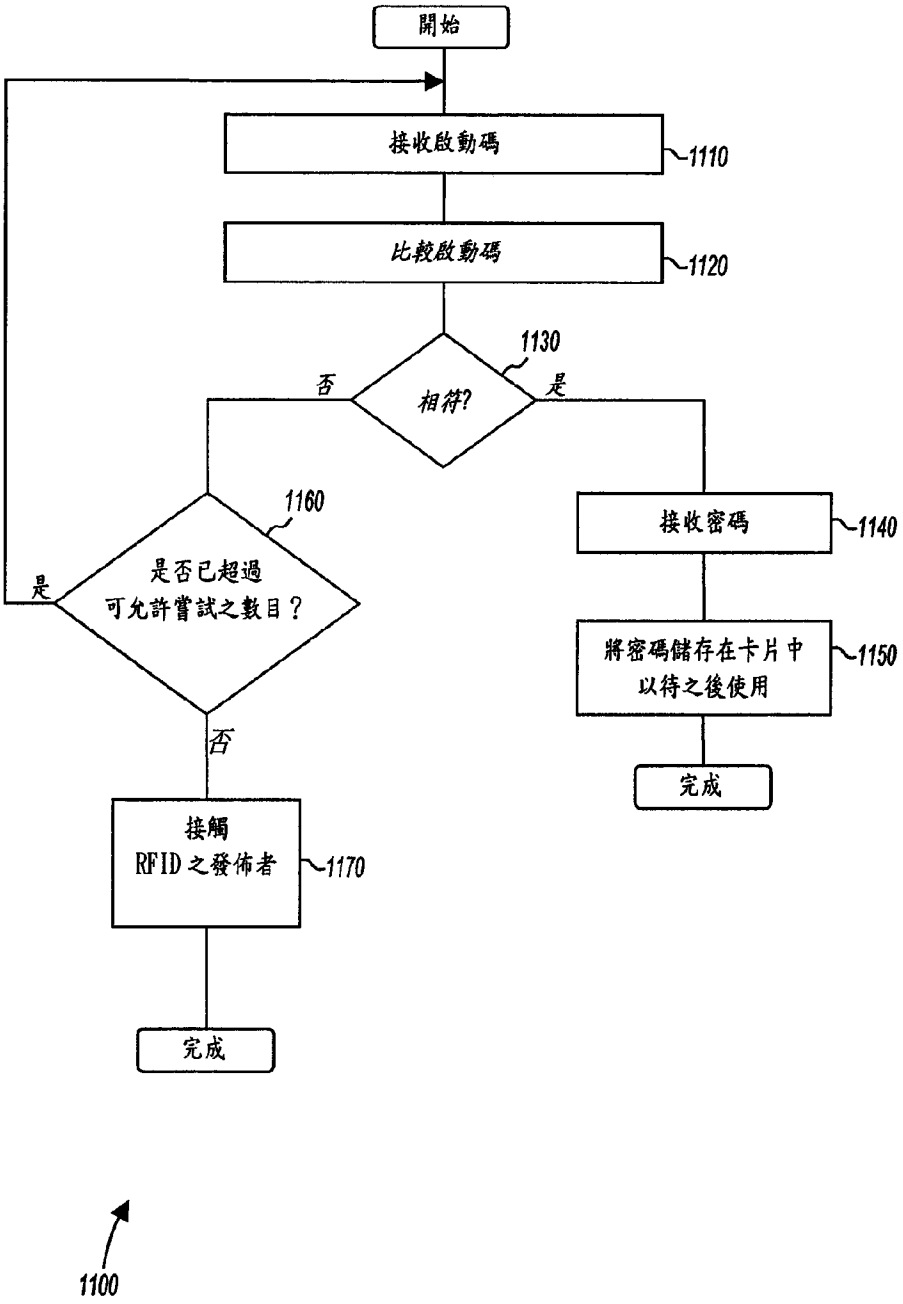
(54)名稱

用於小型ＲＦＩＤ卡的功率協商

POWER NEGOTIATION FOR SMALL RFID CARD

(57)摘要

一種相容於記憶卡之 RFID 卡包括一智慧卡控制器，其能從一主機裝置端接收電力。RFID 卡亦可包括一小型感應裝置，其能夠與一 RFID 讀取器感應式耦接。該小型感應裝置是小到足以與記憶卡的結構因數(form factor)相稱。命令可被傳送到 RFID 卡以讓 RFID 卡維持供電狀態。


開始
接收啟動碼
1110
比較啟動碼
1120
1130
相符?
否
是
1160
是否已超過
可允許嘗試之數目?
是
否
接收密碼
1140
將密碼儲存在卡片中
以待之後使用
1150
完成
接觸
RFID之發佈者
1170
完成
1100

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201023662 A1

(43)公開日： 中華民國 99 (2010) 年 06 月 16 日

(21)申請案號：098126588 (22)申請日： 中華民國 98 (2009) 年 08 月 06 日

(51)Int. Cl.： *H04W24/00 (2009.01)*

(30)優先權：2008/08/08 美國 12/188,382

(71)申請人：泰豐股份有限公司 (美國) TYFONE, INC. (US)
美國

(72)發明人：納廉達西瓦G NARENDRA, SIVA G. (IN) ；塔迪帕里波拉伯哈卡爾 TADEPALLI, PRABHAKAR (IN) ；伽拉柏堤索瑞 CHAKRABORTY, SAURAV (IN)

(74)代理人：蔡坤財；李世章

申請實體審查：有 申請專利範圍項數：19 項 圖式數：13 共 50 頁

(54)名稱

用於小型ＲＦＩＤ卡的功率協商

POWER NEGOTIATION FOR SMALL RFID CARD

(57)摘要

一種相容於記憶卡之 RFID 卡包括一智慧卡控制器，其能從一主機裝置端接收電力。RFID 卡亦可包括一小型感應裝置，其能夠與一 RFID 讀取器感應式耦接。該小型感應裝置是小到足以與記憶卡的結構因數(form factor)相稱。命令可被傳送到 RFID 卡以讓 RFID 卡維持供電狀態。

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：98126588

※ 申請日期：2009 年 8 月 6 日　　※IPC 分類：

H04W 24/00 (2009.01)

一、發明名稱：（中文/英文）

用於小型 RFID 卡的功率協商

POWER NEGOTIATION FOR SMALL RFID CARD

二、中文發明摘要：

一種相容於記憶卡之 RFID 卡包括一智慧卡控制器，其能從一主機裝置端接收電力。RFID 卡亦可包括一小型感應裝置，其能夠與一 RFID 讀取器感應式耦接。該小型感應裝置是小到足以與記憶卡的結構因數(form factor)相稱。命令可被傳送到 RFID 卡以讓 RFID 卡維持供電狀態。

三、英文發明摘要：

A memory card compatible RFID card includes a smartcard controller that receives power from a host device. The RFID card also includes a small inductive device capable of inductive coupling with an RFID reader. The small inductive device is small enough to fit in the form factor of a memory card. Commands may be sent to the RFID card to keep the RFID card powered.

IPR2025-00645 Page 00264

四、指定代表圖：

(一)本案指定代表圖為：第（11）圖。

(二)本代表圖之元件符號簡單說明:

無

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

IPR2025-00645 Page 00265

六、發明說明：

【發明所屬之技術領域】

本發明通常係有關於無接觸之通訊裝置，而更具體而言之，是指小型無線射頻識別(RFID)卡。

【先前技術】

RFID「標籤」(tags)可被分成兩個寬廣的範疇：主動標籤以及被動標籤。主動標籤之特徵為一區域電力來源，像是電池。主動標籤通常藉由在 RF 載波頻率之選擇上進行廣播之方式來傳輸資訊，其中 RF 載波頻率之選擇係使用用一區域產生之 RF 載波。主動標籤一般是用來在長距離上傳輸，通常被稱為「遠場通訊」(far field communications, FFC)。採用主動 RFID 標籤之天線有做的較大的傾向，以允許在長距離上之通訊。

被動標籤則未被供電。被動標籤能從一訊問(interrogating)RF 場中取得供給該標籤所需之能源，並藉由調變該阻抗(其為天線呈現給該訊問場之阻抗)之方式使用那能源來傳輸回應碼，借此調變該反射回到讀取天線之訊號。被動標籤一般用來在短距離上傳輸，通常被稱為「近場通訊」(near field communications, NFC)。例如，運作在 13.56MHz 的被動標籤一般被設計成能在距若干公分遠的距離與 RFID 讀取器通訊。

被動元件一般係連接到「迴路天線」(loop antennas)。

IPR2025-00645 Page 00266

迴路天線之範例係如於 2003 年 5 月 27 日授與 Carpier 以及其他人之美國專利號：6,568,600 中所示。在美國 6,568,600 號專利中所描述之裝置可被認為是「信用卡尺寸」的被動式 RFID 卡（更具體而言，一種能符合 ISO 7816 尺寸需求的卡）。該迴路天線有必要是大的，因為被動標籤係使用由該天線所接收的能源來供電，該能源係來自由 RFID 讀取器處所傳輸之訊號。

第 12 圖顯示隨著時間所發展之電力供應電壓，其係藉由在一訊問 RF 場之存在下而整流在迴路天線中所感應之電壓。一旦該電力供應電壓達到一臨界值，則該標籤作業可不符合回應時間之規格。低於此一天線尺寸，該電力供應電壓會永遠無法達到該臨界值，而該標籤則永遠無法啟動。

針對 RFID 應用之天線設計係在 Microchip Technology, Inc 之 Youbok Lee 博士在 2003 年所發表(月份未記載)之應用筆記中所敘述，標題為"Antenna Circuit Design for RFID Applications"。Lee 博士的應用筆記詳細描述了如何針對一運作在 13.56MHz 之被動式 RFID 標籤天線來決定其尺寸需求。在該應用筆記之第 5 頁，Lee 博士展示了迴路天線線圈(coil)之最佳半徑是等於所需讀取距離的 1.414 倍。此分析確認了對於大約若干公分之讀取距離而言，一信用卡尺寸的迴圈天線可幾乎達到最佳化。

在許多應用中，可看到被動標籤正被廣泛使用著。例如，行動裝置製造商將被動式 RFID 標籤嵌入到用於 NFC 應用之行動裝置中。示範性行動應用包括，但不限於，票卷販賣以及行動式付款。於 2008 年 2 月 19 日授與 Leizerovich 及其他人的美

國專利號:7,333,062 顯示一用於 NFC 裝置之具有整合式迴圈天線之行動電話。如美國專利 7,333,062 號所示，行動電話提供了實作一 13.56MHz 之迴路天線所必要的真實狀況(real estate)。

在較小的行動裝置中實作被動標籤之方式已嘗試過多次。這些嘗試未能達成有限的成功，部分是由於該迴路天線尺寸之故。例如，第 13 圖顯示一在一安全數位(SD)記憶卡中之 RFID 標籤實作，該安全數位(SD)記憶卡係由 Wireless Dynamics, Inc. of Calgary, Alberta Canada 所製造。卡 1300 包括一天線，但是因此 SD 卡明顯地太大。同樣地舉例而言，美國公開號：2006/0124755A1 顯示一具有被動標籤之記憶卡，但是該卡必須被插入到一插槽中以存取在不同裝置上之迴路天線。按此實作方式，行動裝置之真實狀況是仍依賴迴路天線之實作。因此，可預見的是，天線的尺寸會被當作為要進一步微型化被動式 RFID 標籤的障礙。

對於能不用依賴外部裝置來收納天線之小型足跡(footprint)RFID 標籤的需求是存在著。對於能相容於在行動裝置上之標準記憶卡插槽的記憶卡相容 RFID 標籤的需求，亦是存在著的。

【發明內容】

本發明之一態樣係揭示一種對一記憶卡相容之附加插槽維持未受干擾之電力的方法，該方法包含週期性地對該記憶卡相容附加插槽發送記憶卡寫入命令。

本發明之另一態樣係揭示一種修改對一雙介面智慧卡

IPR2025-00645 Page 00268

控制器之電力傳遞的方法，該方法包含以下步驟：將一隱藏命令嵌入到一記憶卡寫入命令內，該隱藏命令係對一在一記憶卡相容無線射頻識別(RFID)卡上之雙介面智慧卡控制器，指定進行電力傳遞之修改；以及將該記憶卡寫入命令發送到該記憶卡相容 RFID 卡。

本發明之又一態樣係揭示一種修改對一雙介面智慧卡控制器之電力傳遞的方法，該方法包含以下步驟：在一記憶卡控制器處接收一命令，其中該命令包括一指令，以用來修改對一雙介面智慧卡控制器之電力傳遞，該雙介面智慧卡控制器係與該記憶卡控制器共同放置在一記憶卡上；以及修改對該雙介面智慧卡控制器之電力傳遞。

本發明之又另一態樣係揭示一種用指令所編碼而成之電腦可讀取媒體，其中當由一記憶卡控制器存取時該等指令會造成該記憶卡控制器能執行以下動作：在該記憶卡控制器處接收一命令，其中該命令包括一指令，以用來修改對一雙介面智慧卡控制器之電力傳遞，該雙介面智慧卡控制器係與該記憶卡控制器共同放置在一記憶卡上；以及修改對該雙介面智慧卡控制器之電力傳遞。

【實施方式】

在以下詳細敘述中可參考隨附圖式，該等圖式僅作為說明用途而顯示本發明之各具體實施例。該等具體實施例係充分描述以讓該領域中熟悉技術人士能實現本發

IPR2025-00645 Page 00269

明。應了解到本發明之各具體實施例雖然不同，但並非互斥。例如，關連於一具體實施例之特定特徵、架構或特性可被實作在其他具體實施例中，而無需悖離本發明之精神及範圍。此外，應了解到在所揭示具體實施例內之個別元件之位置或配置，可在不悖離本發明之精神及範圍下進行修改。因此，以下詳細敘述將不會被認為是限制，而本發明之範圍則只由所附的申請專利範圍所定義，並連同由申請專利範圍所主張的均等物之完整範圍一併加以適當地解釋。在圖式中，相似的標號會遍佈於各自的示圖中而涉及到相同或相似的功能。

第 1 圖顯示一行動計算裝置以及一相容於記憶卡插槽之小型 RFID 卡。行動計算裝置 110 在第 1 圖中係顯示成一行動電話，但是這並非當成本發明之限制。例如，行動計算裝置 110 可為個人數位助理(PDA)、智慧型手機、行動電話、手持式電腦、桌上型電腦、或任何其他能夠如此處所述般運作的裝置。

行動計算裝置 110 包括記憶卡插槽 112。記憶卡插槽 112 是能夠接受 RFID 卡 120 的插槽。例如，記憶卡插槽 112 可具有相容於 RFID 卡 120 之實體維度，並可具有使用相容於 RFID 卡 120 之協定來運作的通訊介面。如此所使用般，該用語「記憶卡插槽」可為任何能夠接受一具有記憶體之卡的外加(add-on)插槽，並可由一像是如第 1 圖所示之行動計算裝置所存取。例如，一記憶卡插槽可相容於一工業標準之通訊協定，或可相容於被廣泛接

IPR2025-00645 Page 00270

受之通訊協定，此通訊協定不一定要被正式規範納入為工業標準。範例包括了能相容於多媒體記憶卡(MMC)協定之插槽、記憶棒 DUO(Memory Stick DUO)協定、安全數位(SD)協定、以及智慧型媒體(Smart Media)協定。上述清單僅作為範例性質，而非徹底詳述。除了以上明確所列之協定外，記憶卡 112 還可相容於許多記憶卡插槽協定而不會悖離本發明之範圍。

RFID 卡 120 包括電子接觸 122，其係能與記憶卡插槽 112 通訊之主機端介面的一部分。例如，電子接觸 122 可提供適用於記憶卡之通訊協定的連接性。RFID 卡 120 包括 RFID 功能性，且亦可包括可由行動計算裝置 110 所存取之記憶體。例如，在某些具體實施例中，RFID 卡 120 包括一智慧卡控制器以及一能與 NFC 讀取器（例如 ISO 14443 適用介面）互動的感應元件。在其他具體實施例中，RFID 卡 120 不包括由行動計算裝置 110 所存取的記憶體。RFID 卡 120 可包括記憶體及 RFID 之外的功能。

在本發明之各具體實施例中，在 RFID 卡中的 RFID 功能性係由行動計算裝置 110 使用記憶卡存取命令所存取，該等記憶卡存取命令已被定義以用於記憶卡插槽 112。據此，本發明之各具體實施例能讓 RFID 功能在無需定義新命令的前提下實作出記憶體存取之外的功能。在某些具體實施例中，用於 RFID 之新命令被嵌入到資料位元之內，該等新命令係接續在記憶卡讀取/寫入命令之後。然後 RFID 卡 120 決定新進入之資料位元是否為

IPR2025-00645 Page 00271

用於 RFID 功能的正規讀取/寫入功能。換言之，除了標準記憶卡功能之外的功能可透過在資料串流中之「隱藏」命令來存取，該「隱藏」命令可使用現存記憶卡存取命令及功能來交換。根據本發明之各具體實施例，現存記憶卡功能及 RFID 功能兩者可在無需對如何建立主機端協定的方式進行改變的前提下實作。

行動計算裝置 110 及 RFID 卡 120 的結合可被用於任何目的。例如，在某些具體實施例中，RFID 卡 120 可與銷售時點情報系統(point-for-sale)付費裝置進行互動，以達到行動付款的效果。同樣作為範例，在某些具體實施例中，RFID 卡 120 可被用於大眾運輸環境中採感應即付款(wave and pay)方式的票卷銷售上，像是 MIFARE。

第 2 圖顯示一行動計算裝置之方塊圖。行動計算裝置 110 包括天線 240、射頻電路 230、處理器 210、記憶體 220 以及記憶卡插槽 112。在某些具體實施例，行動計算裝置 110 是行動電話，或包括行動電話功能。例如，天線 240 以及射頻電路 230 可運用於與一蜂巢式電話網路進行通訊。更甚者，在某些具體實施例中，行動計算裝置 110 是無線區域網路(WLAN)或無線廣域網路(WWAN)裝置。例如，天線 240 以及射頻電路 230 可運用於與一無線存取點進行通訊。在某些具體實施例中，天線 240 及無線電路 230 被忽略，而行動計算裝置 110 無法運用無線連接。

處理器 210 代表一能夠與其他在行動計算裝置 110 中

IPR2025-00645 Page 00272

所示方塊通訊的處理器。例如，處理器 210 可為微處理器、數位訊號處理器(DSP)、微控制器等等。進一步而言，可依據狀態機或其他序列邏輯來構成處理器 210。在運作中，處理器 210 可讀取來自記憶體 220 的指令並因應於該等指令而執行動作。例如，處理器 210 可執行能影響在行動計算裝置 110 以及耦接到記憶卡插槽 112 之裝置間之通訊的程式指令。

記憶卡插槽 112 係連同第 1 圖作為參考並如上所述。記憶卡插槽 112 包括相容於 RFID 卡 120 的電路。行動計算裝置 110 可藉由使用記憶卡存取命令之標準集合，而與 RFID 卡 120 通訊。例如，處理器 210 可使用記憶卡寫入命令，以寫入到在 RFID 卡 120 內之記憶體，並可使用記憶卡讀取命令來從在 RFID 卡 120 內之記憶體處讀取資料。

行動計算裝置 110 可使用嵌入於記憶卡存取命內之「隱藏」命令，而存取在 RFID 卡 120 內之 RFID 功能。例如，一記憶卡寫入命令可包括一唯一資料串，以將該記憶卡寫入命令識別成一被轉移成除了記憶體寫入外之目的之命令。此外，供給記憶卡寫入命令之該區段位址，可被設定成一特定位址值，以進一步將記憶卡寫入命令識別成一被轉換之命令。除了指定位址/資料值能將該記憶卡存取命令識別成一被轉換除了記憶體存取外之目的之命令，該記憶存取命令可包括資料位元，以進一步指定隱藏命令的類型及功能。隱藏命令的範例格式係進一

IPR2025-00645 Page 00273

步如下所述。在某些具體實施例中，一讀取命令在一寫入命令後立即發佈，以啟動從非記憶卡功能到主機端之間的資料流，其中該寫入命令的資料曾有隱藏命令。記憶卡寫入命令以及記憶卡讀取命令的結合可按此方式來使用，以形成一隱藏讀取命令。

在某些具體實施例中，記憶卡插槽 112 係在非主動週期之後關閉電源，以節省電力。例如，可於處理器 210 發佈一記憶卡寫入或讀取命令時而對記憶卡插槽 112 啟動電源，但是可於之後關閉電源以節省電力。當記憶卡插槽 112 被關閉電源時，任何耦接到記憶卡插槽之裝置亦被關閉電源。例如，若 RFID 卡 120（第 1 圖）被耦接到記憶卡插槽，則當記憶卡插槽 112 被關閉電源時 RFID 卡 120 亦會關閉電源。

在本發明之各具體實施例中，處理器 210 執行駐存在記憶體 220 中之軟體，以維持對記憶卡插槽 112（以及對 RFID 卡 120）的電力。例如，週期性隱藏命令可為了讓電力持續供應之目的而被發送到 RFID 卡 120，同時 RFID 卡 120 被期望能提供 RFID 的功能。同樣作為範例，一隱藏命令可為了將電力循環到一駐存在卡上之智慧卡控制器之目的，而被發送到 RFID 卡 120。這些隱藏命令會在以下連同後面的圖式而加以詳細描述。

第 3A 圖顯示一具有整合感應元件並相容於記憶卡之 RFID 卡。RFID 卡 300 代表 RFID 卡 120（第 1 圖）之可能具體實施例。RFID 卡 300 包括主機端介面 310、記憶

卡控制器 340、記憶體 360、智慧卡控制器 340、程式記憶體 332、以及小型感應元件 350。RFID 卡能夠與一在行動計算裝置內之記憶卡插槽進行通訊。進一步而言，RFID 卡 300 不需要記憶卡插槽來實作出延伸的輸入/輸出功能。例如，且非為限制，在 SD 的具體實施例中，RFID 卡 300 能運作在任何 SD 記憶卡插槽中，且不需要安全數位輸入輸出(SDIO)的記憶卡插槽。

主機端介面 310 包括電子接觸，以與記憶卡插槽交互聯繫。例如，主機端介面 310 包括了像是接觸 122(第 1 圖)般的接觸。同樣作為範例，在某些具體實施例中，主機端介面 310 包括了隱蔽的電子接觸。主機端介面 310 亦可包括像是驅動器、接收器、終端等等的電路。

在由第 3A 圖所表示之具體實施例中，記憶卡控制器 340 使用記憶卡存取命令來與行動裝置通訊。記憶卡控制器亦可與記憶體 360 通訊。記憶卡控制器判斷是否各命令應形成與記憶體 360 之記憶體運作、是否一隱藏命令應被轉換成智慧卡控制器 330、或是否記憶卡控制器 340 應該因應於隱藏命令而採取行動。在某些具體實施例中，記憶卡控制器 340 執行除存在一內部記憶體內或是儲存在記憶體 360 內之指令。在某些具體實施例中，記憶卡控制器 340 包括特殊目的硬體，其在判斷一命令是否應被轉換上很有用。在其他具體實施例中，記憶卡控制器 340 可為一在各方面都等同於在記憶卡中所找到之控制器的微控制器，除了其執行之程式之外。

IPR2025-00645 Page 00275

記憶體 360 可為任何類型的揮發性或非揮發性記憶體。例如，記憶體 360 可為揮發性記憶體，像是靜態隨機存取記憶體(SRAM)或是動態隨機存取記憶體(DRAM)。同樣作為範例，記憶體 360 可為非揮發性記憶體，像是 NOR 快閃記憶體或 NAND 快閃記憶體。在本發明之各具體實施例中，記憶體 360 代表能使用記憶卡存取命令而由行動計算裝置所存取之記憶體，該等記憶卡存取命令係為此目的所定義。

當 RFID 卡 300 正與在一行動計算裝置內之記憶卡插槽進行通訊時，該行動計算裝置可發送一記憶卡存取命令，以便存取記憶體 360。同樣作為範例，該行動計算裝置可發送一含有隱藏命令之記憶卡存取命令。記憶卡控制器 340 偵測該隱藏命令之存在，並使用通訊匯流排 342 來轉移所有或部分的記憶體存取命令到智慧卡控制器 330。通訊匯流排 342 可具有任何數目的導線(conductors)並可採用任何形式。例如，通訊匯流排 342 可為序列埠、並列埠、或可包括多個資料導線、多個位指導線及/或能載送控制訊號之導線，像是時脈訊號。在某些具體實施例中，記憶卡控制器 340 因應一隱藏命令而採取一或更多動作。例如，記憶卡控制器 340 可因應於一隱藏命令而修改時脈訊號。

記憶卡控制器 340 可用許多方式來偵測隱藏命令。例如，在某些具體實施例中，該記憶卡存取命令可包括一特定位址值或特定資料值。記憶卡控制器 340 偵測到包

IPR2025-00645 Page 00276

括了特定位址值或特定資料值其中之一或兩者的命令，並將該命令適當地繞送。用於此目的之該特定位址值及特定資料值在此能被視為隱藏命令位址值及隱藏命令資料值。

在某些具體實施例中，記憶卡控制器 340 能只基於隱藏命令位址值而偵測到隱藏命令之存在。在此些具體實施例中，記憶卡控制器 340 檢查含闊在一記憶卡存取命令中的位址值，且若是該命令與該隱藏命令位址值相符，則將其轉換（或採取某些動作）。在某些具體實施例中，記憶卡控制器 340 只基於隱藏命令資料值而偵測到隱藏命令的存在。在此些具體實施例中，記憶卡控制器 340 檢查一含括在記憶卡存取命令中的資料值，且若是該命令與該隱藏命令資料值相符，則將其轉換。在其他進一步之具體實施例中，記憶卡控制器 340 能基於隱藏命令位址值及隱藏命令資料值兩者而偵測到隱藏命令的存在。在這些具體實施例中，只在記憶卡存取位址及資料兩者與隱藏命令位址值及隱藏命令資料值分別相符時，記憶卡控制器 340 才會轉換命令。

隱藏命令位址值及隱藏命令資料值可按許多方式來指定。例如，所有 RFID 卡可用固定值來發佈。在這些具體實施例中，每次存取 RFID 功能時，相同的隱藏命令位址及/或資料值被含括在記憶卡存取命令中。同樣作為範例，不同的 RFID 卡可用獨一(unique)值來發佈。在此些具體實施例中，當需要時，各 RFID 卡可提供這些值

IPR2025-00645 Page 00277

給一行動計算裝置。同樣作為範例，隱藏命令位址及/或資料值可由該行動計算裝置來指定。在其他進一步具體實施例中，隱藏命令位址及資料值可為動態。隱藏命令位址及資料值可在每當施加電力時或是按一週期性基礎而改變。

智慧卡控制器 330 接收由記憶卡控制器 340 所轉換之隱藏命令。智慧卡控制器 330 進一步轉譯該等隱藏命該等隱藏命令並因應於此而執行動作。智慧卡控制器 330 執行儲存在程式記憶體 332 中之指令。在某些具體實施例中，程式記憶體 332 被嵌入到智慧卡控制器 330 內，而在其他具體實施例中，程式記憶體 332 是記憶體 360 的一部分。

智慧卡控制器 330 是具有含括了 RFID 功能之多個介面中之一者的雙介面智慧卡控制器。在某些具體實施例中，智慧卡是相容於在 NFC 應用內之被動 RFID 標籤讀取器。例如，智慧卡控制器 330 可為一能夠實現所有或部分用於無接觸 NFC 裝置之 ISO 14443 標準的裝置。同樣作為範例，智慧卡控制器 330 可為能夠實現用於接觸/無接觸需求之 ISO 7816 及 ISO 14443 兩者的雙介面智慧卡控制器。來自 Netherlands 之 NXP 的可用控制器的“SmartMX”家族，為適合之雙介面智慧卡控制器的範例。這些控制器提供了在 13.56MHz 上之 RFID 功能。本發明之各種具體實施例能運作在 13.56MHz，但是並未限制其只能在此頻率上運作。在某些具體實施例中，智慧

IPR2025-00645 Page 00278

卡控制器與用於票卷應用之 MIFARE 系統交互運作。

智慧卡控制器 330 從該主機端介面接收電力。藉由不從該訊問 RF 場接收電力的方式，能否定掉用於電力產生之一迴路天線的必要性。智慧卡控制器 330 包括天線埠 334。天線埠 334 係耦接到小型感應元件 350。

小型感應元件 350 包括一環繞著一磁核纏繞的線圈。對於從該訊問 RF 場汲取電力而言該線圈太小了，但是由於智慧卡控制器 330 係由該主機端裝置通過主機端介面 310 來供電，所以這方式並非很必要。小型感應元件 350 係與在 RFID 讀取器內之天線互動，其互動方式近似於主要及次要線圈在變壓器內之互動。該 RFID 讀取器具有在 13.56MHz 共鳴的線圈，其扮演著如變壓器之主要線般的功能。小型感應元件 350 扮演著如變壓器之次要線般的功能。據此，該傳輸器能「看見」次要線圈(小型感應元件 350)的阻抗。智慧卡控制器 334 能夠使用電路來調變經反射之訊號，以修改在天線埠 334 處之阻抗。

小型感應元件 350 可被做的非常小。例如，在某些具體實施例中，RFID 卡 120 為一 miniSD 卡，而小型感應元件 350 小到足以被完整地含在該 miniSD 的外觀尺寸內。在記憶卡外觀尺寸內之小型感應元件之指定具體實施例係如下般參考第 4 圖所述。

在本發明之各具體實施例中，記憶卡控制器 340 以及智慧卡控制器 330 係按許多不同的方式所實作。例如，在某些具體實施例中，各種組件被實作成硬體。在這些

IPR2025-00645 Page 00279

具體實施例中，各種組件可被實作成個別之積體電路，或是實作成一組合式積體電路。同樣作為範例，在某些具體實施例中，各種組件可被實作成軟體，或是硬體與軟體的組合。在某些具體實施例中，RFID卡300可包括一微處理器，而該等組件可被實作成運行於該微處理器上之軟體模組。在其他具體實施例中，RFID卡300可包括多個處理器，而該等組件可被實作成跨越該等多個處理器所散布的軟體模組。

第3B圖顯示一具有整合感應元件之記憶卡相容RFID卡的方塊圖。RFID卡302代表RFID卡120（第1圖）之可能具體實施例。RFID卡302包括主機端介面310、記憶卡控制器340、記憶體360、智慧卡控制器340、程式記憶體332以及小型感應元件350，所有這些元件皆如上參考第3A圖般所描述。RFID卡302能夠與一在行動計算裝置內之記憶卡插槽進行通訊。更進一步，RFID卡302不需要記憶卡插槽來實作延伸的輸入/輸出功能。例如，且非為限制，在SD具體實施例中，RFID卡302能夠運作在任何的SD記憶卡插槽中，且不需一安全數位輸入輸出(SDIO)記憶卡插槽。

在由第3B圖所代表之具體實施例中，智慧卡控制器330從記憶卡控制器340處接收電力。在這些具體實施例中，記憶控制器340能通過對智慧卡控制器330提供之電力而直接進行控制。記憶控制器340可因應於通過主機端介面所接收之命令，而施加及/或移除來自智慧卡

控制器 330 之電力。例如，記憶控制器 340 可接收一隱藏命令，以藉由透過電力循環來重新啟動之方式來重置智慧卡控制器 330。

第 4 圖顯示一具有整合感應元件之記憶卡相容 RFID 卡的照片圖。RFID 卡 120 係按一 SD 卡之外觀尺寸顯示，然此並非為本發明之限制。RFID 卡 120 包括電子接觸 122、記憶卡控制器 340、智慧卡控制器 330、記憶體 360、磁核 450、線圈 452，以上全部皆被固定至電路板 402。

磁核 450 以及線圈 452 能實作小型感應元件 350(第 3 圖)。如照片中可見，該小型感應元件能整個裝配到記憶卡外觀尺寸內。該小型感應元件不對智慧卡控制器 330 提供電力之產生，故因此不須為了此目的而將尺寸做得比較大。

第 5 圖，顯示一記憶卡寫入命令之資料部分。含括在內的有隱藏命令資料值 510、狀態欄 520、密碼欄 530、裝置 ID532、命令索引 540 以及隱藏命令相關資料 550。在第 5 圖之範例中，資料部分之長度為 512 位元組，然此並非作為本發明之限制。任何數量之數目可被含括在寫入命令中，而第 5 圖中之各欄位可為任何長度。

在第 5 圖之範例中，隱藏命令資料值為 256 位元的長度，然此處可使用任何長度而不會悖離本發明之範圍。在某些具體實施例中，隱藏命令資料值 510 被用來將一記憶體寫入命令識別成一隱藏命令。當一寫入命令接收了一在前 256 位元處擁有之資料（其與隱藏命令資料值

相符）時，該命令被識別為一正被待轉換到智慧卡控制器之命令。如上所述，一隱藏命令位址值可被用來與一隱藏命令值相關連或是相反地不相關連，以將該記憶體寫入命令識別成一隱藏命令。

當記憶體寫入為一隱藏命令時，剩餘的欄位更顯其重要性。例如，若前 256 個位元與隱藏命令資料值不相符時（或若該寫入位址與該隱藏命令位址值不相符時，或是兩者皆是），則在資料欄中之剩餘位元會被當成在一般記憶體寫入命令內之資料看待。相反地，當記憶體寫入是一隱藏命令時，則剩餘欄位被用來進一步轉譯該隱藏命令。

記憶卡控制器 340（第 3、4 圖）檢驗該隱藏命令資料值 510、狀態欄 520，而可能的話還檢驗密碼欄 530 及裝置 ID532。在某些具體實施例中，若命令被識別成一隱藏命令，記憶卡控制器 340 會將密碼 530、命令索引 540 及相關資料 550 前傳到智慧卡控制器 330。在其他具體實施例中，記憶卡控制器 340 可基於隱藏命令而直接地採取動作。

狀態欄 520 可包括任何相關於隱藏命令狀態之資訊。例如，狀態欄 520 可包括一或更多的位元以對記憶卡控制器 340 表示該主機端（行動計算裝置）是否期望該智慧卡能因應於該隱藏命令而回傳資料。例如，當狀態欄 520 表示出一寫入之意思時，記憶卡控制器 340 會在未期望回傳任何資料到主機端之情況下將密碼、裝置 ID、

命令索引、及相關資料前傳。同樣作為範例，當狀態欄520表示一讀取之意思時，記憶卡控制器340會在期望該智慧卡330將提供資料以因應於一記憶卡讀取命令而將 料發送到主機端之情況下，將密碼、裝置ID、命令索引、及相關資料前傳。在其後有一記憶卡讀取命令短暫尾隨著的記憶卡寫入命令之結合，可被用來提供「讀取」功能給智慧卡控制器。來自智慧卡控制器之讀取作業係進一步如下參考第8圖所述。

密碼欄530包括一密碼，以允許智慧卡控制器330用該主機端對該符記(token)鑑別。在某些具體實施例中，每個隱藏命令包括一密碼。每次密碼、裝置ID、命令索引、及相關資料被轉換到智慧卡控制器時，即檢查密碼以用該主機端對該符記鑑別。

裝置ID532獨一地識別該主機端（行動計算裝置）。該裝置ID可由該智慧卡控制器來檢查以確保該符記被插入到其所被鑑別之主機端。本發明之某些具體實施例會使用裝置ID來加強獨一主機端/卡組對，而其他具體實施例允許智慧卡控制器之功能能由任何主機端來存取。

命令索引540識別隱藏命令之類型。可能的隱藏命令之數目是只有受限於配置於其上之位元數目。任何數目的位元可被配置到命令索引540，而不會背離本發明之範圍。隱藏命令相關資料550可針對隱藏命令之各類型而不同地使用。任何數目的位元可被用於隱藏命令相關資料550。

IPR2025-00645 Page 00283

在第 5 圖中所示之資料係當做一範例來提供，而記憶卡存取命令之資料欄位可包括相較在第 5 圖中所示資料欄位下更多或更少的資料欄位。本發明未受限於在記憶卡存取命令內之欄位內容或數目。

第 6 圖根據本發明之各種具體實施例而顯示一流程圖。在某些具體實施例中，方法 600 可由一行動計算裝置所使用，以與在記憶卡插槽內之 RFID 卡進行通訊。在某些具體實施例中，方法 600，或是其部分，係由一具有記憶卡插槽之行動計算裝置所執行，而在其他具體實施例中，方法 600，或是其部分，係由軟體所執行。在方法 600 內之各式動作可按所呈現之順序、按不同順序、或是同時地執行。更進一步，在某些具體實施例中，列於第 6 圖內之某些動作會從方法 600 中忽略。

方法 600 開始於 610，其中一資料圖樣(pattern)以及一位址值係從一在記憶卡插槽內之 RFID 卡處接收。資料圖樣對應到隱藏命令資料值，而位址值對應到隱藏命令位址值。在某些具體實施例中，行動裝置只接收資料值，而在其他具體實施例中，行動裝置只接收位址值。在某些具體實施例中，當 RFID 卡首次插入到記憶卡插槽時，610 之動作會發生一次。每當行動裝置建立了一隱藏命令時，該行動計算裝置則可使用位址及資料值。在其他具體實施例中，每次 RFID 卡被插入到記憶卡插槽時，則會發生 610 之動作。在更進一步之具體實施例中，資料圖樣可為相同或不同，而位址值可為相同或不同。

IPR2025-00645 Page 00284

在 620 處，記憶卡存取命令之資料欄位會被資料圖樣所填滿(populated)，使得命令被轉換到在 RFID 卡上之智慧卡。例如，資料圖樣可被當成隱藏命令資料值 510 而寫入到資料欄位（第 5 圖）。

在 630 處，該記憶卡存取命令之一位址欄位會被位址值填滿，以進一步使得命令被轉換到智慧卡控制器。在某些具體實施例中，只有 620 或 630 其中之一被使用。在這些具體實施例中，隱藏命令的存在係單獨由資料圖樣或是單獨由位址值所表示。

在 640 處，記憶卡存取命令之資料欄位係用一命令字串所填滿，以指定除了記憶卡存取之外的目的。例如，命令字串可被寫入到資料欄以當成用於該智慧卡控制器之命令索引 540。此命令可被用於任何目的上。例如，一或更多之隱藏命令可有一維持對記憶卡插槽提供電力之唯一目的，使得該 RFID 卡持續接收電力。

在 650 處，記憶卡存取命令之資料欄位係用一密碼鎖填滿，以鑑別耦接到記憶卡插槽之 RFID 卡之存取。在某些具體實施例中，一密碼被含括在每個隱藏命令之資料欄位中。在其他具體實施例中，一密碼只被含括在一交換之開始處。

在 660 處，記憶卡存取命令被發送到耦接至記憶卡插槽之 RFID 卡。例如，一行動計算裝置(110，第 1、2 圖)可發送記憶卡存取命令到一在記憶卡插槽(112，第 1、2 圖)內之 RFID 卡(120，第 1、3、4 圖)。RFID 卡包括記

IPR2025-00645 Page 00285

憶卡控制器(340、第 3 圖)以基於在方法 600 內所填之資料欄位來轉換命令。

第 7 圖根據本發明之各具體實施例來顯示一流程圖。在某些具體實施例中，方法 700 可由一在記憶卡插槽內之 RFID 卡所使用。在某些具體實施例中，方法 700，或是其部分，係由在記憶卡相容 RFID 卡內之記憶卡控制器所執行，而在其他具體實施例中，方法 700，或是其部分，係由軟體所執行。在方法 700 中之各種動作可按所呈現之順序、按不同順序、或是同時地執行。更進一步，在某些具體實施例中，列於第 7 圖內之某些動作會從方法 700 中忽略。

方法 700 開始於 710 處，其中一記憶卡存取命令係從一行動計算裝置經由一主機端介面所接收。710 之動作係對應到在行動計算裝置之記憶卡插槽內之 RFID 卡，其接收一記憶卡存取命令。

在 720 處，記憶卡控制器檢查在記憶卡存取命令中之準則，以判斷該記憶卡存取命令是否應該被轉換成駐存在 RFID 卡上之智慧卡控制器。該準則可為一隱藏命令資料值或一隱藏命令位址值其中之一或兩者。若在 730 處有一準則相符，則呈現一隱藏命令，且該記憶卡存取命令之至少一部分會在 740 處被轉換。若沒有準則是相符的，則沒有隱藏命令會被呈現，並在 750 處執行記憶體存取。

第 8 圖顯示根據本發明之各具體實施例來顯示一流程

IPR2025-00645 Page 00286

圖。在某些具體實施例中，方法 800 可由一在記憶卡插槽內之 RFID 卡所使用。在某些具體實施例中，方法 800，或是其部分，係由在 RFID 卡內之記憶卡控制器所執行，而在其他具體實施例中，方法 800，或是其部分，係由軟體所執行。在方法 800 中之各種動作可按所呈現之順序、按不同順序、或是同時地執行。更進一步，在某些具體實施例中，列於第 8 圖內之某些動作會從方法 800 中忽略。

方法 800 開始於 810 處，其中一記憶卡存取命令係從一行動計算裝置經由一主機端介面所接收。若記憶卡寫入命令被判斷為是一隱藏命令，則處理程序持續到 840；否則則在 830 處執行記憶體寫入。

在 840 處，隱藏命令被轉換到智慧卡控制器。若在 850 處隱藏命令被判斷成是「讀取」，則處理程序在 860 處持續；否則，即視為完成隱藏命令處理程序。在 860 處，記憶卡控制器會從智慧卡控制器處擷取非記憶體資料，而在 870 處，會從行動計算裝置處接收記憶卡讀取命令。在 880 處，非記憶體資料會被回傳到行動計算裝置。

方法 800 展示了一行動計算裝置如何可從一在記憶卡相容 RFID 卡內之智慧卡控制器處執行讀取的方式。行動計算裝置發佈了一具有隱藏命令之記憶卡寫入命令，該隱藏命令具有一表示讀取之狀態欄位，而然後該行動計算裝置會發佈一記憶卡讀取命令。在卡片中之處理程序接收該隱藏命令，將其識別為讀取，而然後因應於隨

後之記憶卡讀取命令而將資料回傳到行動計算裝置。

第 9 圖顯示根據本發明之各具體實施例來顯示一流程圖。在某些具體實施例中，方法 900 可由一在記憶卡插槽內之 RFID 卡所使用。在某些具體實施例中，方法 900，或是其部分，係由在 RFID 卡內之智慧卡控制器所執行，而在其他具體實施例中，方法 900，或是其部分，係由軟體所執行。在方法 900 中之各種動作可按所呈現之順序、按不同順序、或是同時地執行。更進一步，在某些具體實施例中，列於第 9 圖內之某些動作會從方法 900 中忽略。

方法 900 開始於 910 處，其中一智慧卡存取命令從該記憶卡控制器接收一命令。此命令對應到一由記憶卡控制器所接收之隱藏命令。在 950 處，該智慧卡控制器判斷該命令是否為「虛擬」(dummy)命令，其主要用於維持對該記憶卡插槽之電力的目的。若否，則在命令中所指定之智慧卡功能會在 930 處執行。若是，則在 960 處忽視該命令。

方法 900 能在當在主機裝置內之記憶卡插槽將會移除電力以節省能源時之週期期間，允許一在記憶卡插槽內之記憶卡相容 RFID 卡能仍然保持著供電的狀態。此為在記憶卡存取命令內之軟體建構隱藏命令、將隱藏命令轉換到智慧卡控制器之記憶卡控制器、以及忽略該命令之智慧卡控制器之間的合作努力。根據由第 3A 圖所代表的具體實施例，提供電力給 RFID 之方式亦提供電力給

IPR2025-00645 Page 00288

智慧卡控制器，借此允許小型感應裝置的使用，像是蠕第 3 及 4 圖所示般。

第 10 圖根據本發明之各具體實施例來顯示一流程圖。在某些具體實施例中，方法 1000 可由一在記憶卡插槽內之 RFID 卡所使用。在某些具體實施例中，方法 900，或是其部分，係由在 RFID 卡內之記憶卡控制器所執行，而在其他具體實施例中，方法 900，或是其部分，係由軟體所執行。在方法 900 中之各種動作可按所呈現之順序、按不同順序、或是同時地執行。更進一步，在某些具體實施例中，列於第 10 圖內之某些動作會從方法 1000 中忽略。

方法 1000 開始於 1010 處，其中一記憶卡控制器從一行動計算裝置處接收一隱藏命令。若在 1020 處，該記憶卡控制器判斷該隱藏命令正待被轉換到智慧卡控制器，則該命令在 1030 處被轉換。若該命令未準備被轉換，則該記憶卡控制器不會轉換該命令；然而，在 1040 處該記憶卡控制器可基於該隱藏命令而採取其他動作。例如，該記憶卡控制器可修改一提供給智慧卡控制器之時脈訊號。同樣作為範例，記憶卡控制器可判定(assert)一重置信號給該智慧卡控制器。仍然作為範例，該記憶卡控制器可修改對該智慧卡控制器之電力傳遞。在由第 3B 圖所表示之具體實施例中，該記憶卡控制器能夠修改對該智慧卡控制器的電力傳遞。電力傳遞可藉由移除電力、施用電力、循環電力等方式來修改。

IPR2025-00645 Page 00289

修改對該智慧卡控制器的電力傳遞之步驟可為在主機端計算裝置及 RFID 卡內之記憶卡控制器之間的合作努力。例如，供應至該記憶卡插槽之電力可藉由將虛擬隱藏命令供給至 RFID 卡之方式來維持，可參考第 9 圖如上般所述。當電力被持續供應至記憶卡插槽時，可使用隱藏命令，以使得記憶卡控制器能將電力修改、施用或循環到智慧卡控制器。

電力傳遞之修改可允許額外的安全特徵。例如，關閉對該智慧卡控制器之電力，會顯示該智慧卡為非運作狀態，而因此可讓劣質的讀取器避免掉會對卡片進行不必要的讀取。由於天線以要對智慧卡控制器提供足夠電力而言太小，為了能適當地運作卡片的讀取功能，則需要從記憶卡控制器或是從主機端介面處得到電力。

第 11 圖顯示一種讓一行動計算裝置對在一記憶卡相容 RFID 卡內之一或更多功能鑑別之方法。方法 1100 開始於方塊 1110，其中一啟動碼係在 RFID 卡處從行動計算裝置所接收。在 1120，已接收之啟動碼係與儲存在 RFID 卡內之編碼相比較。若啟動碼相符，則在 1140 處 RFID 卡從行動計算裝置接收一密碼，並在 1150 處將密碼儲存在 RFID 卡內以於之後使用。若啟動碼不相符，則在 1160 處 RFID 卡判斷可允許嘗試之數目是否已經超過。若可允許嘗試之數目已經超過，則在 1170 處接觸 RFID 卡發佈者，而若可允許嘗試之數目尚未超過，則該方法會重複嘗試直到不是該啟動碼相符就是可允許嘗試

IPR2025-00645 Page 00290

之數目已經超過為止。

當一 RFID 卡被發佈給一使用者時，可執行方法 1100。例如，RFID 卡可為一行動式支付卡(payment card)，其由一金融機構所發佈。可提供使用者一啟動碼，以「啟動」該 RFID 卡。當使用者成功地輸入該啟動碼時，會提供使用者一組密碼，而該密碼會被儲存以待在未來隱藏命令上之使用。

在某些具體實施例中，在 RFID 卡內之多個非記憶體功能係使用方法 1100 來鑑別。例如，多個非記憶體功能各者可具有已儲存之啟動碼，而各功能已分別被啟動。而各個分別啟動之功能可具有不同的密碼，或者該等多個功能可共享一密碼。

雖然本發明已經連同若干具體實施例加以描述，吾人應了解到可在不背離本發明之精神與範圍的情形下，如該領域中熟悉記憶人士所能輕易理解般地加以修改及變化。此類修改及變化被認為是落在本發明及隨附申請專利範圍之範疇內。

【圖式簡單說明】

第 1 圖顯示一行動計算裝置以及一與記憶卡差曹相容之小型 RFID 卡；

第 2 圖顯示一行動計算裝置之方塊圖；

第 3A-3B 圖顯示具有整合感應元件之記憶卡相容

IPR2025-00645 Page 00291

RFID卡的方塊圖；

第4圖顯示具有一整合感應元件之記憶卡相容RFID卡的照片；

第5圖顯示一記憶體寫入命令之資料部分；

第6-11圖顯示根據本發明之各具體實施例之方法的流程圖；

第12圖顯示在存在著一訊問RF場的情況下，藉由整流在一迴路天線內所感應之電壓而隨著時間所發展的電源供應電壓；以及

第13圖顯示在一安全數位(SD)記憶卡中之一先前技術之RFID標籤實作。

【主要元件符號說明】

110 行動計算裝置

112 記憶卡插槽

120 RFID卡

122 電子接觸

210 處理器

220 記憶體

230 無線射頻電路

240 天線

310 主機端介面

330 智慧卡控器

IPR2025-00645 Page 00292

332 程式記憶體

334 天線埠

340 記憶卡控制器

342 通訊匯流排

350 小型感應元件

360 記憶體

402 電路板

450 磁核

452 核線圈

IPR2025-00645 Page 00293

七、申請專利範圍：

1. 一種對一記憶卡相容之附加插槽維持未受干擾之電力的方法，該方法包含週期性地對該記憶卡相容附加插槽發送記憶卡寫入命令。

2. 如申請專利範圍第 1 項所述之方法，其中該等記憶卡寫入命令包括在一資料欄之一隱藏命令。

3. 如申請專利範圍第 1 項所述之方法，其中該等記憶卡寫入命令包括一獨一性資料字串，以江該記憶卡寫入命令識別成具有一隱藏命令。

4. 如申請專利範圍第 1 項所述之方法，其中週期性地發送記憶卡寫入命令之步驟包括將在該記憶卡相容附加插槽內被一裝置所忽略的隱藏命令，集結成該等記憶卡寫入命令。

5. 如申請專利範圍第 1 項所述之方法，其中週期性地發送記憶卡寫入命令到一記憶卡相容附加插槽之步驟包括，發送該等記憶卡寫入命令到下列其中一者：
一 SD 插槽、一迷你 SD 插槽、或一微 SD 插槽。

6. 一種修改對一雙介面智慧卡控制器之電力傳遞的方

IPR2025-00645 Page 00294

法，該方法包含以下步驟：

將一隱藏命令嵌入到一記憶卡寫入命令內，該隱藏命令係對一在一記憶卡相容無線射頻識別(RFID)卡上之雙介面智慧卡控制器，指定進行電力傳遞之修改；以及

將該記憶卡寫入命令發送到該記憶卡相容 RFID 卡。

7. 如申請專利範圍第 6 項所述之方法，其中發送該記憶卡寫入命令到該記憶卡相容 RFID 卡之步驟包括，將該記憶卡命令發送到一記憶卡插槽。

8. 如申請專利範圍第 7 項所述之方法，其中發送該記憶卡寫入命令到該記憶卡插槽之步驟包括，發送該記憶卡命令到下列其中一者：

一 SD 插槽、一迷你 SD 插槽、或一微 SD 插槽。

9. 如申請專利範圍第 6 項所述之方法，其中將一隱藏命令嵌入到一記憶卡寫入命令內之步驟包括，將一資料字串含括到該記憶卡寫入命令內，以將該記憶卡寫入命令識別成一隱藏命令。

10. 一種修改對一雙介面智慧卡控制器之電力傳遞的方法，該方法包含以下步驟：

在一記憶卡控制器處接收一命令，其中該命令包括一指令，以用來修改對一雙介面智慧卡控制器之電力傳

IPR2025-00645 Page 00295

遞，該雙介面智慧卡控制器係與該記憶卡控制器共同放置在一記憶卡上；以及

修改對該雙介面智慧卡控制器之電力傳遞。

11. 如申請專利範圍第 10 項所述之方法，其中修改對該雙介面智慧卡控制器之電力傳遞的步驟包括，將電力從該雙介面智慧卡控制器移除。

12. 如申請專利範圍第 10 項所述之方法，其中修改對該雙介面智慧卡控制器之電力傳遞的步驟包括，將電力施用到該雙介面智慧卡控制器。

13. 如申請專利範圍第 10 項所述之方法，其中在一記憶卡控制器處接收一命令之步驟包括，從一主機端裝置處接收一記憶卡寫入命令，其中該記憶卡係與該主機端裝置連接。

14. 如申請專利範圍第 10 項所述之方法，其中在一記憶卡控制器處接收一命令之步驟包括，接收在一記憶卡寫入命令內之一隱藏命令。

15. 如申請專利範圍第 10 項所述之方法，更包含接收在該記憶卡控制器處接收一第二命令，其中該第二命令包括一指令，以重置該雙介面智慧卡控制器。

IPR2025-00645 Page 00296

16. 一種用指令所編碼而成之電腦可讀取媒體，其中當由一記憶卡控制器存取時該等指令會造成該記憶卡控制器能執行以下動作：

在該記憶卡控制器處接收一命令，其中該命令包括一指令，以用來修改對一雙介面智慧卡控制器之電力傳遞，該雙介面智慧卡控制器係與該記憶卡控制器共同放置在一記憶卡上；以及

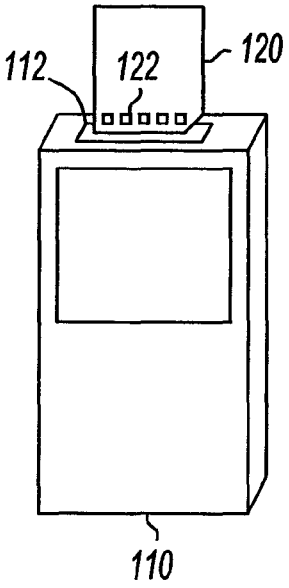
修改對該雙介面智慧卡控制器之電力傳遞。

17. 如申請專利範圍第 16 項所述之電腦可讀取媒體，其中修改對該雙介面智慧卡控制器之電力傳遞的步驟包括將電力循環到該雙介面智慧卡控制器。

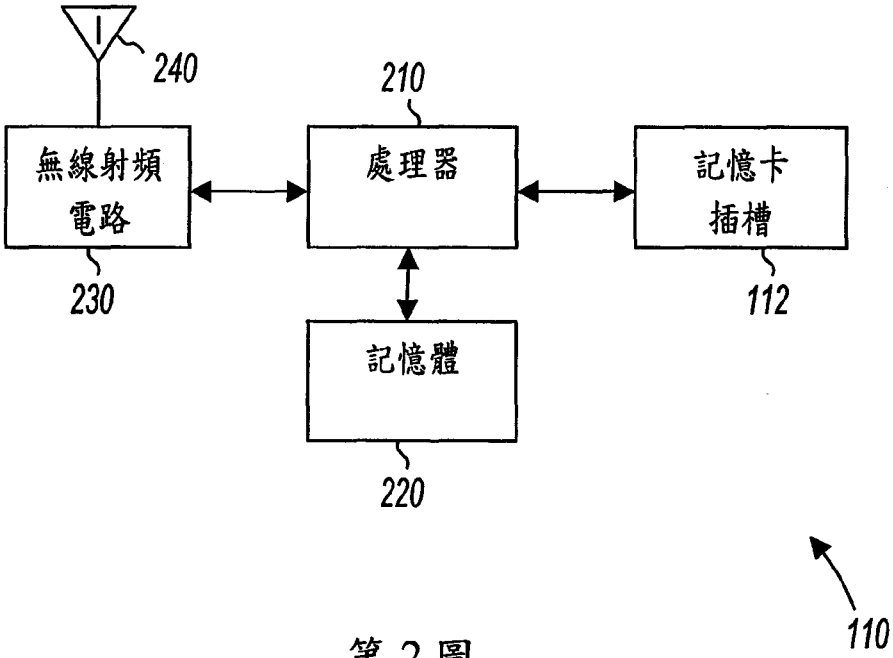
18. 如申請專利範圍第 16 項所述之電腦可讀取媒體，其中在該記憶卡控制器處接收一命令之步驟包括，從一主機端裝置處接收一記憶卡寫入命令，其中該記憶卡係與該主機端裝置連接。

19. 如申請專利範圍第 16 項所述之電腦可讀取媒體，其中在該記憶卡控制器處接收一命令之步驟包括，接收在一記憶卡寫入命令內之一隱藏命令。

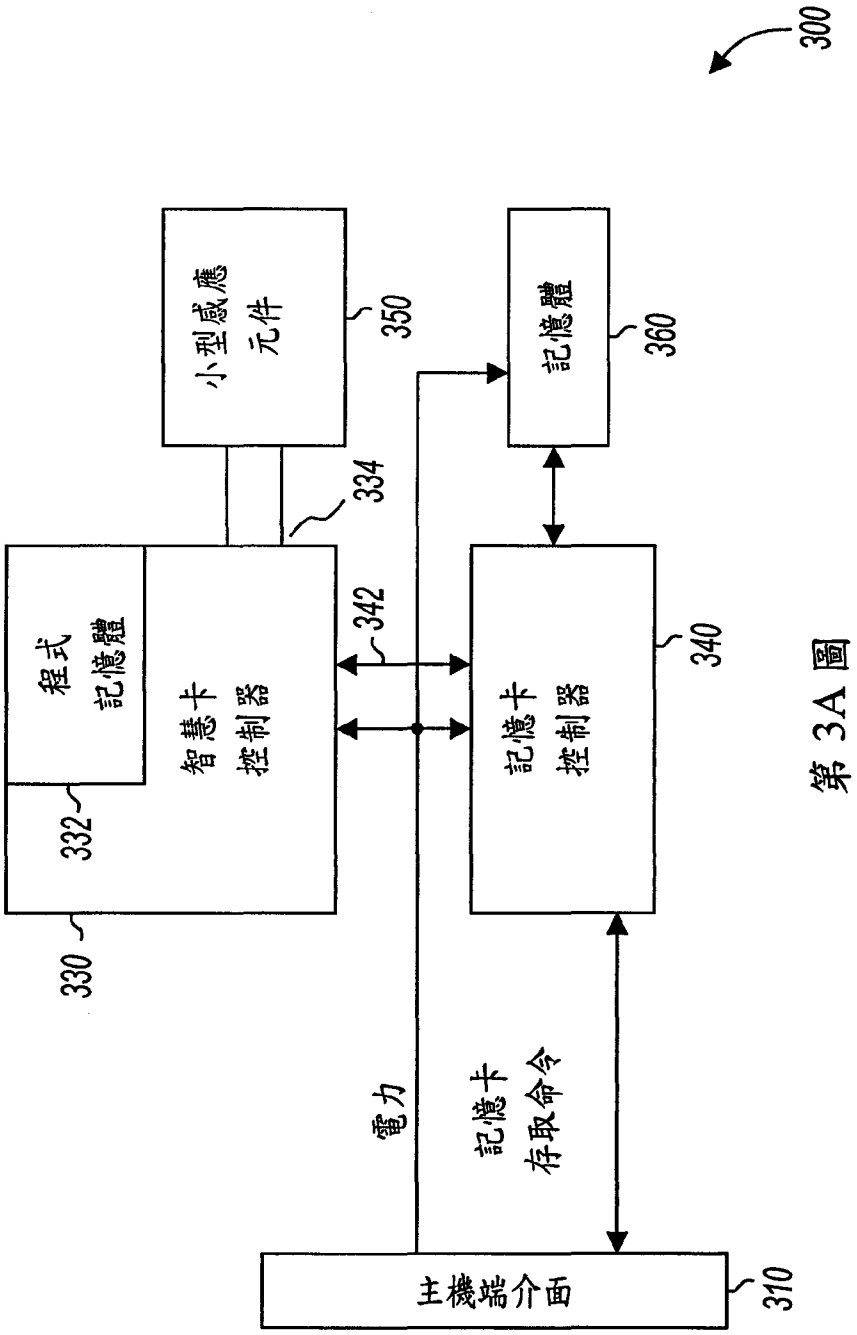
IPR2025-00645 Page 00297



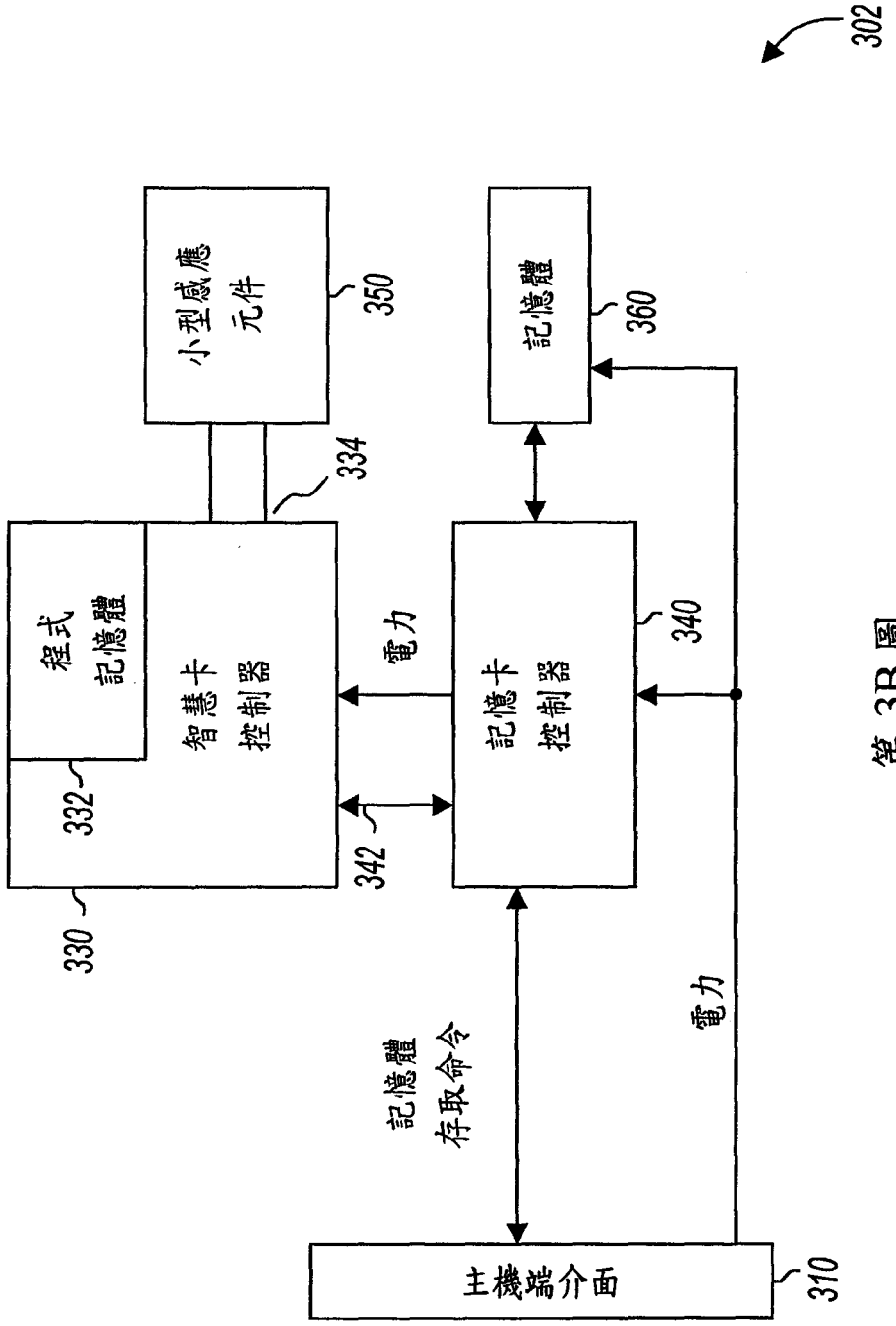
第 1 圖



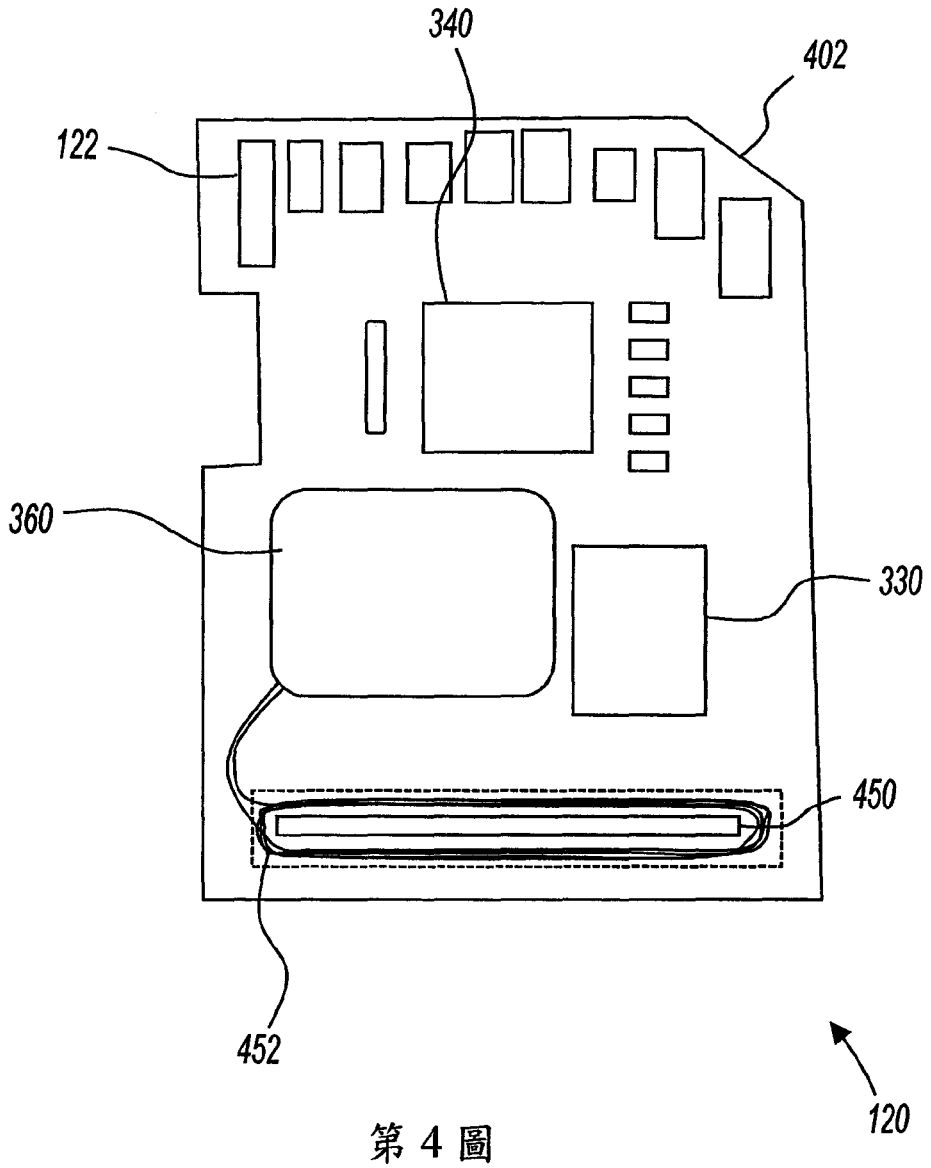
第 2 圖


300
小型感應元件
350
記憶體
360
334
程式記憶體
智慧卡控制器
342
記憶卡控制器
340
332
330
電力
記憶卡存取命令
主機端介面
310

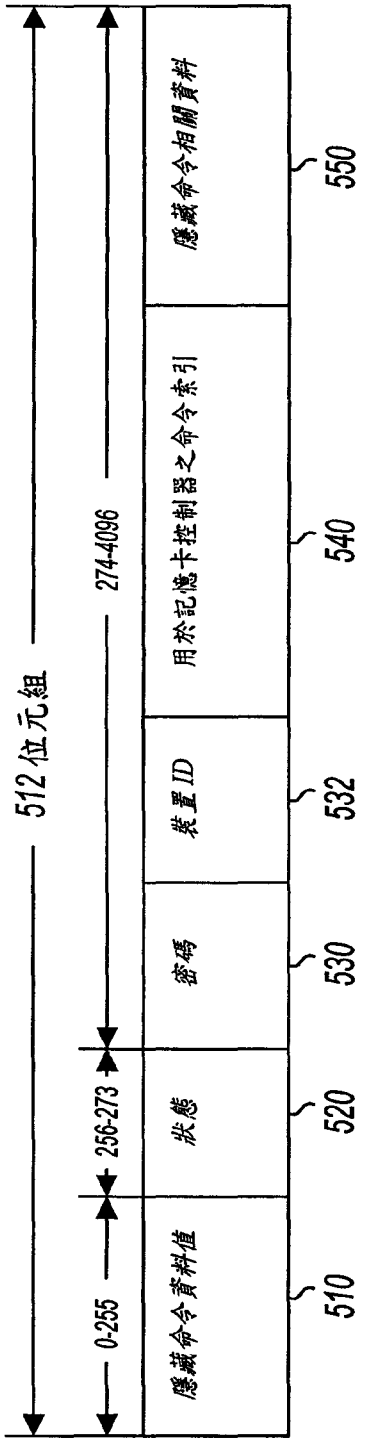
第 3A 圖


302
小型感應元件
350
記憶體
360
334
程式記憶體
智慧卡控制器
電力
記憶卡控制器
340
332
342
330
記憶體存取命令
電力
主機端介面
310

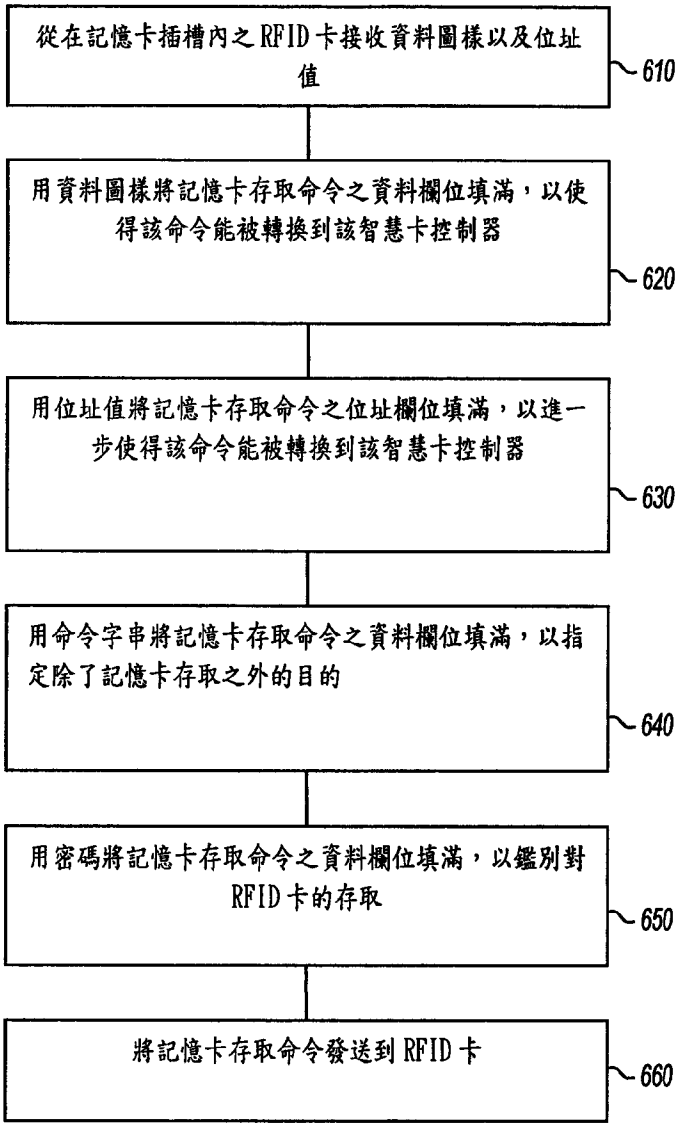
第 3B 圖



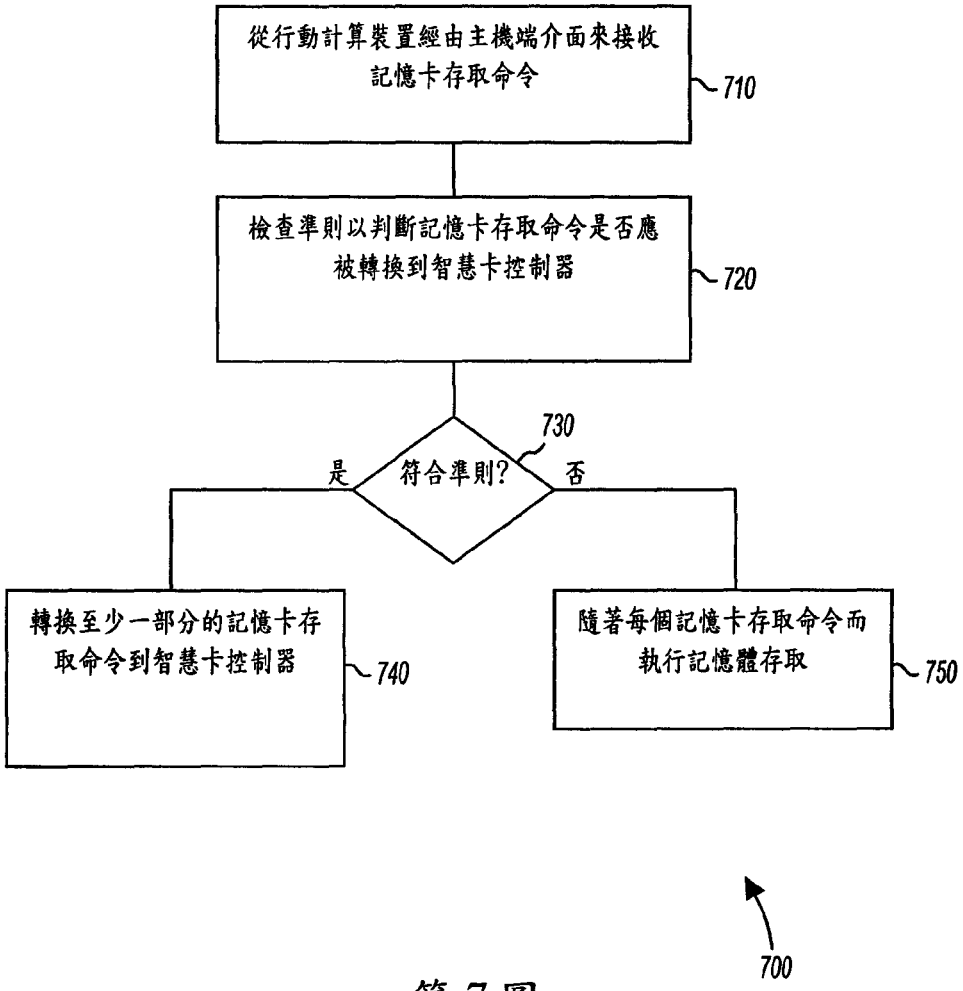
第 4 圖


512 位元組
274-4096
256-273
0-255
隱藏命令資料值
狀態
密碼
裝置 ID
用於記憶卡控制器之命令索引
隱藏命令相關資料
510
520
530
532
540
550

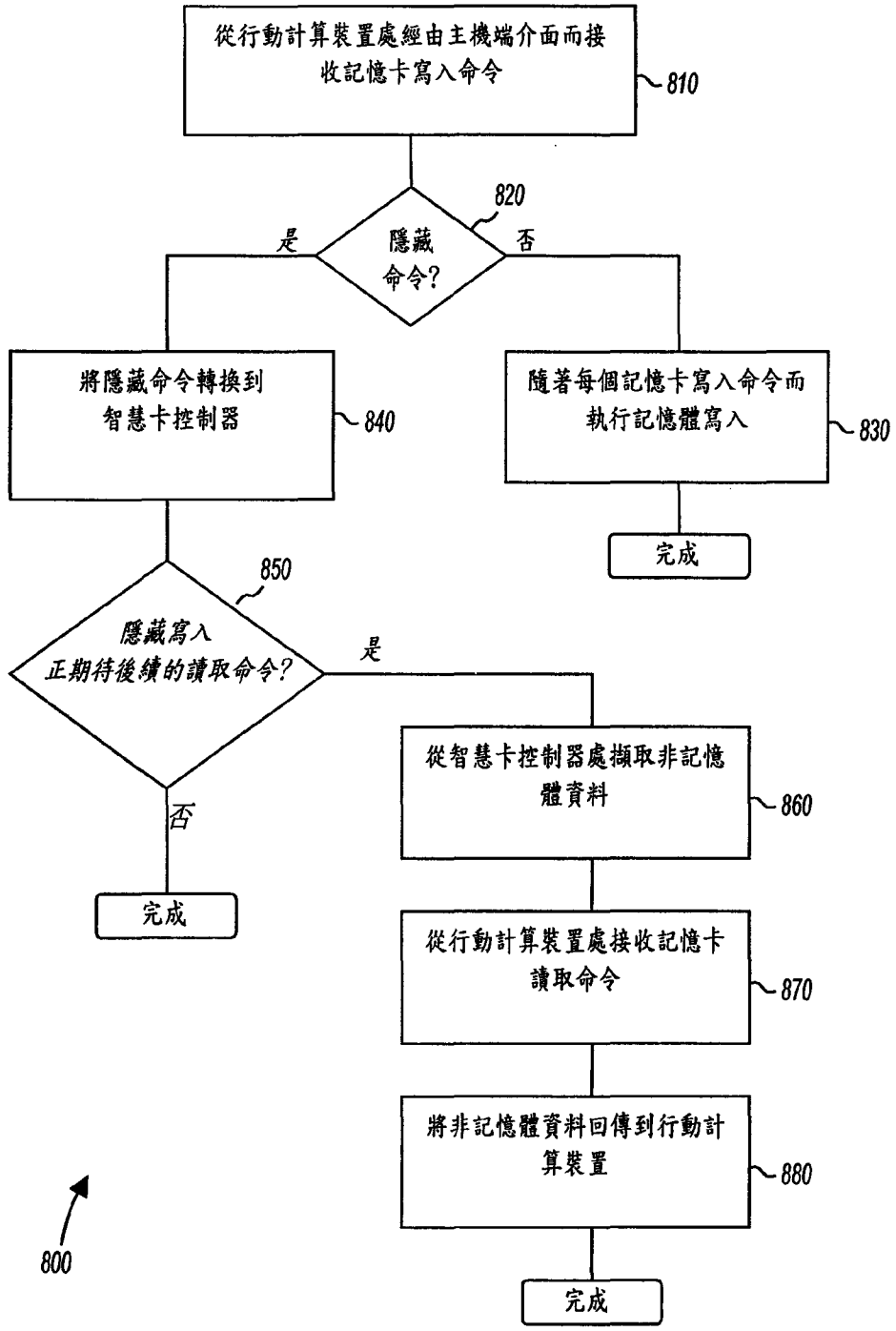
第 5 圖


從在記憶卡插槽內之 RFID 卡接收資料圖樣以及位址值
610
用資料圖樣將記憶卡存取命令之資料欄位填滿，以使得該命令能被轉換到該智慧卡控制器
620
用位址值將記憶卡存取命令之位址欄位填滿，以進一步使得該命令能被轉換到該智慧卡控制器
630
用命令字串將記憶卡存取命令之資料欄位填滿，以指定除了記憶卡存取之外的目的
640
用密碼將記憶卡存取命令之資料欄位填滿，以鑑別對 RFID 卡的存取
650
將記憶卡存取命令發送到 RFID 卡
660
600

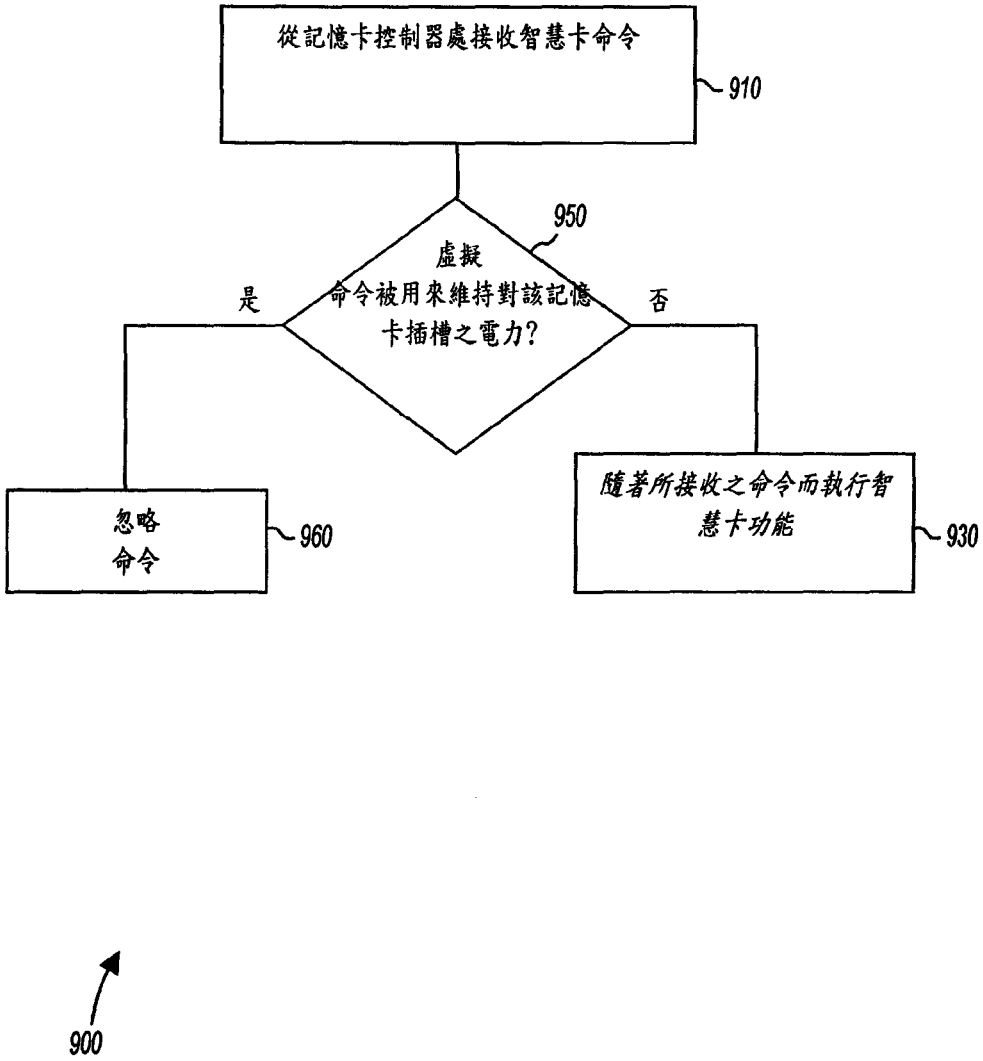
第 6 圖


從行動計算裝置經由主機端介面來接收記憶卡存取命令
710
檢查準則以判斷記憶卡存取命令是否應被轉換到智慧卡控制器
720
730
是
符合準則?
否
轉換至少一部分的記憶卡存取命令到智慧卡控制器
740
隨著每個記憶卡存取命令而執行記憶體存取
750
700

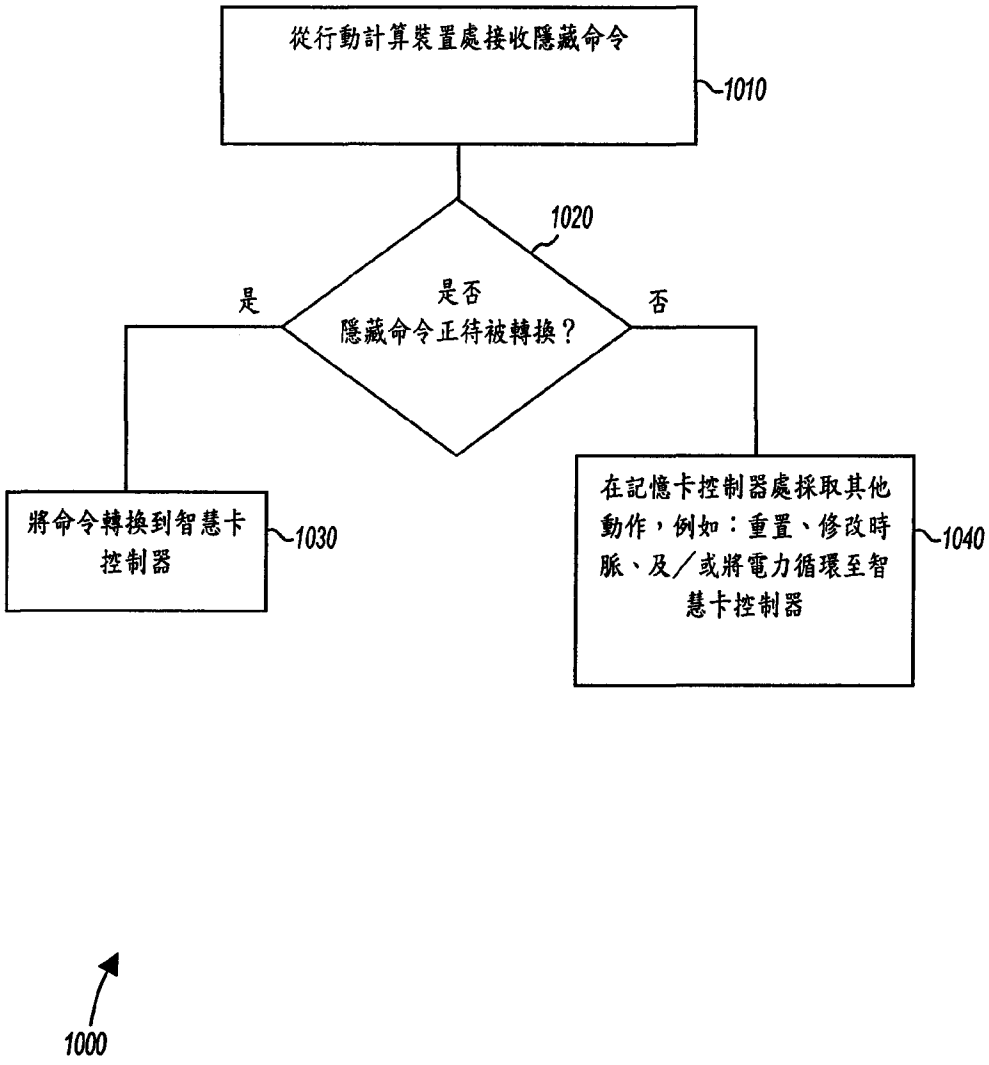
第 7 圖


從行動計算裝置處經由主機端介面而接收記憶卡寫入命令
810
820
隱藏命令?
是
否
將隱藏命令轉換到智慧卡控制器
840
隨著每個記憶卡寫入命令而執行記憶體寫入
830
完成
850
隱藏寫入正期待後續的讀取命令?
是
否
完成
從智慧卡控制器處擷取非記憶體資料
860
從行動計算裝置處接收記憶卡讀取命令
870
將非記憶體資料回傳到行動計算裝置
880
完成
800

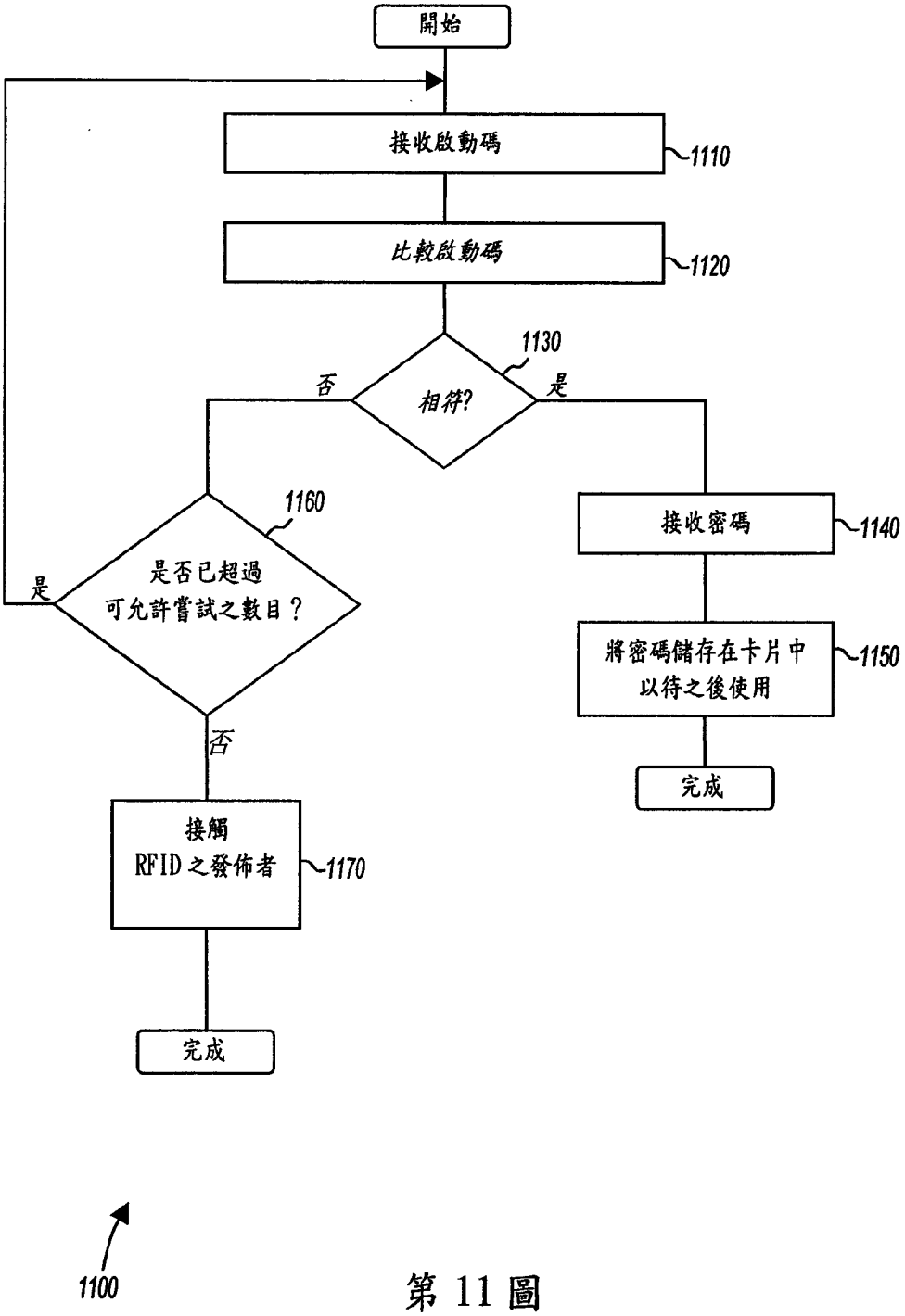
第 8 圖


從記憶卡控制器處接收智慧卡命令
910
950
虛擬
命令被用來維持對該記憶卡插槽之電力?
是
否
忽略
命令
960
隨著所接收之命令而執行智慧卡功能
930
900

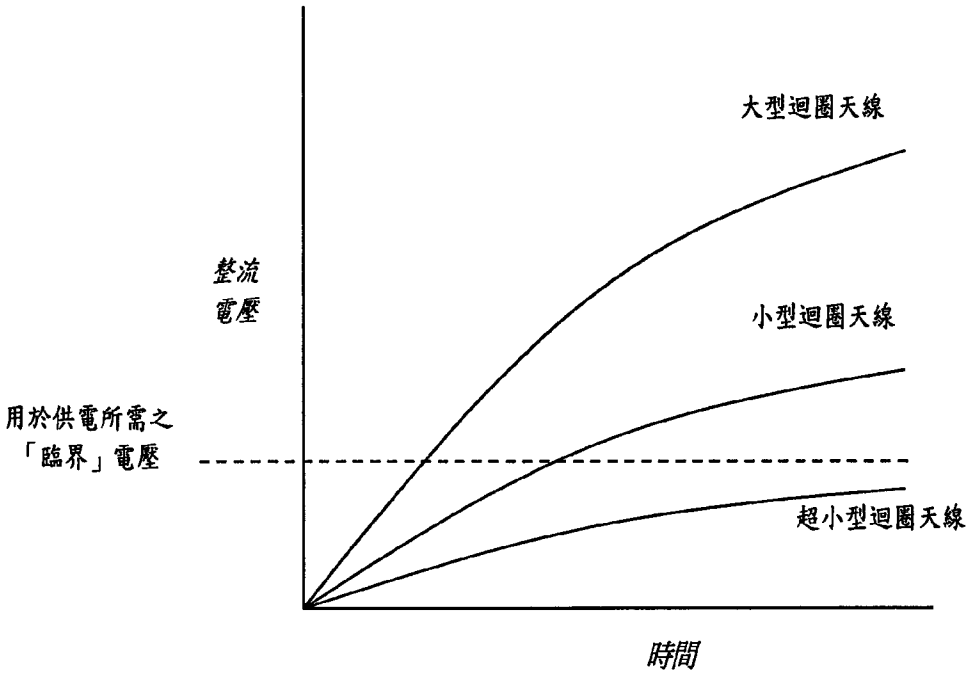
第 9 圖


從行動計算裝置處接收隱藏命令
1010
1020
是否
隱藏命令正待被轉換？
是
否
將命令轉換到智慧卡控制器
1030
在記憶卡控制器處採取其他動作，例如：重置、修改時脈、及／或將電力循環至智慧卡控制器
1040
1000

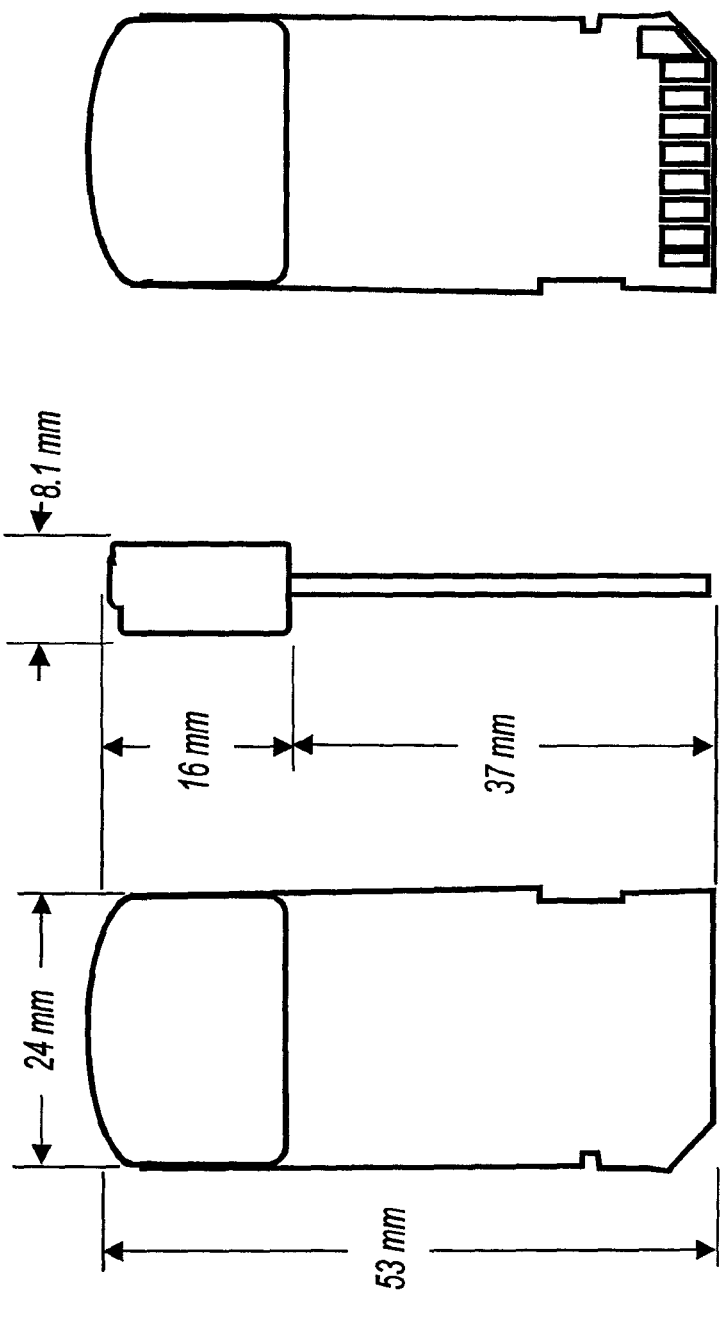
第 10 圖


開始
接收啟動碼
1110
比較啟動碼
1120
1130
相符?
否
是
1160
是否已超過
可允許嘗試之數目?
是
否
接收密碼
1140
將密碼儲存在卡片中
以待之後使用
1150
完成
接觸
RFID之發佈者
1170
完成
1100

第 11 圖



第 12 圖
(先前技術)



第 13 圖
(先前技術)

卡控制器 340、記憶體 360、智慧卡控制器 330、程式記憶體 332、以及小型感應元件 350。RFID 卡能夠與一在行動計算裝置內之記憶卡插槽進行通訊。進一步而言，RFID 卡 300 不需要記憶卡插槽來實作出延伸的輸入/輸出功能。例如，且非為限制，在 SD 的具體實施例中，RFID 卡 300 能運作在任何 SD 記憶卡插槽中，且不需要安全數位輸入輸出(SDIO)的記憶卡插槽。

主機端介面 310 包括電子接觸，以與記憶卡插槽交互聯繫。例如，主機端介面 310 包括了像是接觸 122(第 1 圖)般的接觸。同樣作為範例，在某些具體實施例中，主機端介面 310 包括了隱蔽的電子接觸。主機端介面 310 亦可包括像是驅動器、接收器、終端等等的電路。

在由第 3A 圖所表示之具體實施例中，記憶卡控制器 340 使用記憶卡存取命令來與行動裝置通訊。記憶卡控制器亦可與記憶體 360 通訊。記憶卡控制器判斷是否各命令應形成與記憶體 360 之記憶體運作、是否一隱藏命令應被轉換成智慧卡控制器 330、或是否記憶卡控制器 340 應該因應於隱藏命令而採取行動。在某些具體實施例中，記憶卡控制器 340 執行除存在一內部記憶體內或是儲存在記憶體 360 內之指令。在某些具體實施例中，記憶卡控制器 340 包括特殊目的硬體，其在判斷一命令是否應被轉換上很有用。在其他具體實施例中，記憶卡控制器 340 可為一在各方面都等同於在記憶卡中所找到之控制器的微控制器，除了其執行之程式之外。

IPR2025-00645 Page 00311

The English Translation of Patent Gazette for Laid-Open

Laid-open No. : 201126422

Laid-open date : August 1, 2011

Examination : Yes

Invention title : CONTACTLESS DEVICE WITH MINIATURIZED ANTENNA

Serial number : 99105179 Filing date : February 23, 2010

Priority claiming : 61/155,144

Inventors : NARENDRA, SIVA G. ; TADEPALLI, PRABHAKAR

Applicant : Tyfone, Inc.

Patent Attorney : Thomas Q. T. Tsai ; Victor S. C. Lee

Abstract : A contactless device includes a miniaturized antenna. The antenna includes an inductive coupling element that presents a field coupling surface area to couple to a magnetic field. The inductive element may be made of layers where conductive loops are formed parallel to the layers or perpendicular to the layers. When conductive loops are formed perpendicular to the layers, the effective field coupling surface area is increased. The inductive element is positioned on an outside edge of a memory card compatible device with the field coupling surface area perpendicular to the card.

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201126422 A1
(43)公開日： 中華民國 100 (2011) 年 08 月 01 日

(21)申請案號：099105179 (22)申請日： 中華民國 99 (2010) 年 02 月 23 日
(51)Int. Cl.： *G06K19/077 (2006.01)* *H01Q1/24 (2006.01)*
H01Q7/00 (2006.01)
(30)優先權：2009/02/24 美國 61/155,144
(71)申請人：泰豐股份有限公司 (美國) TYFONE, INC. (US)
美國
(72)發明人：納廉達西瓦G NARENDRA, SIVA G. (IN) ；塔迪帕里波拉伯哈卡爾 TADEPALLI, PRABHAKAR (IN)
(74)代理人：蔡坤財；李世章
申請實體審查：有 申請專利範圍項數：23 項 圖式數：0 共 23 頁

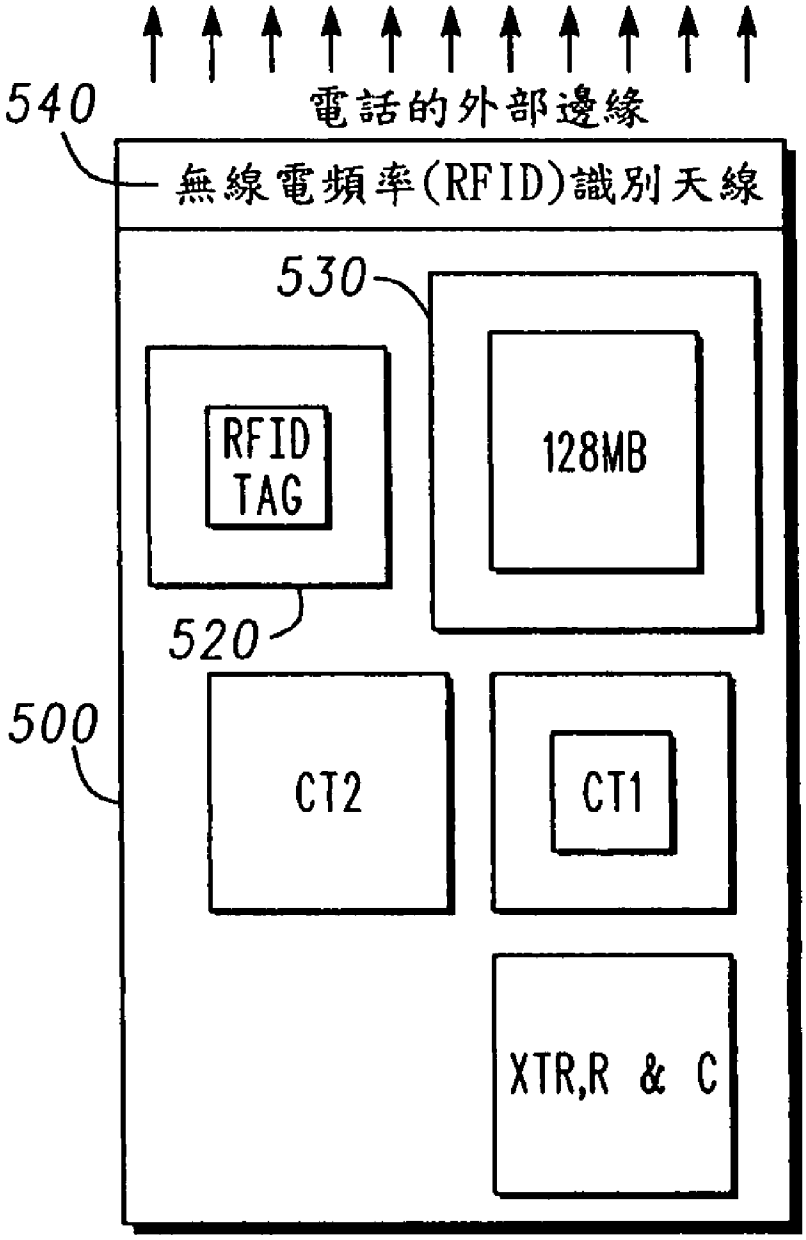
(54)名稱

具有微型天線的無觸點裝置

CONTACTLESS DEVICE WITH MINIATURIZED ANTENNA

(57)摘要

一無接觸裝置包括一微型天線。該天線包括一感應耦合元件，其顯露一電磁場耦合表面區域以耦合至一磁場。該感應元件可由分層所構成，其中導電迴圈之形成係平行於該分層或垂直於該分層。當導電迴圈之形成係垂直於該分層時，該有效電磁場耦合表面區域會被增加。該感應元件被置於一記憶卡相容裝置之一外部邊緣上，其電磁場耦合表面區域係垂直於該卡片。



500：記憶卡

520：無線電頻率識別記號(RFID)記號

530：記憶體

540：RFID 天線

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201126422 A1
(43)公開日： 中華民國 100 (2011) 年 08 月 01 日

(21)申請案號：099105179 (22)申請日： 中華民國 99 (2010) 年 02 月 23 日
(51)Int. Cl.： *G06K19/077 (2006.01)* *H01Q1/24 (2006.01)*
H01Q7/00 (2006.01)
(30)優先權：2009/02/24 美國 61/155,144
(71)申請人：泰豐股份有限公司 (美國) TYFONE, INC. (US)
美國
(72)發明人：納廉達西瓦G NARENDRA, SIVA G. (IN) ；塔迪帕里波拉伯哈卡爾 TADEPALLI, PRABHAKAR (IN)
(74)代理人：蔡坤財；李世章
申請實體審查：有 申請專利範圍項數：23 項 圖式數：0 共 23 頁

(54)名稱

具有微型天線的無觸點裝置

CONTACTLESS DEVICE WITH MINIATURIZED ANTENNA

(57)摘要

一無接觸裝置包括一微型天線。該天線包括一感應耦合元件，其顯露一電磁場耦合表面區域以耦合至一磁場。該感應元件可由分層所構成，其中導電迴圈之形成係平行於該分層或垂直於該分層。當導電迴圈之形成係垂直於該分層時，該有效電磁場耦合表面區域會被增加。該感應元件被置於一記憶卡相容裝置之一外部邊緣上，其電磁場耦合表面區域係垂直於該卡片。

201126422 第99105179號專利案99年6月修正

99年6月10日 補正

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：99105179

※ 申請日期：2010年2月23日 ※IPC 分類：

G06K 19/077 (2006.01)
H01Q 1/24 (2006.01)
H01Q 7/00 (2006.01)

一、發明名稱：（中文/英文）

具有微型天線的無觸點裝置

CONTACTLESS DEVICE WITH MINIATURIZED ANTENNA

二、中文發明摘要：

一無接觸裝置包括一微型天線。該天線包括一感應耦合元件，其顯露一電磁場耦合表面區域以耦合至一磁場。該感應元件可由分層所構成，其中導電迴圈之形成係平行於該分層或垂直於該分層。當導電迴圈之形成係垂直於該分層時，該有效電磁場耦合表面區域會被增加。該感應元件被置於一記憶卡相容裝置之一外部邊緣上，其電磁場耦合表面區域係垂直於該卡片。

三、英文發明摘要：

A contactless device includes a miniaturized antenna. The antenna includes an inductive coupling element that presents a field coupling surface area to couple to a magnetic field. The inductive element may be made of layers where conductive loops are formed parallel to the layers or perpendicular to the layers. When conductive loops are formed perpendicular to the layers, the effective field coupling surface area is increased. The inductive element is

IPR2025-00645 Page 00316

positioned on an outside edge of a memory card compatible device with the field coupling surface area perpendicular to the card.

四、指定代表圖：

(一)本案指定代表圖為：第（ 5 ）圖。

(二)本代表圖之元件符號簡單說明:

500 記憶卡

520 無線電頻率識別記號（RFID）記號

530 記憶體

540 RFID 天線

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【相關申請】

根據 35 U.S.C 19（e）由 Narendra et al. 於 2009 年 2 月 24 日請求美國臨時申請案案號 61/155,144，發明名稱「具有微型天線的無觸點裝置」，其已於此處併入參考。

【發明所屬之技術領域】

本發明一般係與無接觸裝置有關，更特言之係與微型無接觸裝置有關。

【先前技術】

第 1A、1B、2A 及 2B 圖顯示先前技術。第 1A 及 1B 圖顯示與基板平行之天線。此典型為包括無接觸技術之信用卡。第 2A 及 2B 圖顯示先前技術卡片，其被實質平行於該讀卡機加以拿持以從該讀卡機耦合磁性能量至該線圈。

【發明內容】

一感應元件，其包含一底部表面及多個與該底部表面實質平行的分層，該多個分層包括導電材料及電性絕緣材料之一組合，因而當彼此結合時該多個分層形成至少一導電線圈，該導電線圈具有與該底部表面實質垂直的一電磁場耦合表面區域。

一種多層感應耦合元件，其包含一下層，其含有具有

軌跡終端之至少一導電平面軌跡；至少一中間層，其具有導電穿越軌跡，該導電穿越軌跡之位置係用以電性接觸該下層上的該軌跡終端及一上層，其具有至少一對準之導電平面軌跡以電性接觸該導電穿越軌跡以形成具有至少一匝的一導電線圈。

一電子裝置，包含一電路板，其具有一記憶卡插槽介面；一無接觸通信裝置，其附著於該電路板，該無接觸通信裝置具有一天線埠及一感應元件，其附著於該電路板且與該天線埠電性耦合，該感應元件具有一導電線圈，該導電線圈具有與該電路板實質垂直的一電磁場耦合表面區域。

一種設備，其包含一記憶卡相容基板，其具有至少一表面、一內部邊緣以及與該內部邊緣相對的一外部邊緣；電子接觸，其位於該至少一表面上且沿著該內部邊緣放置以及一導電線圈，其沿著該外部邊緣放置，該導電線圈具有與該至少一平面實質垂直的一電磁場耦合表面區域。

一設備，其至少包含一記憶卡相容基板，其具有至少一表面、一內部邊緣以及相對於該內部邊緣的一外部邊緣；電子接觸，其位於該至少一表面上且沿著該內部邊緣放置以及一三維導電線圈，其沿著該外部邊緣放置。

IPR2025-00645 Page 00320

【實施方式】

在以下實施方式中，本發明之各種實施例將參照顯示之附隨圖示加以說明。這些實施例係以足夠細節加以描述以使本發明所屬技術領域中具有通常知識者實施本發明。將了解本發明之各種實施例雖然彼此不同但卻不必然相互排除。舉例來說，結合一實施例加以描述之一特定特徵、結構或特性可被實施於其他實施例中而不會偏離本發明之範圍。此外，將了解各個被揭露之實施例中個別元件的位置或配置可加以修改而不會偏離本發明之範圍。因此，以下實施方式不可被視為一限制意義，而本發明之範圍僅由適當解釋該附加申請專利範圍並伴隨該附加申請專利範圍被賦予之所有均等物範圍加以定義。在該圖示中，各圖示之類似編號係指相同或類似的功能。

第 3 圖顯示該先前技術天線將如何影響一記憶卡之使用。若一記憶卡 320 具有一環狀天線平行該基板纏繞，則該卡將如圖示平行於該讀卡機加以拿持。

第 4 圖顯示該先前技術天線將如何影響一記憶卡於插入至一行動裝置時的使用。該電磁場係垂直於該讀卡機 410 流動。若該記憶卡 320 具有平行該基板繞線之一環狀天線，則該行動裝置 420 將如第 4 圖中所示平行於該讀卡機加以拿持。為了消費者之便利，該記憶卡通常不

會自該行動裝置 420 取出。若該行動裝置 420 係如第 4 圖所示加以拿持，則由於在該記憶卡天線及該讀卡機 410 之間有其他金屬區域而使該系統可能無法運作。這些其他金屬區域可能是該行動裝置內部的記憶卡固定槽以及該行動裝置之印刷電路板（PCB）金屬路徑及元件/焊錫。因此，源自該讀卡機 410 之電磁場可能會因為被其他金屬區域吸收而無法到達該天線之導體金屬。

第 5 圖顯示一微型天線在一記憶卡上的放置。記憶卡 500 被顯示為具有無線電頻率識別記號（RFID）標記 520、RFID 天線 540、記憶體 530 以及各種其他元件。該微型天線 540 係由一感應裝置以至少一線圈所形成。該感應裝置如圖所示被置於該記憶卡 500 之外層邊緣。該記憶卡 500 可為任何格式，包括安全數位（SD）、小型 SD（mini-SD）、微型 SD（micro-SD）等等。

為了允許擷取源自該讀卡機而垂直於該讀卡機流動的電磁場，該微型天線 540 被置於該記憶卡 500 的最邊緣，因而當被插入至一行動裝置時，該微型天線 540 靠近該記憶卡插槽的外部邊緣。

本發明之各種實施例提供製造一感應線圈小到足以被置於該外部邊緣的方法，且該線圈之放置及定位可允許源自該讀卡機之電磁場流入該天線。

第 6 圖顯示一微型天線在一記憶卡上的定位。微型天線 540 為裝入一填充材料 614 中的一三維（3D）感應線圈。該感應裝置如圖示被置於該記憶卡的外部邊緣。天

線 540 之定位係使源自讀卡機 410 的電磁場耦合至該天線的 3D 感應線圈。該記憶卡可為各種格式，包括安全數位（SD）、mini-SD、micro-SD 等等。

第 7 圖顯示一記憶卡關於一讀卡機的定位。記憶卡 500 包括位於該卡片之邊緣的一微型天線。參照第 5 及 6 圖。當該天線被置於如第 6 圖中所示之記憶卡 500 之上時，該記憶卡 500 可如第 7 圖中所示被垂直於該讀卡機 410 加以放置。

第 8 圖顯示一行動裝置關於一讀卡機的定位。當第 7 圖之記憶卡 500 被插入至第 8 圖中的行動裝置 420 時，則該行動裝置 420 可如圖中所示加以定位。此允許該電磁場進入位於該記憶卡 500 之邊緣的天線而不需首先滲透該行動裝置之背後。

第 9 圖顯示一微型天線關於源自一讀卡機之一磁場的定位。讀卡機 410 射出一特定頻率如 13.56MHz 之電磁能量。如前所述，該微型天線包括一感應線圈 612。設計該線圈 612 以盡量耦合源自讀卡機 410 的磁場。

該讀卡機線圈以及該感應線圈 612 可被視為一變壓器中的兩線圈。該讀卡機線圈為固定的，而設計該線圈 612 為該變壓器之第二線圈，其耦合源自該讀卡機線圈（主線圈）之電磁場。最大化該感應線圈 612 的耦合區域江將增加該讀卡機線圈與該天線線圈之間的耦合。

第 10 圖顯示變壓器設計。該讀卡機（該變壓器的主要線圈）被顯示係由電感 L1、串列電阻 RL1、串列電容 C1S

IPR2025-00645 Page 00323

以及並列電容 C1P 所構成。該微型天線（該感應器的第二線圈）被顯示係由電感 L2、串列電阻 RL2 以及並列電阻 C2 所構成。

變壓器耦合本身並不適用一確切設計程序，因有許多因素會影響耦合程度。該線圈之幾何、線圈之間的空間、使用的線心材料以及屏蔽等均對任何設計所獲取之耦合程度有一顯著影響。降低該主要及第二線圈之間的空間會增加該耦合。增加磁路的磁導性會增加該耦合。而屏蔽一變壓器會降低其負載的 Q 因而有增加該耦合的效果。

第 11 圖顯示依據本發明之各種實施例之方法的一流程圖。流程圖 1100 討論於設計一第二變壓器線圈供使用作為一微型天線時將考慮的參數。於 1110 可了解為了有效耦合，該第二變壓器線圈應緊密耦合至該讀卡機線圈，該讀卡機線圈實質共振於 13.56MHz，且具有一高的 Q，但因 Q 將限制頻寬（BW）故不會太高。

於 1120 可了解耦合與表面區域密切相關，而電感與匝數量密切相關。於 1130 可了解對於任何特定電感值而言，可藉由調整一外部電容的數值而達成調整共振。

於 1140 選擇該表面區域以最大化耦合，選擇該線圈中的匝數以定義該電感，而選擇導線的寬度/長度以增加 Q。

第 12-14 圖顯示微型天線。第 12 及 13 圖顯示適合使用作為一記憶卡之一外部邊緣之一微型天線的一感應元件。該側視圖為使用時暴露於該磁場的方向。第 12 圖定

IPR2025-00645 Page 00324

義『A』為總長度，『B』為總高度，而『C』為總深度。第 12 圖亦定義『D』為耦合該線圈至該記憶卡之感應終端區域的長度。當使用於一 SD 格式時的示範尺寸為 A=10.4mm、B=0.7mm、C=2mm 及 D=0.5mm。這些尺寸僅被提供作為範例，且本發明之各種實施例並不如此受限。舉例來說，用於一 micro-SD 卡的一感應元件一般會具有較小尺寸。

第 14 圖顯示進入該感應元件之側視圖的磁場。第 14 圖亦定義該電磁場耦合表面區域 1410。當被裝設於一電路板上時，該電磁場耦合表面區域係實質垂直於該電路板。

該天線的機械結構佔據之三維為長度 A、高度 B 及深度 C。該結構包括金屬 1420 以供形成該線圈以及一填充材料 1430 以佔據剩餘空間。該填充材料 1430 可為金屬材料或陶瓷材料的一複合物。用於該 3D 線圈的金屬繞線係佔據描繪該天線之長度及高度的週長以形成一匝。額外的匝係藉由重複沿著該深度描繪之週長所完成，其於鄰接的匝之間具有歐姆連接以建立一連續的矩形線圈如一矩形彈簧。

該電磁場耦合表面區域 1410 為沿著形成該週長描邊之兩維度的表面區域。此區域從一外部表面（例如讀卡機 410）耦合該電磁場至該 3D 天線線圈而感應電壓及電流於該 3D 天線線圈中。

在某些實施例中，天線 540 被置於該記憶卡 500 中因

IPR2025-00645 Page 00325

而該線圈之長度配合當該記憶卡被插入至一主機裝置時其將具有之外部邊緣。該記憶卡之內部邊緣係於將具有該電子連接器以供該記憶卡匯流排連接至該記憶卡插槽之處。

在某些實施例中，天線 540 被置於該記憶卡 500 中，因而當該記憶卡被插入至一主機裝置中時該線圈之長度係對齊該記憶卡將具有的外部邊緣。該記憶卡之內部邊緣所在之處為

在某些實施例中，定位天線 540 而使得該記憶卡被插入至一主機裝置時該電磁場耦合表面區域 1410 係與該主機裝置之外部表面平行。此定位將使源自該外部來源的入射支配電磁場與該電磁場耦合表面區域成 90 度。此定位組合該配置將使該電磁場耦合表面區域最為接近該主機的外部表面，藉以最大化該 3D 線圈中由於一外部電磁場來源的感應電壓及電流。

第 15 圖顯示感應線圈的尺寸。如該上視圖中所示，一單一天線可包括數個平行的線圈。在第 15 圖之範例中包括 M=6 之線圈，其中各線圈之 N=5.5 匝，然而 M 及 N 可採用任何數值。該導體長度為 2(Ai+Bi+2w)(N-0.5)+Ai，其中 Ai 及 Bi 為該線圈之內部尺寸，而 w 為該導體之寬度。如該側視圖所示，該有效耦合表面面積於 f 及 w 保持為小以最大化 Bi 時會被增加。

第 16 圖顯示依據本發明之各種實施例之設計處理方

法的一流程圖。於 1610 提供該手動繞線及讀取距離測量。於 1620 選擇該耦合表面區域、匝數以及導線的寬度/長度。參見第 11 圖。

於 1630 給予該尺寸 A、B、C 及 D。這些數值受限於該記憶卡的形狀係數。於 1632 最大化 Ai 及 Bi 以最大化耦合。現在回頭參照第 15 圖，該圖顯示該電磁場耦合表面區域會隨 Ai 及 Bi 增加而增加。

於 1634，M 被用於盡可能增加 Q（降低該 DC 電阻）。此對應至增加平行線圈的數量 M。參照第 15 圖。於 1636 選擇 N 以達到所需電感，考量到增加的匝數 N 將增加直流電阻並降低 Q。

於 1638 測量該讀取距離。可修改各種參數並於一重複處理中量測該讀取距離。於 1650 定案各種參數以達到一最終設計。可定案該直流電阻、該電感、該材料以及該尺寸 A、B、C 及 D。在該印刷電路板上的外部電容（參見第 10 圖之 C2）亦可於給定該電感及所需之 13.56 MHz 共振時加以定案。

第 17 及 18 圖顯示依據本發明之各種實施例的感應元件層。各分層包括導電材料及絕緣材料。第 17 圖顯示形成一表面黏著感應元件的一傳統方法。每一層包括一導電迴圈，而該分層於堆疊時會形成多重導電迴圈。該最小尺寸 w（第 15 圖）受限於處理需求。該電感被黏著於該電路板上之『側邊』以顯露該電磁場耦合表面區域於該卡片之外部邊緣。在這些實施例中，該分層係垂直於

IPR2025-00645 Page 00327

該電路板。第 18 圖顯示一增進的製造方法。每一分層僅形成一導電迴圈的一部分。舉例來說，現在參照第 19 圖，該底層 1970 包括具有軌跡終端（trace ends）的軌跡。中間層 1920、1930、1940、1950 及 1960 包括穿越軌跡，其位於用以電性接觸位於該較低層上之軌跡終端的位置，而上層 1910 至少具有一對準的導電表面軌跡以電性接觸該導電的穿越軌跡以形成具有至少一匝的一導電線圈。位於分層 1910 及 1970 上的軌跡可位於該基板的任一側。

在某些實施例中，該感應元件包括磁性材料，因而一電磁核心係形成於該導電線圈之中。再者，於某些實施例中，該感應元件包括位於該導電線圈外部的磁性材料。

第 20-23 圖顯示依據本發明之各種實施例之感應元件的剖面圖。第 21 及 23 圖顯示使用位於相同平面之分層作為該電磁場耦合表面區域所做成的感應元件。第 21 及 22 圖顯示使用垂直於該電磁場耦合表面區域之分層所做成的感應元件。注意該軌跡之寬度 w 在第 21 及 22 圖中較小，藉以增加該有效的電磁場耦合表面區域。於第 22 及 23 圖中藉由延伸該導電軌跡至該裝置之終端而進一步被增加該有效的電磁場耦合表面區域。

雖然已結合特定實施例描述本發明，但將了解可採用修改及變化而不會偏離本發明之範圍，如本發明所屬技術領域中具有通常知識者可輕易了解者。此修改及變化將被視為位於本發明及附加申請專利範圍之範圍中。

IPR2025-00645 Page 00328

【圖式簡單說明】

第 1A、1B、2A 及 2B 圖顯示先前技術之無接觸卡片以及其使用；

第 3 圖顯示該先前技術天線將如何影響一記憶卡的使用；

第 4 圖顯示該先前技術天線將如何影響一記憶卡被插入至一行動裝置時的使用；

第 5 圖顯示一微型天線在一記憶卡上的放置；

第 6 圖顯示一微型天線在一記憶卡上的定位；

第 7 圖顯示一記憶卡關於一讀卡機的定位；

第 8 圖顯示一行動裝置相對於一讀卡機的定位；

第 9 圖顯示一微型天線相對於一讀卡機所發射之一磁場的定位；

第 10 圖顯示一變壓器的設計；

第 11 圖顯示依據本發明之各種實施例之方法的一流程圖；

第 12-14 圖顯示微型天線；

第 15 圖顯示感應線圈的尺寸；

第 16 圖顯示依據本發明之各種實施例之方法的一流程圖；

第 17 及 18 圖顯示依據本發明之各種實施例的感應元件層；

IPR2025-00645 Page 00329

第 19 圖顯示一感應元件的分層；及

第 20-23 圖顯示依據本發明之各種實施例之感應元件的剖面圖。

【主要元件符號說明】

320 記憶卡

310, 410, 610 讀卡機

420 行動裝置

500 記憶卡

520 無線電頻率識別記號（RFID）記號

530 記憶體

540 RFID 天線

550 記憶體

612 線圈

614, 1430 填充材料

1100 流程圖

1410 電磁場耦合表面區域

1420 金屬

1110, 1120, 1130, 1140, 1610, 1620, 1630, 1632, 1634, 1636, 1638, 1650 步驟

1910 上層

1920, 1930, 1940, 1950 中間層

1970 底層

IPR2025-00645 Page 00330

七、申請專利範圍：

1. 一感應元件，其包含：

一底部表面；及

多個與該底部表面實質平行的分層，該多個分層包括導電材料及電性絕緣材料之一組合(combination)，因而當彼此結合時該多個分層形成至少一導電線圈，該導電線圈具有與該底部表面實質垂直的一電磁場耦合表面區域。

2. 如申請專利範圍第1項所述之感應元件，更包含：該底部表面上的結合區域。

3. 如申請專利範圍第1項所述之感應元件，其中該多個分層包括磁性材料，其形成一磁性核心於該至少一導電線圈中。

4. 一種多層感應耦合元件，其包含：

一下層，其含有具有軌跡終端之至少一導電平面軌跡；

至少一中間層，其具有導電穿越軌跡，該導電穿越軌跡之位置係用以電性接觸該下層上的該軌跡終端；及

一上層，其具有至少一對準之導電平面軌跡以電

IPR2025-00645 Page 00331

性接觸該導電穿越軌跡以形成具有至少一匝的一導電線圈。

5. 如申請專利範圍第 4 項所述之多層感應耦合元件，其中該至少一中間層包含：磁性材料，其位於該穿越軌跡之間。

6. 如申請專利範圍第 4 項所述之多層感應耦合元件，其中該下層包括：置於該軌跡終端之上的磁性材料。

7. 如申請專利範圍第 4 項所述之多層感應耦合元件，更包含：位於該下層之下的一底部層，該底部層包括磁性材料置於該下層中至少一導電軌跡之下。

8. 一電子裝置，包含：

一電路板，其具有一記憶卡插槽介面；

一無接觸通信裝置，其附著於該電路板，該無接觸通信裝置具有一天線埠；及

一感應元件，其附著於該電路板且與該天線埠電性耦合，該感應元件具有一導電線圈，該導電線圈具有與該電路板實質垂直的一電磁場耦合表面區域。

9. 如申請專利範圍第 8 項所述之電子裝置，其中該感應元件包含一多層表面黏著電感。

IPR2025-00645 Page 00332

10. 如申請專利範圍第9項所述之電子裝置，其中該多層表面黏著電感係以實質與該電路板平行之分層(layers)所形成。

11. 如申請專利範圍第9項所述之電子裝置，其中該多層表面黏著電感係以實質與該電路板垂直之分層所形成。

12. 如申請專利範圍第8項所述之電子裝置，其中該記憶卡插槽介面包含一安全數位（SD）相容介面。

13. 如申請專利範圍第8項所述之電子裝置，其中該記憶卡插槽介面包含一微型安全數位（microSD）相容介面。

14. 如申請專利範圍第8項所述之電子裝置，其中該記憶卡插槽介面包含一小型安全數位(miniSD)相容介面。

15. 一種設備，其包含：

一記憶卡相容基板，其具有至少一表面、一內部邊緣以及與該內部邊緣相對的一外部邊緣；

電子接觸，其位於該至少一表面上且沿著該內部邊緣放置；以及

IPR2025-00645 Page 00333

一導電線圈，其沿著該外部邊緣放置，該導電線圈具有與該至少一平面實質垂直的一電磁場耦合表面區域。

16. 如申請專利範圍第 15 項所述之設備，其中：

該至少一表面包括彼此實質平行的一頂部表面以及一底部表面；以及

該電性接觸係位於該頂部表面及該導電線圈係位於該頂部表面。

17. 如申請專利範圍第 15 項所述之設備，其中：

該至少一表面包括彼此實質平行的一頂部表面以及一底部表面；以及

該電性接觸係位於該頂部表面，而該導電線圈係位於該底部表面。

18. 如申請專利範圍第 15 項所述之設備，其中該導電線圈包含一多層表面黏著電感。

19. 如申請專利範圍第 18 項所述之設備，其中該多層表面黏著電感係以實質平行於該至少一表面的層所形成。

20. 如申請專利範圍第 18 項所述之設備，其中該多層表

IPR2025-00645 Page 00334

面黏著電感係以實質垂直於該至少一表面的層所形成。

21. 一設備，其至少包含：

一記憶卡相容基板，其具有至少一表面、一內部邊緣以及相對於該內部邊緣的一外部邊緣；

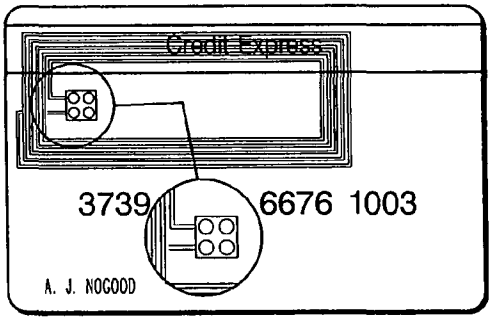
電子接觸，其位於該至少一表面上且沿著該內部邊緣放置；以及

一三維導電線圈，其沿著該外部邊緣放置。

22. 如申請專利範圍第 21 項所述之設備，其中該設備具有一微型安全數位（microSD）形狀係數。

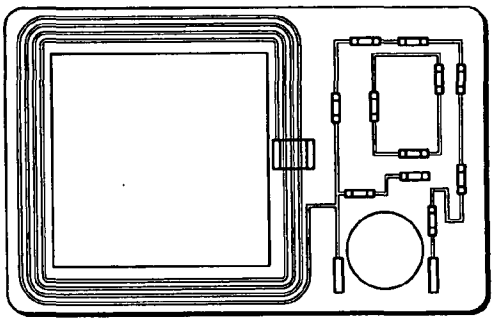
23. 如申請專利範圍第 22 項所述之設備，其中該三維導電線圈具有與該記憶卡之至少一表面實質垂直的一電磁場耦合表面區域。

IPR2025-00645 Page 00335



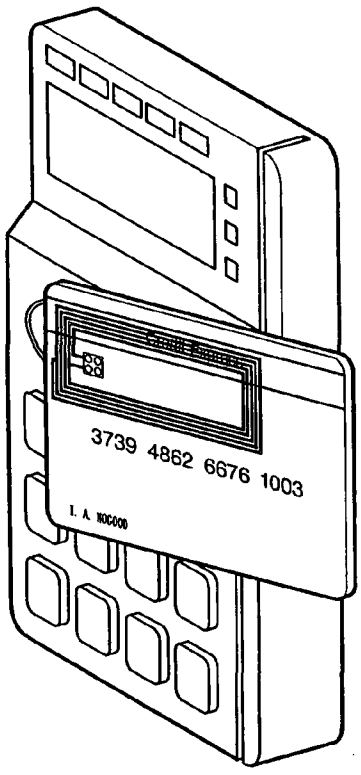
- 先前技術 -

第1A圖



- 先前技術 -

第1B圖

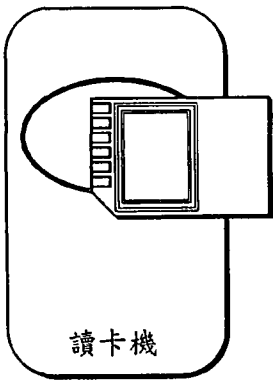


- 先前技術 -

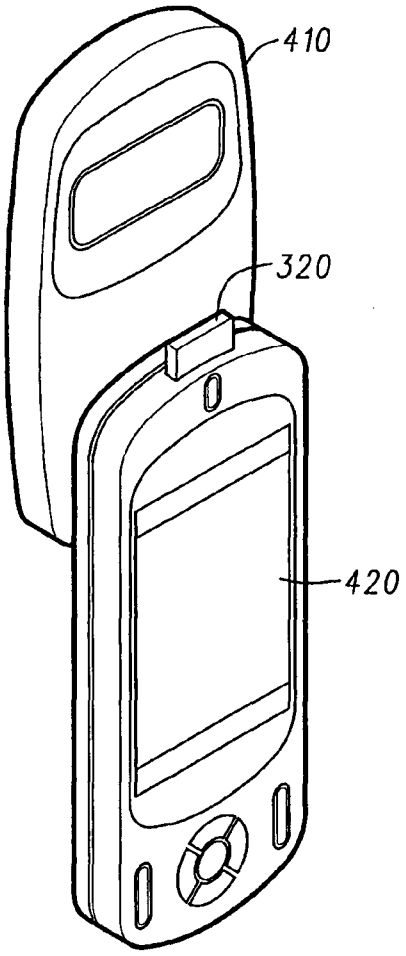
第2A圖

- 先前技術 -

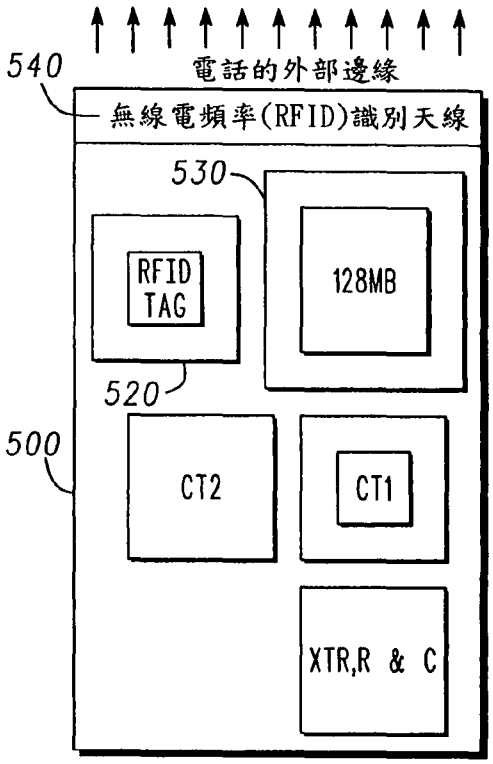
第2B圖



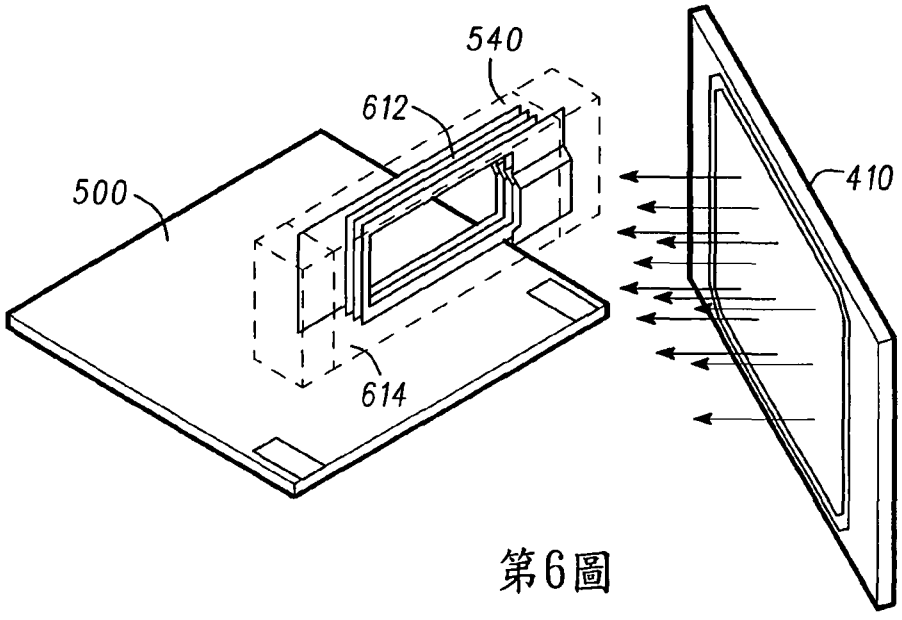
第3圖


410
320
420

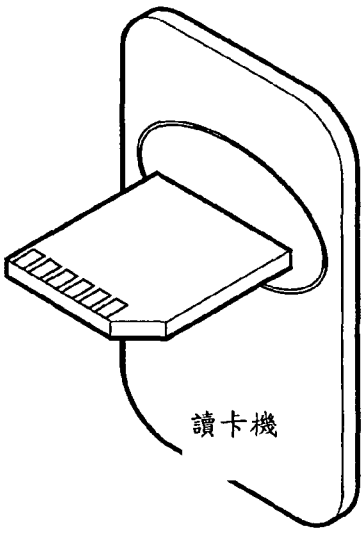
第4圖


電話的外部邊緣
540
無線電頻率(RFID)識別天線
530
RFID TAG
128MB
520
500
CT2
CT1
XTR,R & C

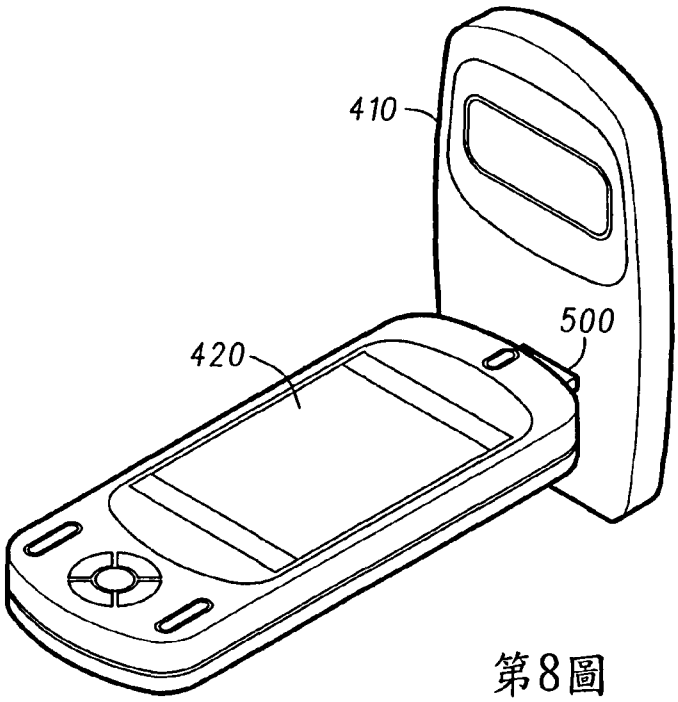
第5圖


540
612
500
410
614

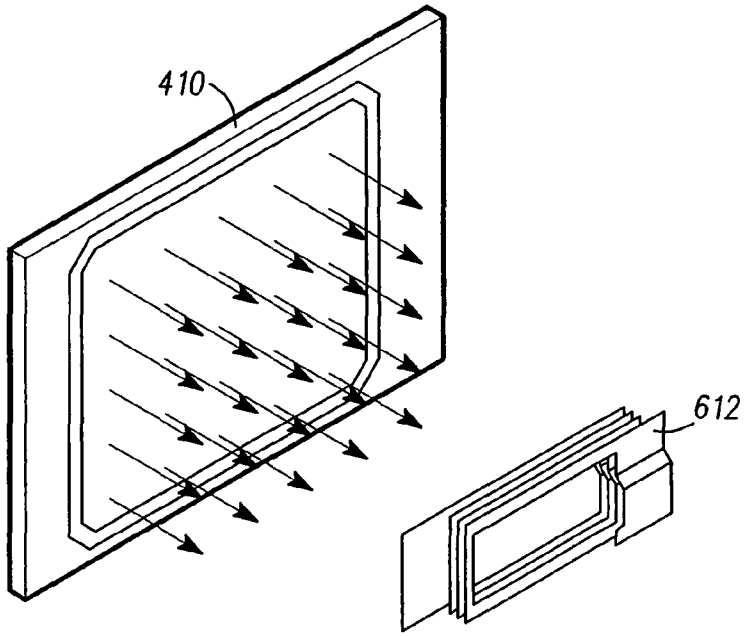
第6圖



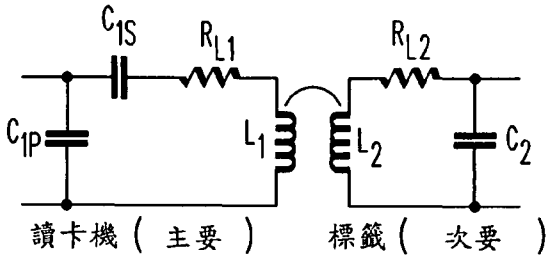
第7圖



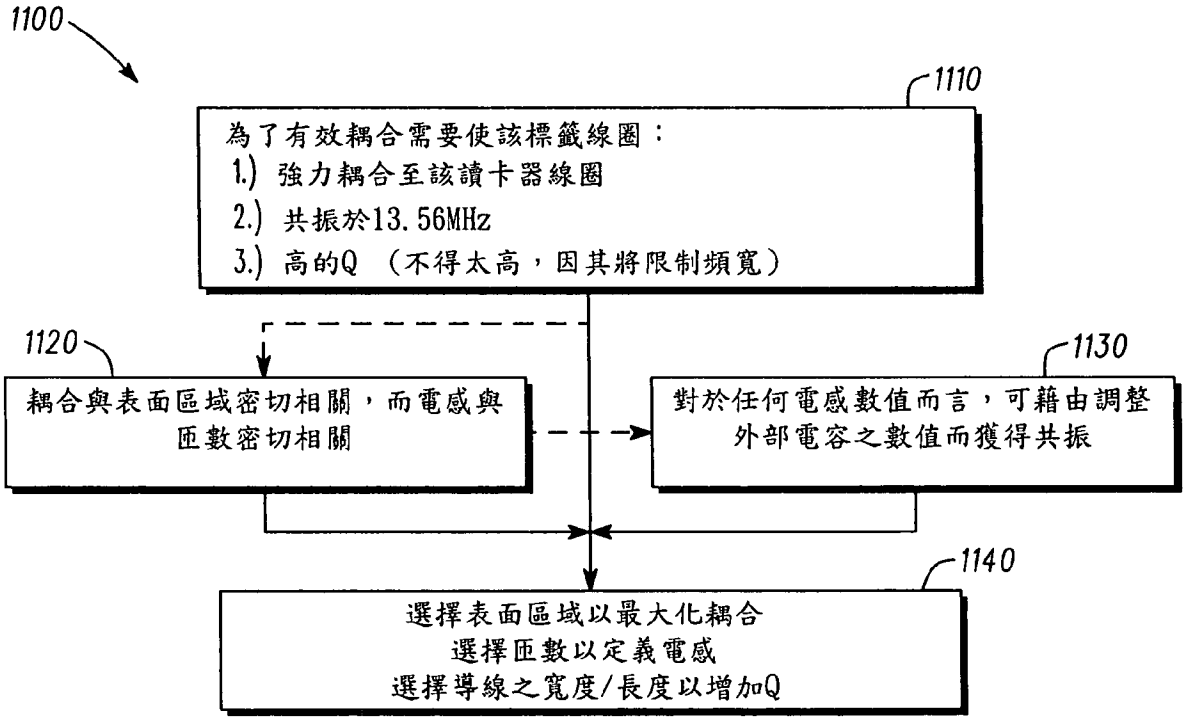
第8圖



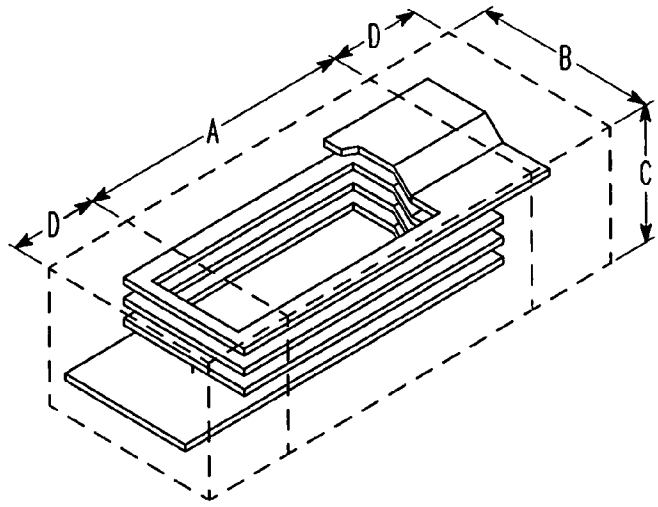
第9圖



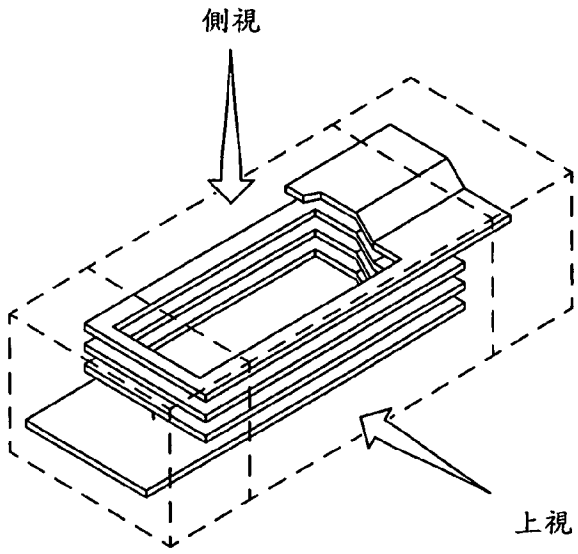
第10圖



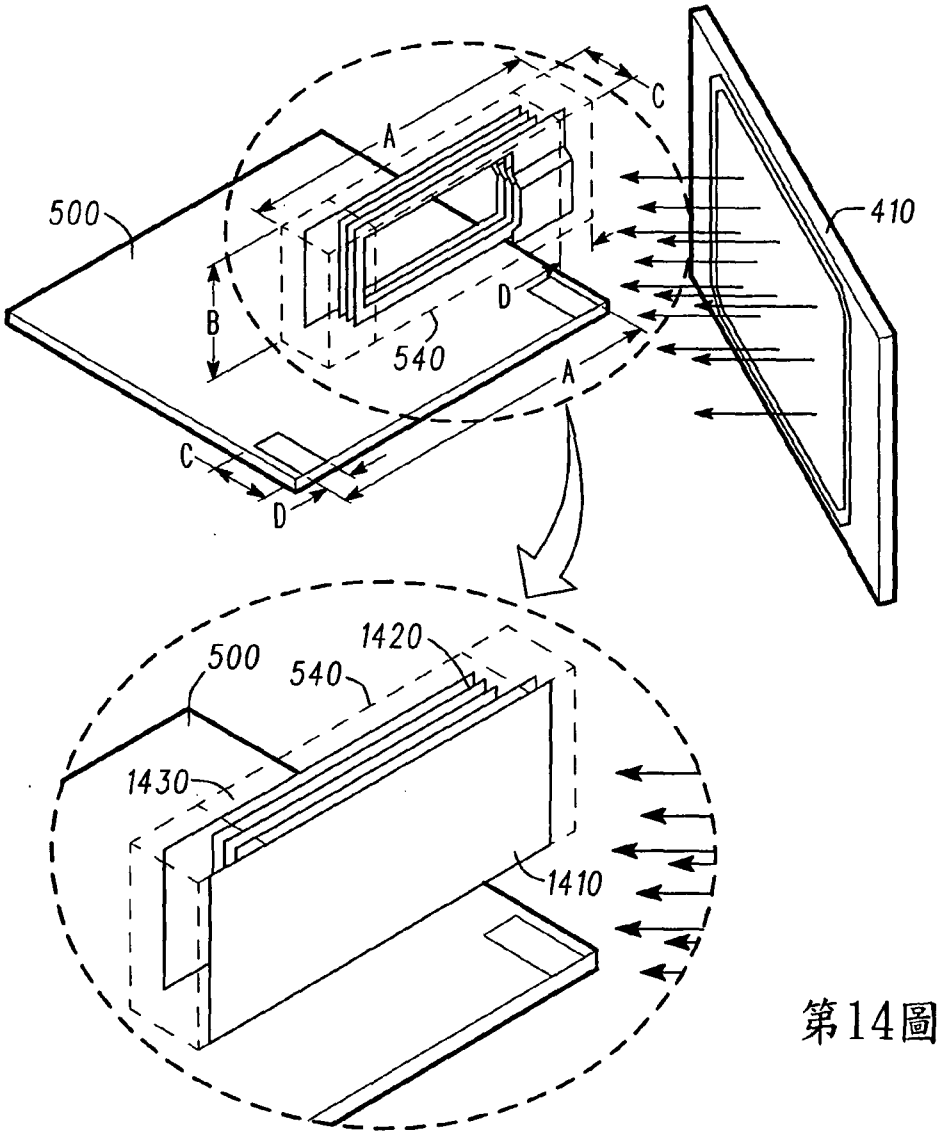
第11圖



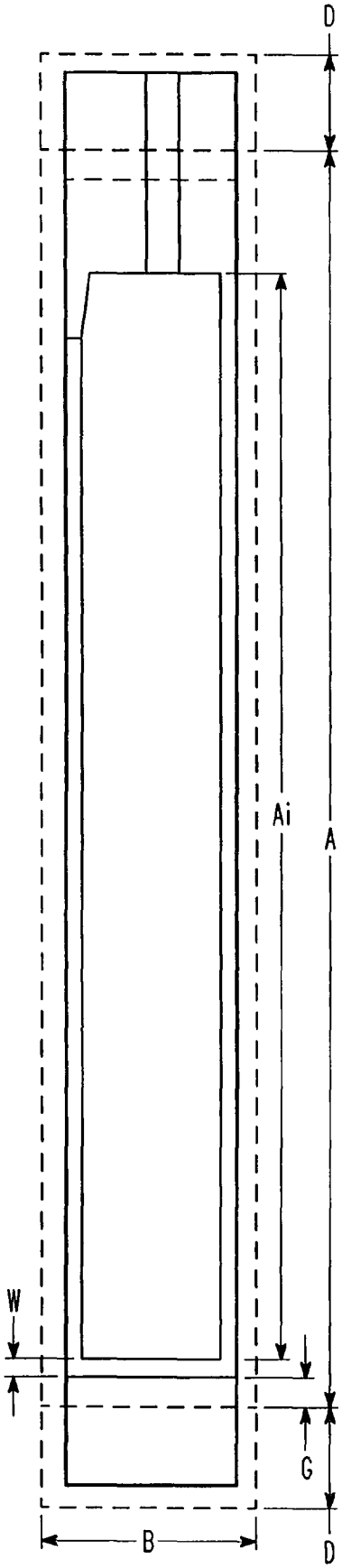
第12圖



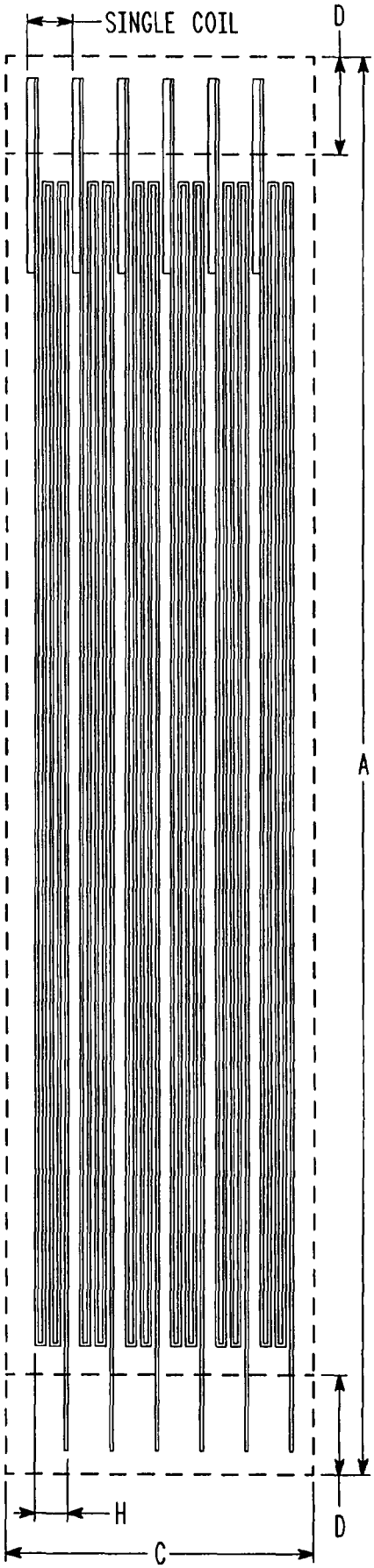
第13圖



第14圖

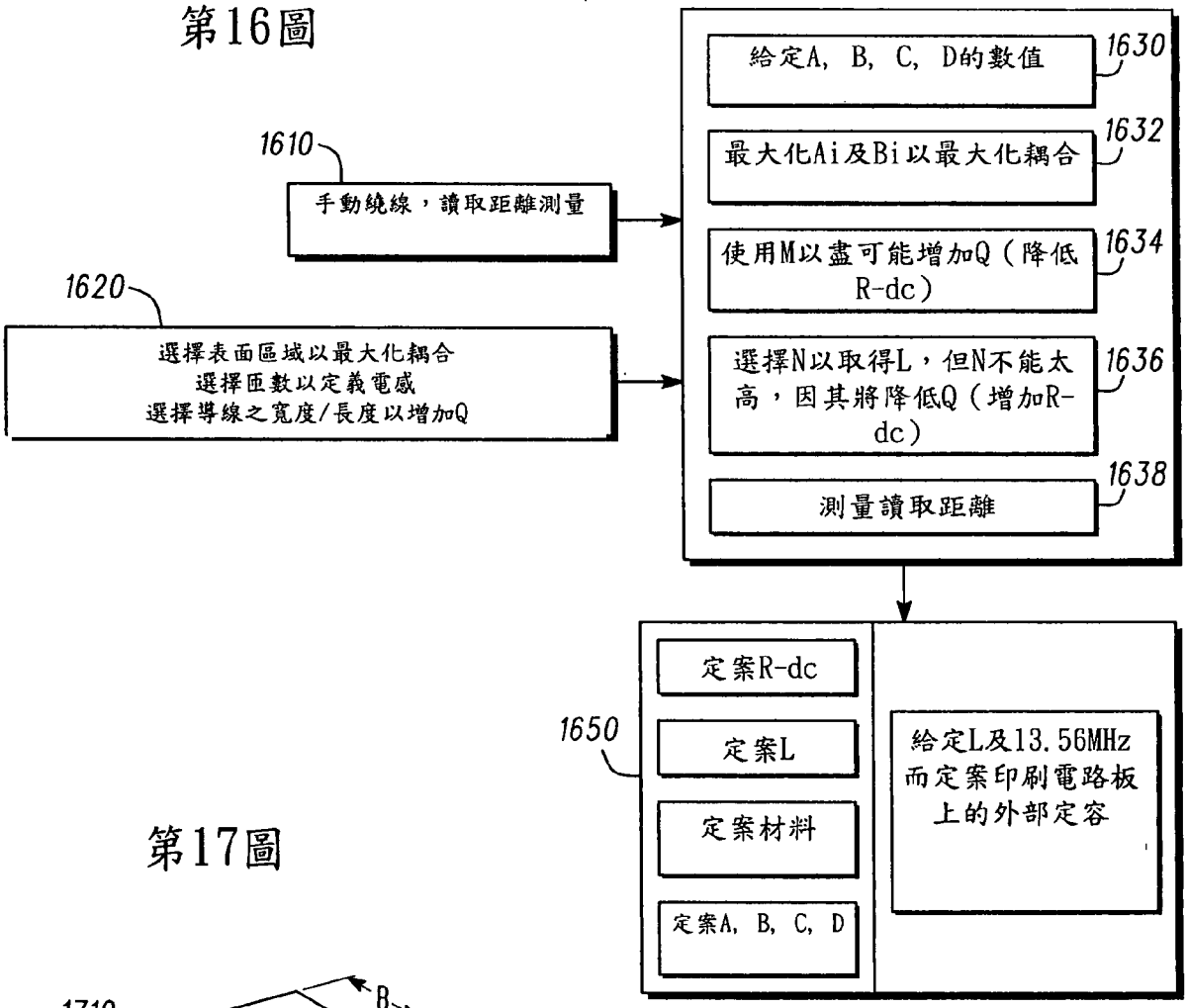


第15A圖

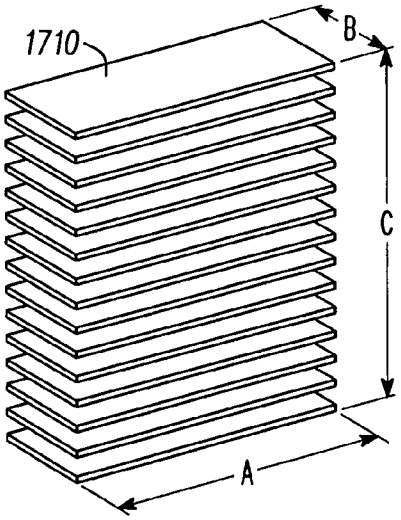


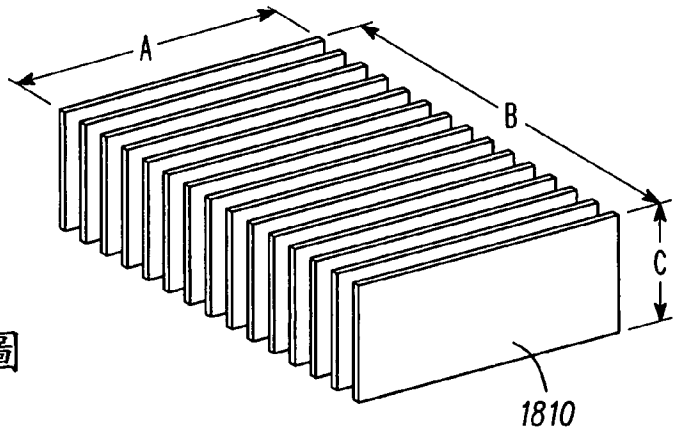
第15B圖

第16圖

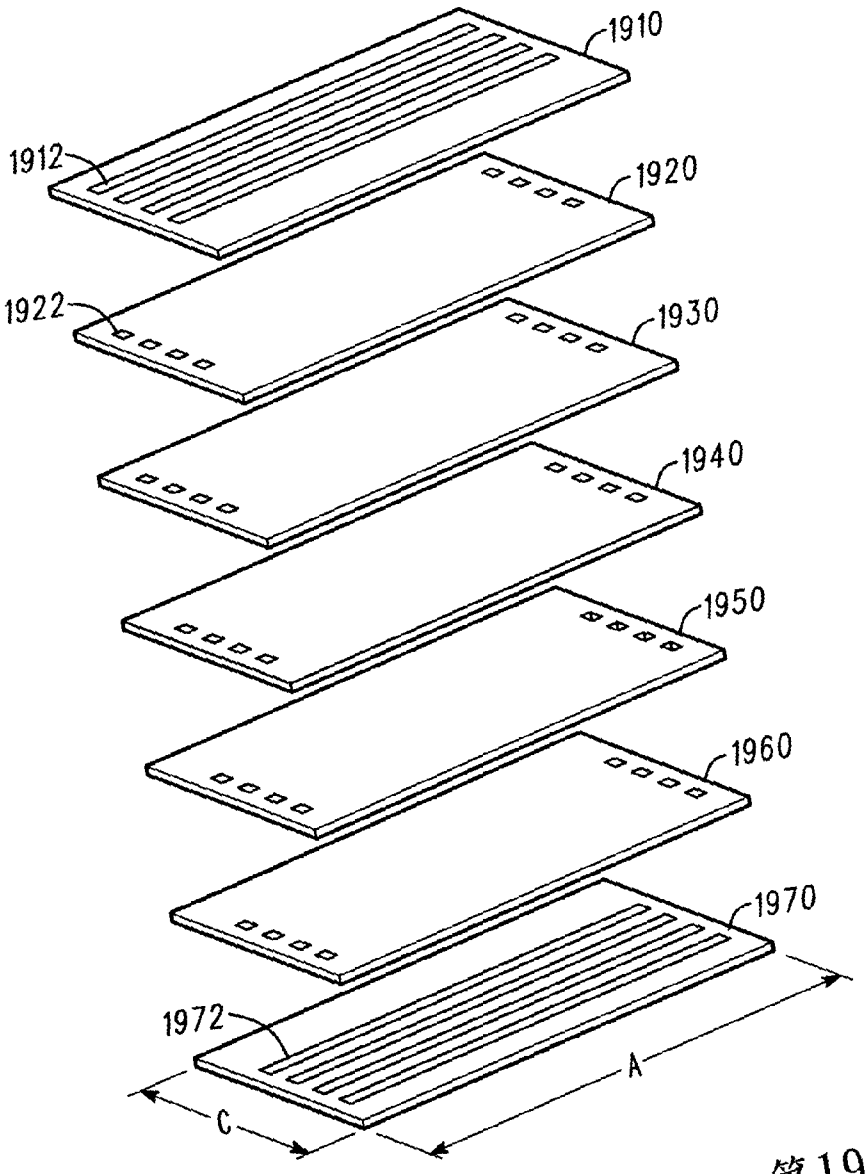


第17圖

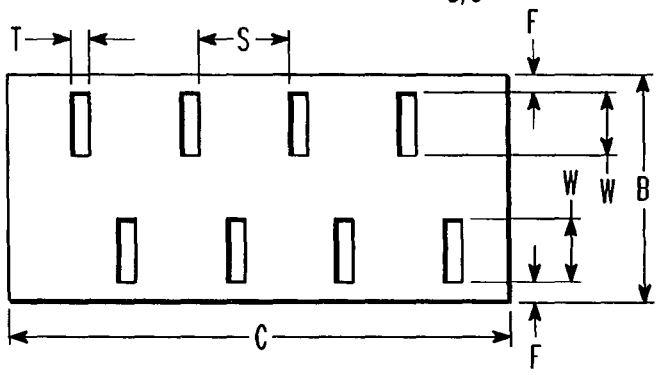




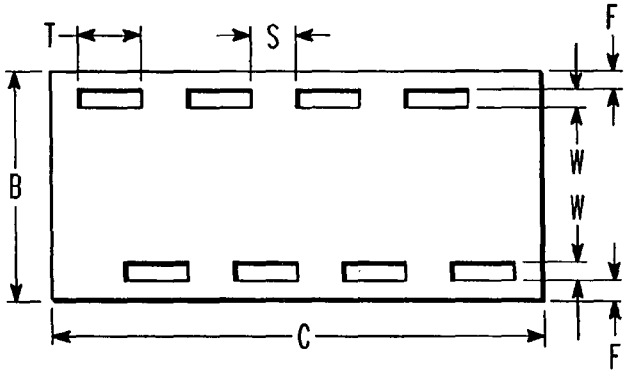
第18圖



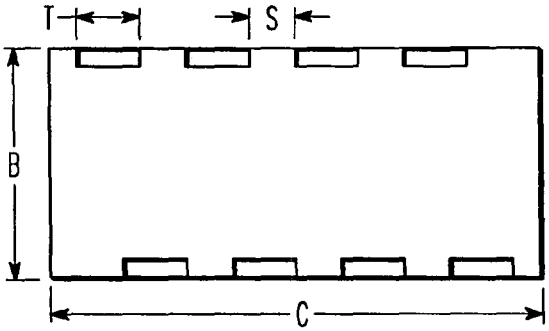
第19圖



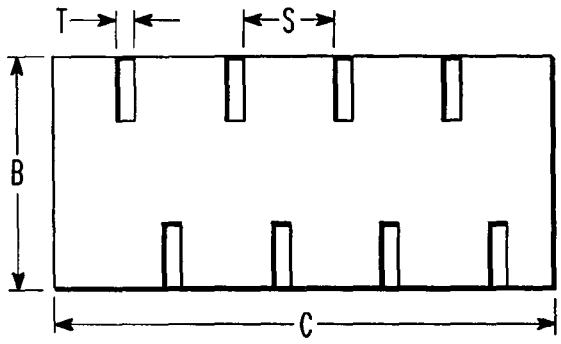
第20圖



第21圖



第22圖



第23圖

_ Biblio _ Print _

Patent/Publication Number 200636592

Title Electronic transaction card

Issued/Publication Date 2006/10/16

Application Date 2006/02/22

Application Number 095105997

IPC G06K-019/06;G06F-017/60

Inventor NARENDRA, SIVA G. IN;

SPITZER, THOMAS N. US;

TADEPALLI, PRABHAKAR IN

Applicant TYFONE, INC.US

Priority Number 20050222US20050063291

Abstract An electronic transaction card communicates with an add-on slot of an intelligent electronic device. The add-on slot may be a memory card slot. 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.

Individual F

_____ _ http://twpat5.tipo.gov.tw/tipotwoc/tipotwekm?00510F821E6101010000...

1 of 1 02/10/2011 12:59 PM

【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I336449

【45】公告日： 中華民國100 (2011) 年01 月21 日

【51】Int. Cl.： G06K19/06 (2006.01) G06Q20/00 (2006.01)

發明　　全 15 頁

【54】名　　稱：電子交易卡

ELECTRONIC TRANSACTION CARD

【21】申請案號：095105997 【22】申請日： 中華民國95 (2006) 年02 月22 日

【11】公開編號：200636592 【43】公開日期： 中華民國95 (2006) 年10 月16 日

【30】優先權： 2005/02/22 美國11/063,291

【72】發明人： 納廉達西瓦G (IN) NARENDRA, SIVA G.；史匹哲湯瑪斯N (US) SPITZER,

THOMAS N.；塔迪帕里波拉伯哈卡爾 (IN) TADEPALLI, PRABHAKAR

【71】申請人： 泰豐股份有限公司TYFONE, INC.

美國

【74】代理人： 蔡坤財

【56】參考文獻：

TW 200413928A

US 4786791

GB 2316908A

US 6669487B1

[57]申請專利範圍

1.
一種相容於一行動電話中之一記憶卡槽的記憶卡，該記憶卡包含：可由該行動電話所存取的非揮發性記憶體、一用於溝通一銷售點(POS)終端機的銷售點介面和保存金融交易資料的揮發性記憶體，其中該銷售點介面接收來自該行動電話的電力。

2.　如申請專利範圍第1
項所述之記憶卡，其中該銷售點介面包含系統電路，用以產生至少

一時變磁場。

3. 如申請專利範圍第2
項所述之記憶卡更包含一處理裝置，其耦接至該非揮發性記憶體、

揮發性記憶體和銷售點介面。

4. 如申請專利範圍第1 項所述之記憶卡，其中該銷售點介面包含一電子磁條(electronic

strip)，其可模仿一磁性磁條(magnetic strip)。

5. 如申請專利範圍第4
項所述之記憶卡，更包含一嵌入的刷讀感測器，用以感測該電子磁

條何時刷過銷售點終端機。

6. 如申請專利範圍第1 項所述之記憶卡，其中該銷售點介面包含一智慧卡介面。

7. 如申請專利範圍第1 項所述之記憶卡，更包含用於安裝在行動電話上的軟體。

8. 如申請專利範圍第7 項所述之記憶卡，其中該軟體包含一用於產生個別交易帳號的模

組。

9. 一種用於執行一金融交易的設備，其包含：
溝通元件，其用於經由在一智慧電子裝置中

之一記憶卡槽而進行溝通；產生元件，其用於產生至少一表示金融交易資料之時變磁

場，其中該產生元件接收來自該記憶卡槽的電力；和儲存元件，其用於儲存該金融交易

資料。

10. 如申請專利範圍第9 項所述之設備，更包含用於安裝在該智慧電子裝置的軟體。

11. 如申請專利範圍第10
項所述之設備，其中該軟體包含一用於產生個別交易帳號的模組。

12. 如申請專利範圍第11 項所述之設備，其中設定該軟體以在一行動電話中執行。

13. 如申請專利範圍第9
項所述之設備，更包含非揮發性記憶體，其可藉由上述經由一記憶

卡槽而進行溝通的溝通元件來存取。

14. 如申請專利範圍第9
項所述之設備，更包含感測元件，以感測該記憶卡是否已刷過一磁

卡讀卡機。

15.
一種電子交易卡，其包含：一記憶卡槽介面；和電路系統，其係由該記憶卡槽介面供電

且用於產生一時變磁場。

16. 如申請專利範圍第15
項所述之電子交易卡，其中設定該電路系統以產生相容於一銷售點

交易裝置的複數時變磁場。

17. 如申請專利範圍第16
項所述之電子交易卡，更包含可經由該記憶卡槽介面來存取的非揮

發性記憶體。

18. 如申請專利範圍第15
項所述之電子交易卡，更包含：一處理裝置，其耦接至該記憶卡槽

介面和用於產生一時變磁場的該電路系統。

19. 如申請專利範圍第18
項所述之電子交易卡，更包含一軟體元件，其當由該處理裝置所執

行時，導致該電路系統產生該時變磁場。

20. 如申請專利範圍第18
項所述之電子交易卡，更包含軟體，其係可被傳輸至該電子交易卡

以外的一裝置。

圖式簡單說明

第1 圖、第2A 圖和第2B 圖顯示智慧型電子裝置和電子交易卡；第3 圖顯示一電子交易

卡的一方塊圖；第4 圖顯示在一磁卡讀卡機之一電子交易卡；第5
圖顯示一智慧型電子裝置

和卡片在一讀卡機中；第6 圖至第8 圖顯示用於使用電子交易卡的轉接器；第9 圖和第10 圖

顯示一具有一智慧卡介面的電子交易卡；第11
圖顯示一結合一電子交易卡的轉接器；第12

圖顯示一具有一孔徑以接收一電子交易卡的轉接器；第13
圖顯示另一種轉接器實施例；第14

圖顯示一電子交易卡；第15 圖顯示一電子交易卡與轉接器的組合；第16
圖顯示一示例燕尾

式讀卡機；第17 圖顯示一電子交易卡與轉接器的組合刷過一磁卡讀卡機；第18
圖顯示一金

融交易卡；第19 圖顯示一記憶卡；第20
圖顯示一結合記憶卡和電子交易卡的方塊圖；第21

圖顯示一如何使用一卡片的圖示；第22
圖顯示一結合記憶卡和電子交易卡的方塊圖；和第23

圖顯示一電話和一卡片的方塊圖。

(2)

- 1778 -

(3)

- 1779 -

(4)

- 1780 -

(5)

- 1781 -

(6)

- 1782 -

(7)

- 1783 -

(8)

- 1784 -

(9)

- 1785 -

(10)

- 1786 -

(11)

- 1787 -

(12)

- 1788 -

(13)

- 1789 -

(14)

- 1790 -

(15)

- 1791 -

- 1792 -

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06K 19/077, G07F 7/10 — A1

(11) International Publication Number: **WO 00/14678**

(43) International Publication Date: 16 March 2000 (16.03.00)

(21) International Application Number: PCT/CA99/00785

(22) International Filing Date: 27 August 1999 (27.08.99)

(30) Priority Data:
09/148,132 4 September 1998 (04.09.98) US

(71) Applicant *(for all designated States except US)*: IC TV INTERACTIVE CYBER TELEVISION INC. [CA/CA]; Suite 410, 1255 University, Montreal, Quebec H3B 3B6 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: COMBALUZIER, Pierre, Michel [CA/CA]; Suite 604, 1400 Des Pins Avenue West, Montreal, Quebec H3G 1B1 (CA).

(74) Agents: DUBUC, Jean, H. et al.; Goudreau Gage Dubuc & Martienau Walker, The Stock Exchange Tower, Suite 3400, 800 Place Victoria, P.O. Box 242, Montreal, Quebec H4Z 1E9 (CA).

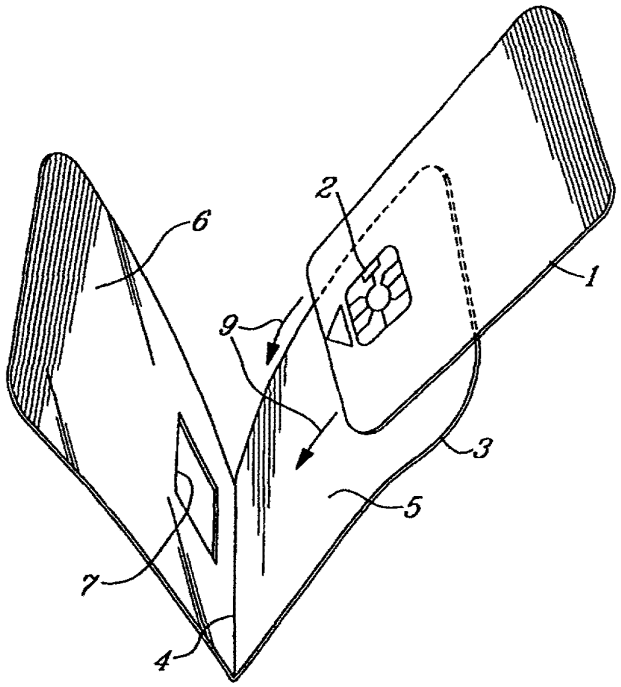
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, 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: IC CARD INTERACTIVE PLASTIC LEAFLET

(57) Abstract

The present invention relates to an envelope (3) for receiving an IC card (1) comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts (2) surface–mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope (3) is formed by a leaflet including two flexible flaps defining between them a flat space for receiving the IC card (1). A window (7) is made in one of the two flaps for accessing the set of surface–mounted contacts (2). A graphic scheme, for example a keyboard layout, is printed on at least one of the two sheet members for permitting use of the IC card (1) for an additional, predetermined function, for example recording the answers given by the user during a TV game. The present invention also relates to the resulting IC card/envelope combination. The invention is further concerned with a system for using the IC card for the additional predetermined function, comprising the leaflet and an IC card reading and/or writing device having a transparent tactile keyboard membrane and a microcontroller. The IC card/leaflet combination is inserted behind the transparent tactile keyboard membrane so that the keyboard membrane of the leaflet appears through the keyboard membrane. The microcontroller writes information in the microprocessor and memory circuit of the IC card in relation to operation of the transparent tactile keyboard membrane.



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		

IC CARD INTERACTIVE PLASTIC LEAFLET

BACKGROUND OF THE INVENTION

1. Field of the invention:

The present invention relates to an envelope for receiving an IC (Integrated Circuit) card in view of permitting use of this IC card for an additional, predetermined function. The present invention also relates to the IC card/envelope combination. The present invention further relates to a system, including the envelope, for using the IC card for the additional, predetermined function.

2. Brief description of the prior art:

Chip cards are currently used as credit cards, for bank transactions, in security systems, etc. A chip card is a plastic card similar in appearance to a credit card, but containing a microprocessor and memory chip programmed to perform several functions when used at a suitable terminal. As well known to those of ordinary skill in the art, a chip card comprises surface-mounted contacts for connection to the terminal.

Certain chip cards, usually called IC (Integrated Circuit) or smart cards and used for making bank transactions at a terminal, contain

not only ROM but RAM as well. Since these cards have microprocessor intelligence and a coded RAM memory, they can record card transactions and store data which are updated with each transaction.

OBJECT OF THE INVENTION

A general object of the present invention is to enable the use of IC cards for additional, predetermined functions.

SUMMARY OF THE INVENTION

More specifically, in accordance with the present invention, there is provided an envelope for receiving an IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope of the invention comprises (a) two sheet members defining between them a flat space for receiving the IC card, (b) a window in one of the two sheet members for accessing the set of surface-mounted contacts, and (c) a graphic scheme printed on at least one of the two sheet members for permitting use of the IC card for an additional, predetermined function.

The present invention also relates to an IC card/envelope combination comprising an IC card and an envelope for receiving the IC

card. The IC card comprises two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope includes:

two sheet members defining between them a flat space for receiving the IC card;

a window in one of the two sheet members for accessing the set of surface-mounted contacts; and

a graphic scheme printed on at least one of the two sheet members for permitting use of the IC card for an additional, predetermined function.

In accordance with a preferred embodiment, the envelope is a leaflet with two flexible flaps, the two sheet members are formed by the two flexible flaps of the leaflet, respectively, and the leaflet further comprises a reinforced edge portion for interconnecting the two flexible flaps and facilitating insertion of the leaflet through a slot of IC card reading and/or writing device. A slippery coating may cover at least in part the two flexible flaps and the reinforced edge portion to facilitate both insertion of the IC card in the leaflet and insertion of the leaflet through the slot of the IC card reading and/or writing device.

According to another preferred embodiment of the invention, the graphic scheme comprises a keyboard layout.

Preferably, indications will be printed on the leaflet to guide both insertion of the IC card in the flat space between the two flexible

flaps and insertion of the leaflet in the slot of an IC card reading and/or writing device.

Further in accordance with the present invention, there is provided a system for using an IC card for an additional predetermined function comprising an envelope for receiving the IC card and an IC card reading and/or writing device. The IC card comprises two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope includes:

two sheet members defining between them a flat space for receiving the IC card and form an IC card/envelope combination;

a window made in a first one of the two sheet members for accessing the set of surface-mounted contacts; and

a keyboard layout printed on the second one of the two flexible sheet members.

The IC card reading and/or writing device includes:

a housing defining a planar wall surface;

a transparent tactile keyboard membrane mounted in front of but spaced apart from the planar wall surface to define a flat cavity between the transparent tactile keyboard membrane and the planar wall surface to receive the IC card/envelope combination;

a connector mounted on the planar wall surface and having a plurality of contacts for connection to the surface-mounted contacts, respectively; and

a microcontroller for writing information in the microprocessor and memory circuit of the IC card through the connector contacts and the surface-mounted contacts in relation to operation of the transparent tactile keyboard membrane.

In operation, when the IC card/envelope combination is inserted in the flat cavity with the connector contacts connected to the surface-mounted contacts and with the keyboard layout visible through the transparent tactile keyboard membrane, the transparent tactile keyboard membrane can be operated in relation to the keyboard layout and the microcontroller can write information in the microprocessor and memory circuit of the IC card in relation to operation of the transparent keyboard membrane.

In accordance with a preferred embodiment, the IC card reading and/or writing device forms part of a TV remote control, the keyboard layout is a TV game keyboard layout for answering questions asked during a TV program, and the microcontroller comprises means for recording the answers to the questions given by a user through operation of the transparent tactile keyboard membrane.

The objects, advantages and other features of the present invention will become more apparent upon reading of the following non restrictive description of a preferred embodiment thereof, given by way of example only with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

In the appended drawings:

Figure 1 is a perspective view of a leaflet in accordance with the invention for receiving an IC card and thereby form an IC card/leaflet combination, showing a window in one of the flexible flaps for accessing the surface-mounted contacts of the IC card;

Figure 2 is a side elevational view of the leaflet of Figure 1;

Figure 3 is a front elevational view of the IC card and leaflet;

Figure 4 is a rear elevational view of a TV remote control including an IC card reading and/or writing device for receiving the IC card/leaflet combination;

Figure 5 is a side elevational view of a leaflet according to the invention including two flexible flaps and a reinforced edge portion for interconnecting these two flexible flaps;

Figure 6a is an example of keyboard layout that can be printed on the outer face of the rear flap of the leaflet according to the invention;

Figure 6b is an example of illustration that can be printed on the outer face of the front flap of the leaflet according to the invention; and

Figure 7 is a block diagram of the electronic circuit of the TV remote control of Figure 4.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to Figure 1 of the appended drawings, the IC card 1 comprises surface-mounted contacts 2 for connection to a bank terminal or any other terminal (not shown). Just a word to mention that the format of most of the IC cards presently available on the market conforms with an ISO standard.

Preferably, the leaflet 3 is made of transparent plastic sheet material. The leaflet 3 comprises a rear flap 5 and a front flap 6 having a configuration and dimensions corresponding to those of the IC card 1. The leaflet 3 comprises a reinforced edge portion 4 for interconnecting the flexible flaps 5 and 6 and facilitate insertion of the leaflet 3 through a slot of IC card reading and/or writing device. Front flap 6 comprises a rectangular window 7 to access the surface-mounted contacts 2 when the leaflet 3 envelops the IC card 1. On the outer face of the rear flap 5 is printed a graphic keyboard layout as shown for example by arrow 8 in Figure 4. This graphical keyboard layout 8 may be composed of various icons, letters, numbers, or other characters or illustrations such as 22.

To further facilitate penetration of the slot of an IC card reading and/or writing device, outer faces 29 and 30 of the reinforced edge portion 4 as well as portion of the flaps 5 and 6 can be covered with a

slippery coating (not shown). In the same manner, portions of the flaps 5 and 6 can be covered with a slippery coating to facilitate insertion of the IC card 1 in the flat space defined between the flaps 5 and 6.

Arrow-like indications such as 31 can also be printed onto the outer faces 29 and 30 to indicate to a user a direction of insertion of the IC card/leaflet combination in the slot of the reading and/or writing device. In addition, guide marks can be printed on the leaflet 3 to guide insertion of the IC card 1 between the two flaps 5 and 6 of the leaflet 3. Finally, visual indications of the new function(s) added to the IC card 1 through the leaflet 3 can be printed onto the leaflet 3, in particular on the outer face of the front flap 6.

Referring now to Figures 1-3, the IC card 1 is inserted between the two flaps 5 and 6 (see arrows 9 in Figure 1, arrow 10 in Figure 2, arrows 12 in Figure 3, and arrow 28 in Figure 5) in such a way as to expose the contacts 2 through the window 7, as best shown in Figure 3.

The IC card 1 can be used in combination with a universal remote control 13 shown in Figure 4. The remote control 13 incorporates all the function protocols of the TV, VCR, Audio commands of most of the brands available on the market (95%). Figure 8 shows a schematic block diagram of the electronic circuit of the remote control 13.

The remote control 13 comprises a plastic housing 14. On the back of the housing 14 is defined a planar wall surface 17. A transparent tactile keyboard membrane 18 is mounted in front but spaced apart from

the planar wall surface to define a flat cavity between the transparent tactile keyboard membrane and the planar wall surface 17 to receive the IC card 1/leaflet 3 combination. In the illustrated non limitative example, the transparent tactile keyboard membrane 18 comprises 15 resistive tactile zones such as 21. The plastic housing 14 of the remote control 13 has a top face 15 formed with a slot 16 for longitudinal insertion of the IC card 1/leaflet 3 combination in the flat cavity behind the transparent tactile keyboard membrane.

On a planar wall surface 17 of the housing 14 situated behind keyboard 18 is mounted a universal IC card connector 19 including a standard group of contacts such as 20 for connection to respective surface-mounted contacts 2 in order to automatically establish a bidirectional communication link between the microprocessor and memory circuit of the IC card 1 and the microcontroller 30 of the remote control 13 (Figure 7) each time the IC card 1 covered by the leaflet 3 is longitudinally inserted through the slot 16.

Of course, the leaflet 3 is so designed that the reinforced edge portion 4 (Figure 5) is introduced first to thereby greatly facilitate insertion of the IC card 1/leaflet 3 combination through the slot 16. After the IC card 1/leaflet 3 combination has been inserted through the slot 16, each icon, letter, number or other illustration 22 appears in a corresponding, for example resistive tactile zone 21.

Referring to Figure 7, the electronic circuit of the remote control 13 comprises the above mentioned microcontroller 30 and a universal remote control circuit 36 incorporating, as stated above, all the function

protocols of the TV, VCR, Audio commands of most of the brands available on the market (95%).

The microcontroller 30 is connected to (a) the transparent tactile keyboard membrane 18 to detect depression of any zone 21 of that membrane, (b) a 4-digit liquid crystal display 25, (c) a piezoelectric transducer 31 to activate this piezoelectric transducer and produce a "bip" when required or desired, (d) a programmable real-time clock 32, (e) an identification number memory 33 for giving to the microcontroller 30 an identification of the user, and (f) the reading head 34 through a card interface 35. The microcontroller 30 is conventionally powered by an electric power supply 37, for example a 9-volt battery, through a 5-volt voltage regulator of circuit 38. The universal remote control circuit 36 is powered by the electric power supply 37 through a 3-volt voltage regulator of circuit 38.

The reading head 34 includes the connector 19 of Figure 4 and is advantageously of the GEMCORE™ technology. This technology has been developed by the company GemPlus to read and write on IC cards.

Regarding the card interface 35, it uses the language MEL (MULTOS Executable Language) developed by the MULTOS which is a merger of financial institutions which establishes standard characteristics to ensure a compatibility of the communications between the members. MULTOS is an industrial standard for many applications of the IC cards, including the electronic purse application.

The remote control 13 may further perform, amongst others, the following functions:

- a pawl 23 to trigger a mechanism (not shown) for ejecting the IC card 1/leaflet 3 combination from the flat cavity through the slot 16 after use (such a mechanism is well known to those of ordinary skill in the art and will not be further described in the present specification);

- a switch 24 to switch the tactile keyboard 18 on;

- the microcontroller 30 will display on the 4-digit liquid crystal display 25:
  - the time obtained from the programmable real-time clock 32;
  - the TV channel in interaction obtained from the universal remote control circuit 36;
  - number of score units recorded and determined from the answers given by the user;
  - minimum and maximum scores reached during a TV game as recorded by the microcontroller 30;
  - the charge of the battery obtained through the voltage regulator circuit 38;
  - etc.

- a push-button 26 connected to the microcontroller 30 for adjusting the time given by the clock 32 and displayed by the microcontroller 30 on the display 25, and for adjusting the intensity of the "bip" produced by the piezoelectric transducer 31 to confirm interactive actions on the transparent tactile keyboard membrane 18 (upon adjustment of the intensity of the "bip" through the push-button 26, a bar code

representative of this intensity is displayed by the microcontroller 30 on the 4-digit liquid crystal display 25);

- a push-button 27 for resetting the score after saving of the game.

Although application of the leaflet 3 to form an IC card 1/leaflet 3 combination to be inserted in a remote control 13 has been described in the foregoing description, the leaflet 3 according to the invention can also be used in connection with an IC card and thereby form an IC card 1/leaflet 3 subsequently inserted into any other type of bank, transaction, communication and/or exchange terminal.

The leaflet 3 according to the invention is also designed for and capable of customizing, adapting, humanizing and/or promoting a functional card of the security type, or creating actions, synergies or interoperabilities for such cards. To easily penetrate the public at large with functional cards of the security type, the leaflet 3 may be used to dress, to complete with added functions or values and/or to make user-friendly and less formal such security cards, while satisfying the standards, prints, ISO 1 back magnetic stripe and/or functional prints of the security organization, monetary or monetics transaction organization, and/or initial issuing organization.

The leaflet 3 according to the invention can further be used:

- to promote or lead towards customer loyalty to any privative bank card, commercial card, credit card, debit card, etc.;

- to instantaneously optimize the visual access of applications of the card being used;

- to guide transactions on a portable card reader; and

- as an envelope for interactive direct television advertising.

Example

The following example is concerned with a leaflet 3 having a back flap 5 on which is printed the layout of a keyboard for playing a game related to a given TV program, for example the popular program ENTERTAINMENT TONIGHT™. Figure 6a illustrates an example of keyboard layout which can be printed on the outer face of the rear flap 5, and Figure 6b illustrates the outer face of the front flap 6 on which can be printed, for example, identification of the issuing organization, advertising of the TV program, identification of the produces, etc.

Just a word to mention that the leaflet 3 according to the present invention can be produced at low cost (some cents by unit) and can be distributed to the public at large:

- on wine bottles;
- on soft drink packs;
- inside weekly TV guides;
- by direct mail;
- in fragrance boxes;
- in magazines;
- on cigarette boxes;

- in photo film boxes;
- in airflight tickets;
- in show tickets envelopes;
- in gift menus;
- in check flyers;
- etc.

Since the leaflet 3 according to the invention is susceptible to increase their sales and profits, the companies involved are likely to incorporate the leaflet to their products at no extra charge.

To use the leaflet 3 according to the present invention, the first step consists of inserting the IC card 1 into the leaflet 3 and inserting the IC card 1/leaflet 3 combination through the slot 16. The keyboard layout of Figure 6a then appears through the transparent tactile keyboard 18. As can be appreciated, each icon of the keyboard layout of Figure 6a appears through a respective resistive area 21 of the transparent tactile keyboard 18.

The microcontroller can further be programmed to respond to insertion of the IC card 1/leaflet 3 combination by:

- pre-programming the clock 32 to synchronize it with the TV program in order to enable correct time dating of the answers selected by the card user on the transparent tactile keyboard membrane 18. This is made by means of a time correction increment or decrement recorded in the microprocessor and memory circuit of the IC card 1 by a bank terminal or any other type of terminal as will be explained hereinafter;

- control the universal remote control circuit 36 to automatically turn the TV set on.

Then the user use the remote control 13 to tune the TV set to the channel on which the TV program associated to the leaflet 3 is broadcasted. Then, the user can answer the questions broadcasted during the TV program. A list of possible questions is presented in attached Appendix 1. As can be seen, an icon 22 of the keyboard layout 8 is associated to each question.

If the user chooses answer 1 as a response to a question, he (she) presses once on the zone 21 of the transparent tactile keyboard 18 behind which the icon 22 corresponding to the question appears. If answer 2 is selected, the user presses twice on the zone 21 of the transparent tactile keyboard 18 behind which the corresponding icon 22 appears. If the user chooses answer 3 as a response to the question, he (she) presses three times on the zone 21 of the transparent tactile keyboard 18 corresponding to the icon 22 associated to the question.

The user will answer to a series of questions during one, two, or up to five TV programs of a TV channel using one or more leaflets such as leaflet 3.

The microcontroller 30 of the remote control 13 is responsive to depression of the tactile zones 21 of the transparent keyboard membrane 18 to record the answers of the user in the microprocessor and memory circuit of the IC card 1 and the time at which these answers are given through the card interface 35, the reading head 34 including the

contacts 20 of the connector 19, and the surface-mounted contacts 2 of the IC card 1. The user's identification number stored in memory 33 will also be recorded in the microprocessor and memory circuit of the IC card 1 for identifying the user.

In this way, the user accumulates rights in relation to his (her) answers. He (She) also defines, in time, his (her) consumer profile. The user can then use his (her) IC card 1 to obtain these rights, through an appropriate terminal, in particular but not exclusively a sponsor banking terminal rent for that purpose, or simply a dedicated terminal.

As soon as the IC card 1 is inserted in the terminal, the server of the TV channel or the sponsor network is contacted. The software of the server reads the contents of the IC card 1, analyses the recorded times and answers, compare the results with the answer key of the questionnaire and/or TV game, and decides the value of the rights to be attributed in relation to the accuracy of the answers recorded in the memory of the IC card 1. Finally, the server of the TV channel and/or sponsor will attribute a remuneration corresponding to the value of rights acquired, consisting of points, coupons, units, miles, etc in the IC card 1. The user can then choose to use this gain to obtain free units or, for example, to credit his (her) VISA account with a corresponding amount of money. To credit his (her) account, the user has simply to type the number of his (her) VISA card on the keyboard of the terminal being used.

Finally, the recorded data are erased by the terminal to prepare the card for a new TV program. Before erasing the recorded data, the

terminal analyses the time dating of the answer recorded and will store in the microprocessor and memory circuit of the IC card 1 the above mentioned time correction increment or decrement that should be applied to the real-time clock 32 to synchronize this clock 32 with the TV program in order to enable correct time dating of the answers given by the card user on the transparent tactile keyboard membrane 18.

At the beginning of each game played or operation made through the remote control 13, the microcontroller 30 stores the user's identification number from memory 33 in the microprocessor and memory circuit of the IC card 1, next to the time dating of the answers. This will enable survey of the population for rating (percent of TV households that are tuned, on the average, to one time period in a particular program).

Finally, it should be mentioned that the above mentioned gain can be paid by any interested party, for example public survey organizations.

Although the present invention has been described hereinabove by way of a preferred embodiment thereof, this embodiment can be modified at will, within the scope of the appended claims, without departing from the spirit and nature of the subject invention.

WHAT IS CLAIMED IS:

1. An envelope for receiving an IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit, comprising:

two sheet members defining between them a flat space for receiving the IC card;

a window in one of said two sheet members for accessing the set of surface-mounted contacts; and

a graphic scheme printed on at least one of said two sheet members for permitting use of the IC card for an additional, predetermined function.

2. The envelope of claim 1, wherein:

- the envelope is a leaflet with two flexible flaps; and

- the two sheet members are formed by the two flexible flaps of the leaflet, respectively.

3. The envelope of claim 2, wherein the leaflet further comprises a reinforced edge portion for interconnecting the two flexible flaps and facilitating insertion of the leaflet through a slot of IC card reading and/or writing device.

4. The envelope of claim 3, further comprising a slippery coating covering at least in part the two flexible flaps and the reinforced edge portion to facilitate both insertion of the IC card in the leaflet and

insertion of the leaflet through the slot of the IC card reading and/or writing device.

5. The envelope of claim 1, wherein the graphic scheme comprises a keyboard layout.

6. The envelope of claim 2, further comprising indications printed on the leaflet to guide both insertion of the IC card in the flat space between the two flexible flaps and insertion of the leaflet in a slot of IC card reading and/or writing device.

7. An IC card/envelope combination comprising:

an IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit; and

an envelope for receiving the IC card, including:

two sheet members defining between them a flat space for receiving the IC card;

a window in one of said two sheet members for accessing the set of surface-mounted contacts; and

a graphic scheme printed on at least one of said two sheet members for permitting use of the IC card for an additional, predetermined function.

8. The IC card/envelope combination of claim 7, wherein:

- the envelope is a leaflet with two flexible flaps; and

- the two sheet members are formed by the two flexible flaps of the leaflet, respectively.

9. The IC card/envelope combination of claim 8, wherein the leaflet further comprises a reinforced edge portion for interconnecting the two flexible flaps and facilitating insertion of the IC card/envelope combination through a slot of IC card reading and/or writing device.

10. The IC card/envelope combination of claim 9, further comprising a slippery coating covering at least in part the two flexible flaps and the reinforced edge portion to facilitate both insertion of the IC card in the leaflet and insertion of the IC card/envelope combination through the slot of the IC card reading and/or writing device.

11. The IC card/envelope combination of claim 7, wherein the graphic scheme comprises a keyboard layout.

12. The IC card/envelope combination of claim 8, further comprising indications printed on the leaflet to guide both insertion of the IC card in the flat space between the two flexible flaps and insertion of the IC card/envelope combination in a slot of IC card reading and/or writing device.

13. A system for using an IC card for an additional predetermined function, the IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the

microprocessor and memory circuit, said system comprising:

an envelope for receiving the IC card, including:

two sheet members defining between them a flat space for receiving the IC card and form an IC card/envelope combination;

a window made in a first one of said two sheet members for accessing the set of surface-mounted contacts; and

a keyboard layout printed on the second one of said two flexible sheet members; and

an IC card reading and/or writing device including:

a housing defining a planar wall surface;

a transparent tactile keyboard membrane mounted in front of but spaced apart from the planar wall surface to define a flat cavity between the transparent tactile keyboard membrane and the planar wall surface to receive the IC card/envelope combination;

a connector mounted on the planar wall surface and having a plurality of contacts for connection to the surface-mounted contacts of said set, respectively; and

a microcontroller for writing information in the microprocessor and memory circuit of the IC card through said the contacts of said connector and the surface-mounted contacts of said set in relation to operation of the transparent tactile keyboard membrane;

whereby, in operation, when the IC card/envelope combination is inserted in the flat cavity with the contacts of the connector connected to the surface-mounted contacts of said set and with the keyboard layout visible through the transparent tactile keyboard membrane, the transparent tactile keyboard membrane can be operated in relation to the keyboard layout and the microcontroller can write information in the microprocessor and memory circuit of the IC card in relation to operation of the transparent keyboard membrane.

14. The system of claim 13, wherein:

- the envelope is a leaflet with two flexible flaps; and

- the two flexible sheet members are formed by the two flexible flaps of the leaflet, respectively.

15. The system of claim 13, wherein:

- the IC card reading and/or writing device forms part of a TV remote control;

the keyboard layout is a TV game keyboard layout for answering questions asked during a TV program; and

the microcontroller comprises means for recording the answers to said questions given by a user through operation of the transparent tactile keyboard membrane.

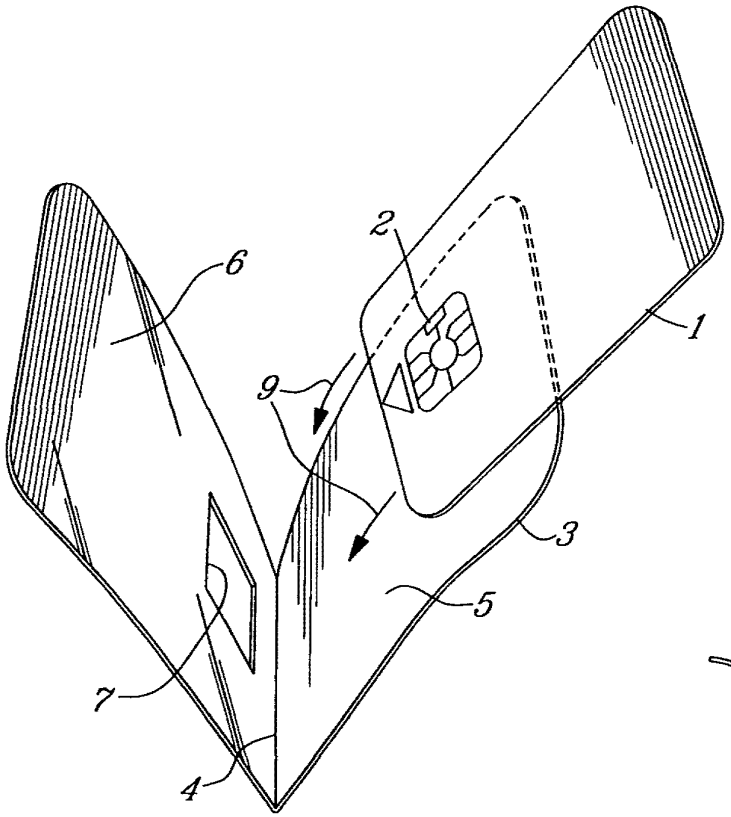


Fig. 1

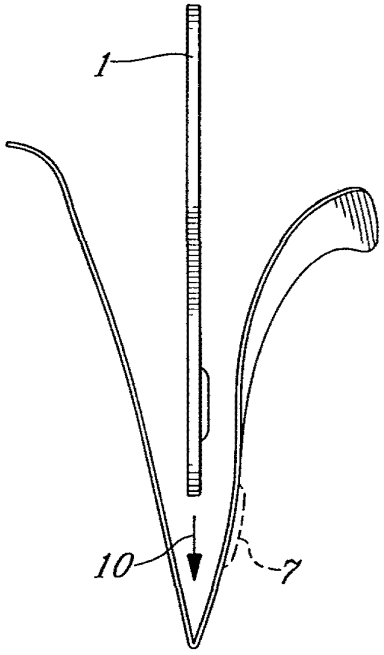


Fig. 2

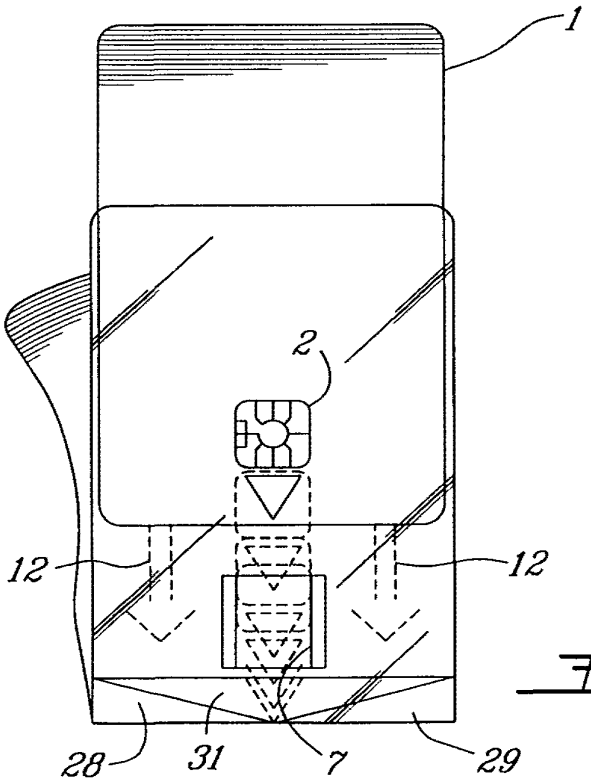


Fig. 3

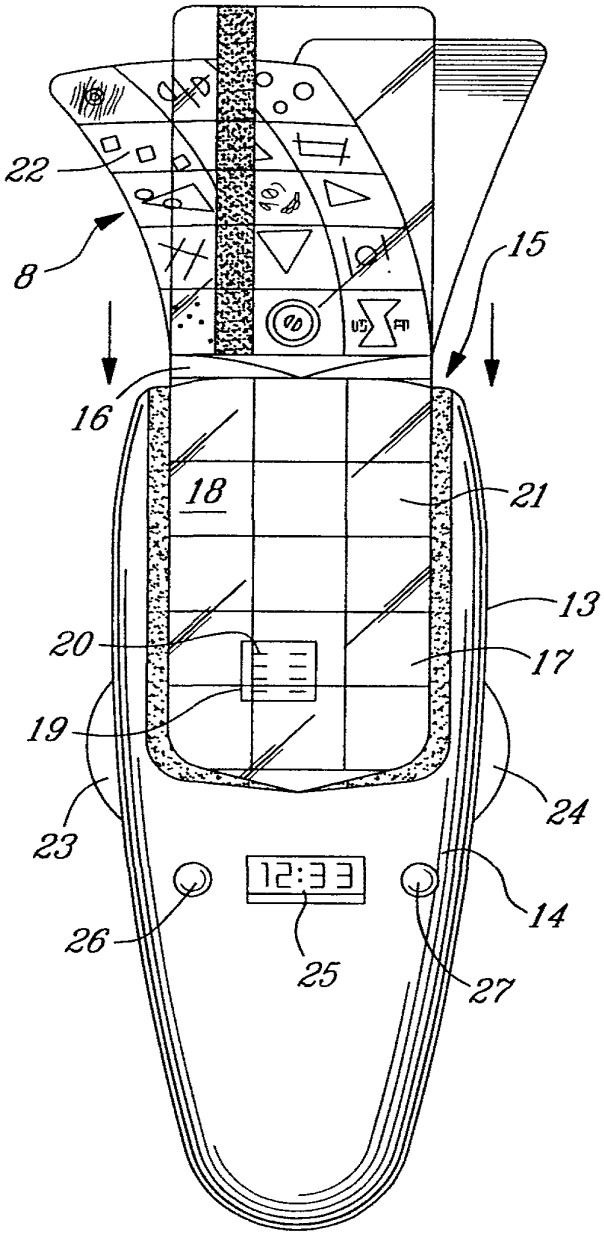


Fig. 4

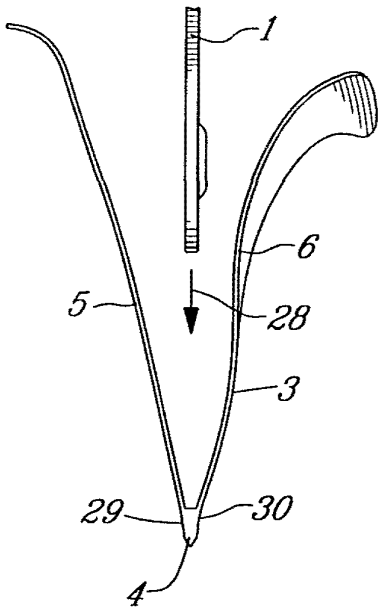


Fig. 5

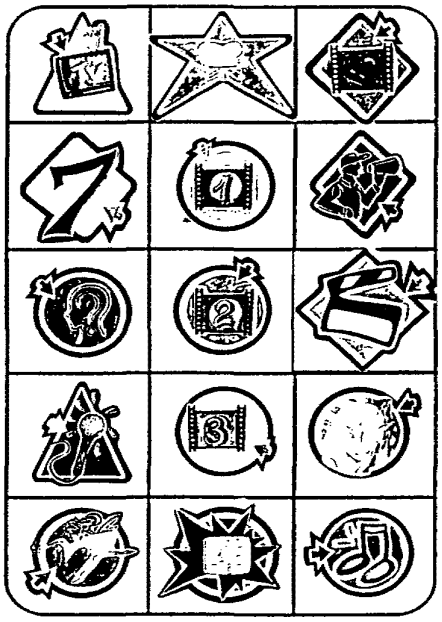


Fig. 6a

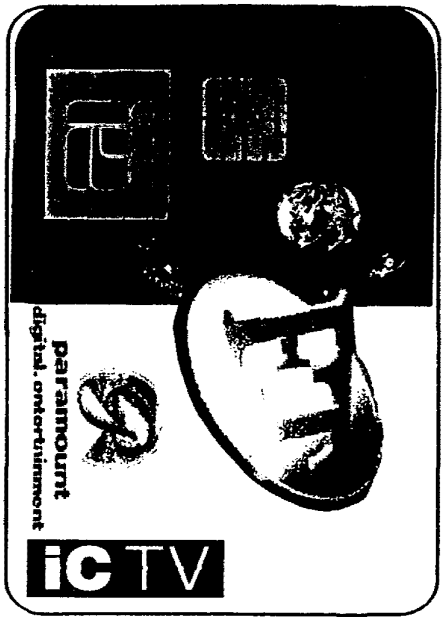


Fig. 6b

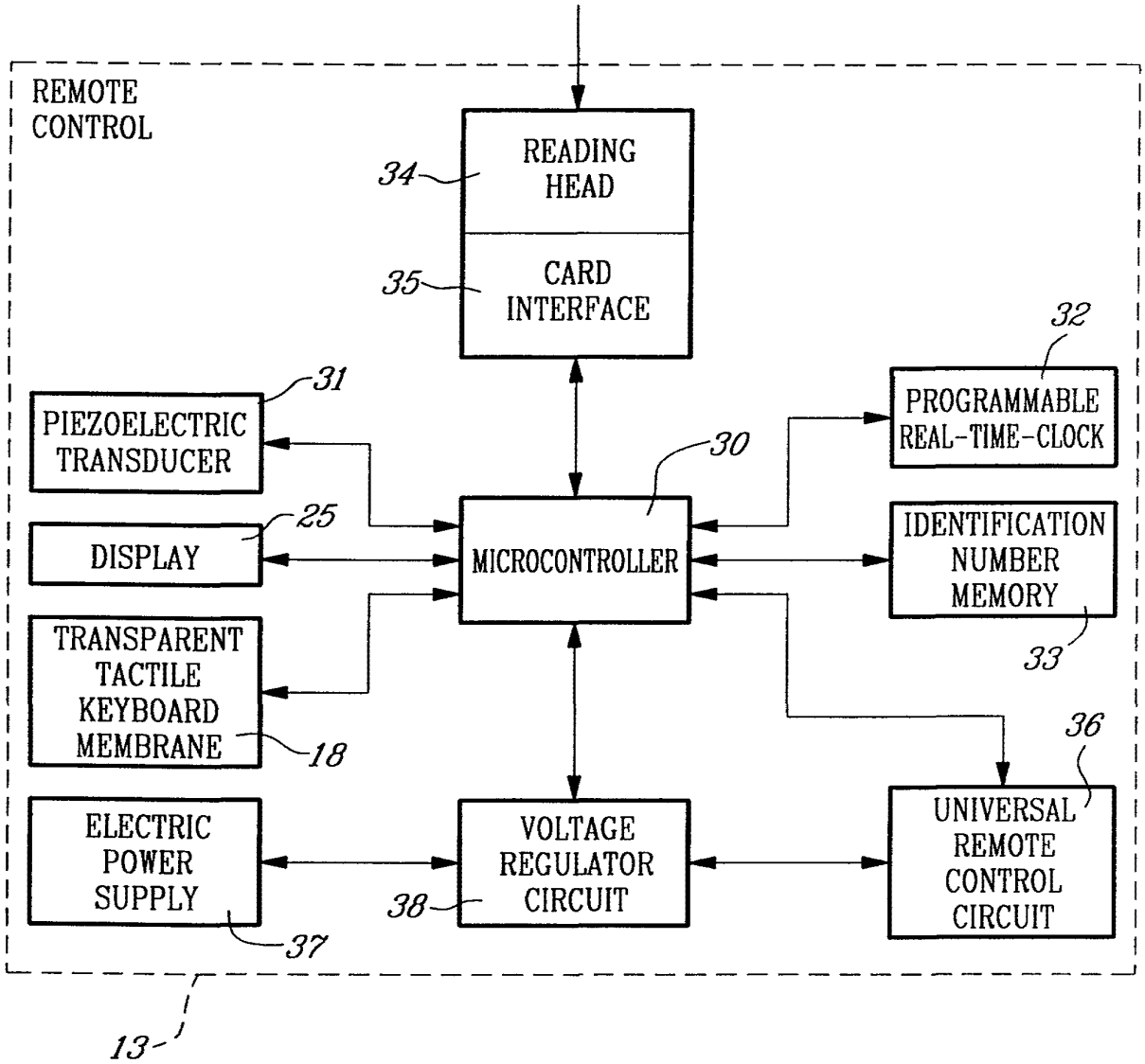

REMOTE CONTROL
READING HEAD
34
CARD INTERFACE
35
32
PROGRAMMABLE REAL-TIME-CLOCK
31
PIEZOELECTRIC TRANSDUCER
30
25
DISPLAY
MICROCONTROLLER
IDENTIFICATION NUMBER MEMORY
33
TRANSPARENT TACTILE KEYBOARD MEMBRANE
18
36
ELECTRIC POWER SUPPLY
VOLTAGE REGULATOR CIRCUIT
38
UNIVERSAL REMOTE CONTROL CIRCUIT
37
13

Fig. 7

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/CA 99/00785

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/077 G07F7/10

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 G07F A63F A45C H04N B65D

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 44 19 073 A (NOKIA MOBILE PHONES LTD) 1 December 1994 (1994-12-01) column 1, line 52 - line 59 claim 1 figure 1	1,7
A	FR 2 674 649 A (DOM INTELL INGENIERIES ;COMBALUZIER PIERRE MICHEL (FR)) 2 October 1992 (1992-10-02) page 5, line 14 - line 33 page 9, line 10 - line 24 figures 1-6	13
A	DE 94 07 198 U (OCIEPKA ROMAN) 22 September 1994 (1994-09-22) page 1, paragraph 8 figures 1,2	1,7

-/--

[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
21 December 1999	13/01/2000

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	de Ronde, J.

1

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2025-00645 Page 00379

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/CA 99/00785

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No
A	DE 295 03 892 U (KEMMLER MANFRED) 18 May 1995 (1995-05-18) page 2 figure 1	1,7

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

IPR2025-00645 Page 00380

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/CA 99/00785

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4419073 A	01-12-1994	FI 932473 A	01-12-1994
FR 2674649 A	02-10-1992	NONE	
DE 9407198 U	22-09-1994	NONE	
DE 29503892 U	18-05-1995	DE 29517165 U	14-03-1996

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 November 2001 (22.11.2001)

PCT

(10) International Publication Number
WO 01/088659 A3

(51) International Patent Classification[7]: G06F 17/00, 17/60, G06K 5/00, 7/01

(21) International Application Number: PCT/US01/15612

(22) International Filing Date: 15 May 2001 (15.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/571,707	15 May 2000 (15.05.2000)	US
09/619,859	20 July 2000 (20.07.2000)	US
09/667,835	21 September 2000 (21.09.2000)	US
09/667,081	21 September 2000 (21.09.2000)	US
09/667,039	21 September 2000 (21.09.2000)	US
09/667,082	21 September 2000 (21.09.2000)	US
09/667,038	21 September 2000 (21.09.2000)	US

(71) Applicant: **PRIVASYS** [US/US]; Suite 300, 40 First Street, San Francisco, CA 94105 (US).

(72) Inventors: **WONG, Jacob, Y.**; 7110 Georgetown Road, Goleta, CA 93117 (US). **ANDERSON, Roy, L.**; 1433 Dwight Drive, Glendale, CA 91207 (US). **BRYANT, William, R., Jr.**; 12001 Coverstone Hill Circle #324, Manasses, VA 20109 (US). **ZIEGLER, Joan, M.**; 2355 Paradise Drive, Tiburon, CA 94920 (US).

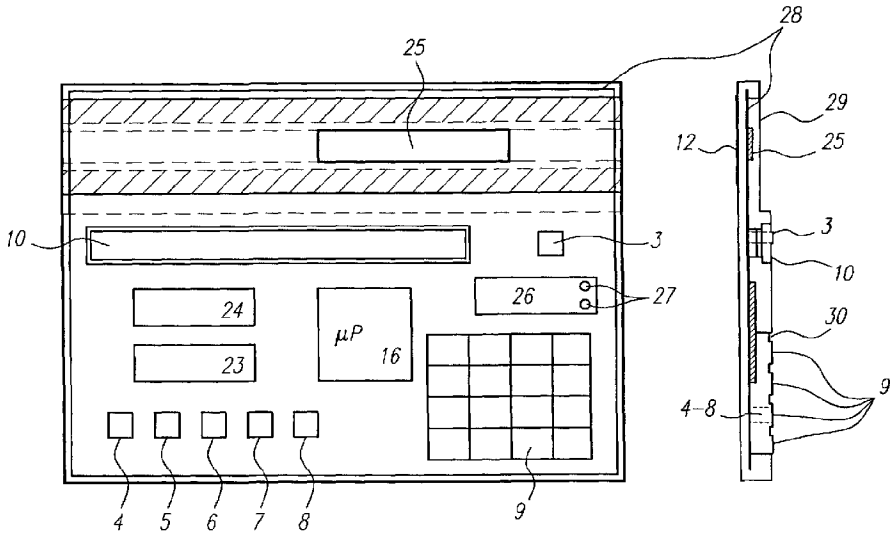
(74) Agent: **MCCONAGHY, John, D.**; Lyon & Lyon LLP, 633 West Fifth Street, 47th Floor, Los Angeles, CA 90071-2066 (US).

(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, 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

[Continued on next page]

(54) Title: ELECTRONIC CARDS CAPABLE OF BEING READ BY A MAGNETIC STRIPE READER AND METHODS FOR THEIR USE



(57) Abstract: An electronic card that can function as an anonymous credit card or banking card for use on or off the Internet utilizes a magnetic storage medium 12 affixed to the card that can be read by a standard magnetic stripe reader. An encoder 25 generates a data packet that can be stored in a designated portion of the magnetic storage medium, which can be a magnetic stripe. The data packet can contain a personal coupon and an alias. A computer or microprocessor 16 generates the personal coupon after a Personal Identification Number is input into the card. The data packet can also be used to convey other information, such as a low battery condition. Several different methods of customizing use of the electronic card provide a vast array of options for handling multiple users, bills, accounts, and for characterizing individual transactions of the card.

WO 01/088659 A3

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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
18 April 2002

(48) Date of publication of this corrected version:
3 January 2003

(15) Information about Correction:
see PCT Gazette No. 01/2003 of 3 January 2003, Section II

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.

ELECTRONIC CARDS CAPABLE OF BEING READ BY A MAGNETIC STRIPE READER AND METHODS FOR THEIR USE

Field of the Invention

The present invention is in the field of cards, such as payment cards, which contain information in a magnetic stripe, and methods for using such cards, including methods for making payments through payment cards.

Background of the Invention

Three forms of money in widespread use today throughout the world are cash, checks and payment cards (debit or credit). Each has distinct advantages, and distinct disadvantages. Cash is readily accepted, easy to use and anonymous, but it does not earn interest, it can be lost or stolen, and it is not always readily accessible. Checks are not always accepted, but they offer many advantages, since they do not have to be written until the time of payment. However, they must be physically presented and they are not anonymous. Payment cards are readily, but not always, accepted, and they offer many advantages over checks. If the card is a credit card, payment can be deferred, but the transaction is not anonymous. If the card is a debit card, payment has usually been made before its use, but it is anonymous. Accordingly, it is apparent that different types of money have different advantages to different persons in different situations. This may be one reason why all these forms of money are still in widespread use, and are even used by the same persons at different times.

As society and international commerce have become more dependent upon electronic transactions, money has also become more electronic. Many attempts have been made to come up with suitable forms of electronic money that mimic the physical world, or even create new forms of electronic money. However, despite the enormous need for such money, and efforts by some of the best minds and most successful companies in the world, electronic money has suffered many setbacks and been far slower to materialize than many had hoped or predicted. The reasons are many and varied, but some of the obvious reasons are security, ease of use/operation, and unwillingness of the public and/or commerce to make radical changes or embrace new technology and/or

procedures. As a result, many efforts, including several potentially promising efforts, have met with failure.

Even though new forms of electronic money have been slow to develop or gain widespread acceptance, electronic payments have still moved forward. Many banks now offer some form of electronic checking. And payment cards have been used for electronic transactions in e-commerce and m-commerce (mobile commerce). Still, there is widespread concern about the safety of such transactions, and recent news stories have uncovered widespread fraudulent activity associated with use of traditional credit card numbers in e-commerce over the Internet. In addition, there is growing concern about consumer privacy, or lack thereof, due to widespread electronic profiling of consumers who make electronic payments.

Although the media has been quick to cover fraud associated with use of credit cards over the Internet, it is often overlooked, at least by the public and the media (but not the credit card companies), that the majority of fraudulent activity concerning credit cards is not associated with e-commerce activity. Most fraud occurs in the "brick and mortar" world, and the numbers are daunting. Despite many attempts to combat unauthorized or fraudulent use of credit cards, it is estimated that credit card fraud now exceeds hundreds of millions, if not several billion, dollars per year. And this does not even count the cost of inconvenience to consumers, merchants and credit card issuer/providers, or the emotional distress caused to victims of such fraud, or the cost to society in terms of law enforcement and preventative activities.

Accordingly, there is a very real, long-felt need to reduce the amount of fraudulent activity that is associated with credit cards, and this need has only grown more acute as consumers and commerce search for better ways to purchase and sell goods and services via e-commerce and m-commerce. However, any solution needs to be something that is acceptable to the public at large. It should be easy to use. It should not be complicated or expensive to implement. Preferably, it should fit within the existing infrastructure, and not be something that requires a great deal of educational effort, or a radical change in behavior or habits of consumers. In other words, it should be user friendly, readily understandable and something that does not require a completely new

infrastructure, which is a reason suggested by some as to why smart cards have not been widely accepted in the United States.

In addition, it is highly desirable that any solution to such problems be capable of widespread use, in many different platforms, for many different applications.

In U.S. Patent No. 5,956,699 issued in September of 1999, Wong and Anderson were the first to introduce the methodology of a system for secure and anonymous credit card transactions on the Internet. This patent introduced a system which used an algorithm to use one's own selected Personal Identification Number or PIN as one's own de facto digital signature. The algorithm instructs the cardholder how to insert one's PIN into one's valid credit card number before using it for any transactions on the Internet. The resultant scrambled up credit card number, which is tailored by the algorithm to having the same number of digits as before, is rendered useless on the Internet because the PIN insertion algorithm is changed automatically after every transaction. This methodology is not only capable of drastically reducing credit card fraud on the Internet, it is also capable of safeguarding one's anonymity, and thus privacy, in credit card purchases on the Internet.

Since the issuance of U.S. Patent No. 5,956,699, Wong and Anderson have also invented an anonymous electronic card for generating personal Coupons useful in commercial and security transactions, as well as a method for implementing anonymous credit card transactions using a fictitious account name. The present invention is an extension of these prior inventions that seeks to provide new methods for allowing a user to customize the use of one-time unique numbers that can be used in credit card transactions in the brick and mortar world, e-commerce, m-commerce and in many other applications. Because the methodology is well suited for use in hardware and software applications, it has widespread applicability to many different types of transactions. In addition, the present invention allows a user to include data in the information that is transmitted as part of a normal payment card transaction. This allows the user a great deal of flexibility in customizing use of such a card. In addition, it allows a provider of the card to receive important information as part of the normal processing of a given transaction.

SUMMARY OF THE INVENTION

The present invention is generally directed to an electronic card that contains a magnetic storage medium, such as a magnetic stripe, and a mechanism for generating a data packet that can be read by a standard magnetic stripe reader. The electronic card also contains a card base, a computer or microprocessor, a display mechanism, an input mechanism and a power source. The present invention is also generally directed to methods for using such an electronic card. Such methods includes use of a data packet that can be read by a magnetic stripe reader and methods of customizing use of such a card, including customizing the use of an electronic card in financial transactions.

In another, separate aspect of the present invention, the data packet contains data representing a personal coupon and an alias that are readable by a standard magnetic stripe reader. The personal coupon and the alias can be used to conduct credit card transactions on or off the Internet. The data packet can also be used in a security device.

In other, separate aspects of the present invention, a computer in the electronic card executes a computer program, which can be a diagnostic program, to generate information that is stored in the data packet. An example of such a program is a program that checks on a battery life parameter. The program can generate a warning signal when a low battery condition is detected or a battery life signal related to an estimated remaining battery life of the battery. Such signals can be sent to the money source so that the user can be provided with a replacement electronic card either before or after the battery life drops below a selected threshold.

In still other, separate aspects of the present invention, a method for customizing payment card transactions is provided by allowing a user of a payment card to select a customization variable for any given transaction involving use of the payment card. The customization variable is submitted with the payment card number and a user identifier to a verification agency for validation. The customization variable may be used in a method for processing a plurality of payment card transactions based upon the user's selection of various customization variables. The present invention is particularly well suited for use

with electronic cards, but it can also be used in any method that uses a card number generator to generate a one-time card number.

The customization variable may involve customization of the generation of a one-time payment card number. An example of one way in which this can be done is to allow the user to choose either a first or a second user key as the key that will be used by an algorithm of a card number generator to generate the one-time payment card number. The customization variable may also involve customization of a user identifier associated with the one-time payment card number. An example of one way in which this can be done is to allow the user to choose either a first or a second identifier. The customization variable may also involve inclusion of a customization variable with the one-time payment card number and the user identifier when they are submitted to the verification agency for validation.

In still further, separate aspects of the present invention, multiple handling options provide numerous options for processing payment card transactions. The handling options can include billing two separate accounts. The user can be sent a single bill for charges to the two separate accounts, even if the accounts are established with different entities, such as different credit card companies or banks, or the user can be sent a first bill for the first account and a separate bill for a second account. One of the accounts can be a credit account and another account can be a debit account. The handling options can provide a mechanism for classifying the nature of the payment card transactions, such as using a first handling option for business transactions and a second handling option for personal transactions. They can also provide different mechanisms for controlling access to information concerning payment card transactions. One mechanism can be used to implement restrictions on distribution of information relating to payment card transactions or restrictions on distribution of personal information of the user to second entities. The user can be charged consideration for use of this mechanism. Another mechanism can be used to permit distribution of information relating to payment card transactions to third parties or permit distribution of personal information of the user to second entities. The user can be given consideration to use this mechanism.

In yet other, separate aspects of the present invention, a method is provided for delivery of an item purchased through a secure and anonymous transaction between a user and a merchant with subsequent. The user selects a customization parameter at the time of purchase that is used to implement an anonymous delivery method. The customization parameter can be used to customize generation of a user-one time payment card number, a fictitious user identifier or as a customization variable included with the user one-time payment card number and the fictitious user identifier in a transaction data packet provided by the user to the merchant, and ultimately to the money source. After the money source confirms that the transaction is valid and that the user has elected an anonymous delivery option, the money source sends a tracking identifier to the merchant and a delivery agent. Next, the merchant delivers the purchased goods to the delivery agent, and the delivery agent delivers the purchased goods to a delivery address provided by the money source. The merchant need not ever be provided with the delivery address, and the delivery agent need not ever be provided with any details concerning the goods or the transactions.

Accordingly, it is a primary object of the present invention to provide an electronic card that can be used for commercial and security transactions in which an input is needed to control the function of the card and methods for using such cards.

This and further objects and advantages will be apparent to those skilled in the art in connection with the drawings and the detailed description of the preferred embodiment set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a physical layout of a preferred embodiment of a Universal Anonymous Credit Card (UACC) in accordance with a preferred embodiment of the present invention.

Figure 2 is a system block diagram of a preferred embodiment of the Universal anonymous Credit card (UACC) in accordance with a preferred embodiment of the present invention.

Figure 3 is a physical layout of a preferred embodiment of the Universal anonymous Credit Card (UACC) in accordance with a preferred embodiment of the present invention.

Figure 4 shows an un-coded magnetic stripe likened to a series of aligned South-North magnetic domains.

Figure 5 shows a sudden introduction of a strong magnet having an opposite orientation on top of a magnetic domain of the magnetic stripe causing flux reversals.

Figure 6 shows flux reversals caused by sudden introduction of strong magnet having opposite magnetic orientation on top of a magnetic domain in a magnetic stripe.

Figure 7A is an un-coded portion of a track of a magnetic stripe having 5 bit cells showing no flux reversals.

Figure 7B shows a representation of all "0", all "1" and "0" and "1" side by side according to the Aiken Biphase encoding code.

Figure 7C shows a representation of decimals "0", "5" and "9" in the Aiken Biphase encoding standard.

Figure 7D shows a preferred embodiment of an encoder head of the present invention.

Figure 8 shows a preferred embodiment of an encoder of the present invention with drive electronics and logic.

Figure 9 is a simplified, schematic diagram of a preferred method of using an electronic card in a financial transaction.

Figure 10 is a physical layout of a front-side of an alternate preferred embodiment of a Universal Anonymous Credit Card.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

1. A preferred embodiment of an electronic card

In a preferred embodiment of the present invention, a unitary, self-contained electronic device is provided having physical planar dimensions that are essentially identical to those of a conventional magnetic stripe credit card, which is widely used in electronic commerce today. The device has several components,

although some components can be combined together or omitted from some embodiments.

An initial component is the card base. The other components, in one way or another, are attached to this base.

Another component is a computer or microprocessor. It is preferable that the computer be a single integrated chip, but it need not be. A computer typically contains a central processing unit connected to both storage memory and random access memory (RAM). RAM is used to load and run application programs as well as for storing data during run time. The storage memory can hold a variety of computer programs.

Still another component is a display controlled by the computer. In one preferred embodiment, this is a liquid crystal display (LCD). The LCD can be controlled by a LCD driver, and the LCD driver can be contained in storage memory of the computer. In an alternative embodiment, the display is a series of light-emitting diodes, each of which is associated with a numeric key of a keypad. In still another alternative embodiment, the display can be an electronic ink display, which is a novel and newly available display medium. The electronic ink display can be fabricated with highly flexible physical dimensions, especially in thickness, which is likened to a thin piece of paper and also much cheaper to manufacture than conventional LCD display.

The card must also have an input mechanism. In the preferred embodiment, this is a keypad. However, it is possible that the input mechanism might rely upon voice recognition as this technology becomes more and more developed.

The card also has a magnetic storage medium, which, as already noted, is a magnetic stripe in an especially preferred embodiment.

The card also has a mechanism for generating a data packet. In a preferred embodiment, an encoder is used to generate a data packet that is stored in a designated portion of the magnetic storage medium. This component allows the electronic device to be dynamic by relying upon an input to generate the data packet.

Finally, the card has a power source. In the preferred embodiment, this is a battery or a solar cell.

1.1 Use of the preferred embodiment in a credit card

The electronic card just described can be used in a method for implementing an anonymous credit card transaction between a user and a merchant. A preferred embodiment of such a method is depicted in Figure 9. In accordance with this preferred embodiment, a user must first establish a user account with a credit source. The credit source may be a bank, a credit card company or any other institution involved with issuance of credit cards or bank debit cards, such as a credit union or other institution, or a money source as described in U.S. Patent No. 5,913,203. When the user establishes a user account with the credit source, one or more user settlement mechanisms through which the user can pay the credit source for charges and fees billed to the user account will be established. For example, in the case of credit card transactions, the user and the credit source will enter into an agreement concerning use of the credit card. As a further example, in the case of debit or electronic checking services, the user and credit source may enter into a separate agreement concerning how and from what account such debits will be debited.

After a user account is established, the credit source will create one or more user account records associated with the user account to contain a variety of information including a user account number, a fictitious account name, a "Proxy Agent," a user key and, when applicable a user insertion key. The fictitious account name can be selected by the cardholder or the issuer of the credit card, but it has to be known by both. The "Proxy Agent" is used to conceal the cardholder's actual address and still comply with current credit card regulations – in other words, it is a fictitious address. Additional information that might typically be contained within such records includes cross references to other accounts, the user's name and the user's billing address.

One function of this electronic credit card, which shall be referred to as the Universal Anonymous Credit Card (UACC), is to allow a credit cardholder to execute secure and anonymous credit card transactions on and off the Internet. This can be done in a system and in methodology in which merchants no longer have access to the cardholder's real name, address and the actual valid credit card number. Such an effectual personal encryption does not, however, prevent the additional use of an Internet standard encryption such as SSL or SET for

online data exchanges. The latter will simply make such online transactions even more secured.

For purposes of clarification and illustration, an example of an application that uses the methodology taught in U.S Patent No. 5,956,699 is presented here. Assume that the card number (CN) stored in the electronic card and the PIN number are, respectively:

CN = 4678 0123 4567 8012 1200

PIN = 2468

Next, assume that the application uses an algorithm that first deletes four (4) digits from the CN and then inserts in their place the PIN according to the insertion sequence indicated by a so-called PIN Sequence Insertion Number (PSIN) in order to come up with a scrambled Anonymous Credit Card Number (ACCN), also containing 20 digits. The 4-digit PSIN number can either be chosen by the cardholder or assigned by the issuer. Let us assume for this example that the cardholder's PSIN is 1357.

Next, assume that the algorithm only operates on digits 7 through 16 of the CN. This takes into account the fact that the first 4 digits of the standard CN denote the identification of the credit card issuer and the last 4 digits of the standard CN are reserved for the expiration date, all of which should be left undisturbed. Thus, it is the middle 11 digits that indicate the account number for the cardholder of the CN. Therefore, the algorithm calls for the cardholder to first delete the last four digits of the 10-digit account number. In this example the 4 digits to be deleted will be "8012". The 6-digit number before the cardholder PIN is inserted according to the cardholder's PSIN is "23 4567".

Now the algorithm defines the numbering convention of the digit positions in the ACCN. The first digit position is defined as the zeroth (0th) and the second is the first (1st) etc. Thus, according to the PISN 1357, the PIN 2468 should be inserted to form the ACCN as follows:

ACCN = 467801 22344658 671200

The 4 digits of the PIN= 2468 occupy, respectively, the 1st, 3rd, 5th and 7th positions (according to PISN=1357) using the defined digit position numbering convention. In a simpler algorithm for inserting the PIN, the PIN number itself can act

effectively as the PSIN so that the cardholder does not have to remember two numbers. Using such an algorithm, in the example above, the ACCN will now be:

ACCN = 467801 2324456687 1200

The 4 digits of the PIN = 2468 also occupy, respectively the 2nd, 4th, 6th and 8th positions of the ACCN (according to an implicit PSIN = PIN = 2468) using the defined digit position numbering convention.

The foregoing is an example of a very simple algorithm to generate a valid personal charge number. As would be apparent to a person of ordinary skill in the art of computer programming, especially with the benefit of this disclosure, much more complicated algorithms could be devised and used which would use the card number and the user key to generate a valid personal charge number.

The applications just described can be used in a system that reduces fraud while protecting consumer privacy through anonymous transactions, on and off the Internet. Such a system has three main components that are provided to complete a commercial credit card transaction. First, instead of using a valid credit card number, an ACCN is used. Second, instead of using the cardholder's real name, an alias is used. The alias can be selected by the cardholder or the issuer of the credit card, but it has to be known by both. Third, instead of using a cardholder's real address, a "Proxy Agent" is used to conceal the cardholder's actual address and still comply with current credit card transaction regulations. In such a system, the use of a credit card for transactions on the Internet can be anonymous to all except the cardholder and the credit card issuer.

When the electronic card is used in a retail transaction, by merely entering one's own PIN into the electronic card prior to giving it to the merchant for swiping the credit card transaction, one takes full advantage of the secure and anonymous transaction afforded by the electronic card. The user can first check his or her alias and entered PIN (note that the PIN is not stored in the electronic card) using the keypad on the electronic card before the electronic card is handed over to the merchant. Since the cardholder has in effect already signed the transaction with a digital signature (his or her PIN), no additional hand signature is required to complete the transaction. The merchant only need receive the PIN-modified anonymous credit card number (ACCN) and the user's alias. The ACCN and the aliases are read by a conventional magnet stripe reader and are processed in

exactly the same fashion as a conventional credit card number and credit cardholder name since such information can be sent to a credit card approval agent for approval of the transaction. The credit card approval agent has all of the information necessary to determine if the transaction is valid or fraudulent. The identity of the entity who authorized the credit card, as well as its expiration date, is available in the ACCN in just the same manner as it is available in a conventional credit card transaction. The card number is verified by confirming the card number contained in the ACCN as valid for the alias.

To use the electronic card for Internet transactions, a cardholder first enters the PIN into the electronic card exactly like that for off the Internet transactions. Next, the cardholder continues the transaction using only the cardholder's alias, the ACCN appearing in the LCD display and also the cardholder's choice of trusted delivery or Proxy Agent (optional) should the cardholder prefer to make this transaction completely anonymous. Thus, by carrying just one electronic card which looks and feels exactly like a regular magnetic stripe credit card, one is now able to make old world credit card transactions like one always has done in the past. But more importantly, one can now use the same electronic card for making secure an anonymous transaction, anywhere in the world, and for both on and off the Internet transactions.

As is apparent from the foregoing description, the real name and address of the cardholder, including the credit card number itself, never need appear on the Internet or even need to be made known to the merchant. Even though the ACCN or Coupon (Customer One-time Unique Purchase Order Number) does appear, together with the alias of the cardholder, across the Internet during the online transaction, this ACCN or Coupon number does not stay the same, but changes automatically after every transaction or use. Thus, no valid credit card numbers are actually available in transmission for theft by anybody. Only the ACCN or Coupon number will appear on any or all transaction records and that number is useless for subsequent transaction because it is time variant.

1.2 Additional details regarding construction of one preferred embodiment of an electronic card

In order to reduce the cost of use of the UACC, and increase the range of applications in which it can be used, the UACC should have a magnetic storage

medium that can be read by a standard magnetic stripe reader. This means that the magnetic storage medium must be capable of being read by a standard magnetic stripe reader. It also means that the portion of the UACC containing the magnetic storage medium must be sized such that the magnetic storage medium will work with standard magnetic stripe readers. A standard magnetic stripe reader works by passing the magnetic stripe portion of a card, such as a credit card, through the magnetic stripe reader in a swiping motion. Standard magnetic stripe readers have been prevalent in retail stores throughout the United States for many years.

An especially preferred embodiment of the present invention will now be described in even greater detail. The especially preferred embodiment uses a standard microprocessor having its usual Central Processing Unit (CPU), Read-Only-Memory (ROM), Random-Access-Memory (RAM) and Input-Output devices (I/O). There are two types of ROMs in the UACC. The first type is a standard semiconductor ROM, ROM1, fabricated as part of the microprocessor. ROM1 stores the microprocessor operating system and also the bulk of the methodology software. The second type of ROM, ROM2, is a portion of a magnetic stripe, namely Tracks 1 and 3. ROM2 stores the relevant information about the cardholder such as primary account number VCCN, name, expiration date, encrypted PIN etc. There are also two types of RAMs in the UACC. The first type of RAM, RAM1, is a standard semiconductor RAM as part of the microprocessor and needed for its normal operation. The second type of RAM, RAM2, is a portion of a magnetic stripe, namely Track 2. RAM2 temporarily stores the encoded ACCN to be read by a standard magnetic stripe reader during a normal credit card transaction after the cardholder inputs the PIN according to the PSIN algorithm into the UACC.

The methodology software is installed into ROM1 of the microprocessor during production. A standard parallel port Input Device serves to interface a numeric keypad and other functional switches of the UACC to the microprocessor. The UACC also has two Output Devices. The first Output Device is a standard parallel output port of the microprocessor used for interfacing to it a 10- or more character alphanumeric LCD display through a driver for outputting information such as recalling from memory alias or typed in PIN verification. It is also used for

production testing and repair or servicing of the UACC. The second Output Device is an integrated circuit (IC) magnetic encoder unit built into the UACC so as to encode Track 2 of the magnetic stripe or RAM2, either statically in conjunction with the existing magnetic stripe, or dynamically without the use of the existing magnetic stripe, with the temporary ACCN information for off the Internet credit card transactions. In this especially preferred embodiment of the present invention illustrated below, only the static magnetic encoder working in conjunction with the existing magnetic stripe is described in detailed. For those skillful in the art, the dynamic thin film magnetic encoder, working without the use of the existing magnetic stripe, can also be used in the present invention as an alternative embodiment. In a preferred embodiment of the present invention, the UACC also contains a battery cell, ON/OFF and other functional switches to render it a fully functional and self-contained credit card (see Figure 1).

The UACC bridges the old economy world of brick and mortar to the new economy world of the Internet. The integrated circuit (IC) magnetic encoder with current-carrying conductive writing heads is fabricated on a flexible and ultra-thin polymer (e.g. polyimide) printed circuit board (PCB) intimately in contact with the magnetic stripe located above for data impression. The encoder driver and digital logic chips are also mounted on the flexible PCB, but in different areas to form the complete IC magnetic encoder. The IC magnetic encoder is technically compatible with conventional magnetic data transfer methodology and makes possible the fabrication of the present UACC with physical dimensions exactly like those for a regular magnetic stripe portion of a credit card.

Even greater detail will now be provided by reference to Figures 1 through 8.

Figure 1 shows the physical layout for an embodiment of the present electronic device or Universal Anonymous Credit Card (UACC) 1. The areal dimensions of the UACC 1are 3.375" x 2.125" or exactly those of a regular magnetic stripe credit card in use in electronic commerce today. The thickness of the UACC 1 varies from ~0.030" at the top where the magnetic stripe resides to 0.030" – 0.060" for the rest of the card dependent upon the thickness of the LCD used (see Figure 1). Besides the ON/OFF switch 3, the front side 2 of this UACC 1 has five (5) more functional switches, 4-8, labeled and defined as follows:

ATM (switch 4) = Reserved for Automatic Teller Machine (ATM) card

ACC (switch 5) = Reserved for Anonymous Credit Card (ACC or A-Card)

IC (switch 6) = Reserved for Internet Type II Cash

MC (switch 7) = Reserved for standard Magnetic Stripe Credit Card

BC (switch 8) = Reserved for A-Card transactions using bar codes

In addition to the switches 3 – 8, there is a 12-character keypad 9. The primary function of the keypad 9 is for the cardholder to enter the PIN into the UACC 1 for generating the ACCN for on and off Internet commerce transactions. There is also a 10- or more character alphanumeric liquid crystal display (LCD) 10 on the front side 2 of the UACC 1. This LCD 10 displays the alias and the ACCN for use for Internet commerce transactions or the alias and bar code representing the ACCN after the cardholder's PIN is entered. The display of the ACCN will automatically erase itself after about 2 minutes to avoid exposing significant information to third parties.

At the top of the back side 11 of UACC 1 is a standard 3-track magnetic stripe 12 found in every common magnetic stripe credit card in use today. Track-1 13 and track-3 14 are used to store the relevant information about the cardholder such as primary account number VCCN, name, expiration date, encrypted PIN etc. Track-2 15 of the magnetic stripe 12 normally contains only the cardholder's VCCN to be read by a magnetic stripe reader at the merchant's site. For the present UACC device, the ACCN, instead of the VCCN, will be generated on command by entering the PIN with the appropriate function switch "MC" 7 by a special encoder 16 located at a designated location underneath the magnetic strip 12. As will be explained in more detail below, the generated ACCN which resides temporarily on Track-2 15 of the magnetic stripe 12 will disappear automatically 2 minutes after it is being generated. This is to ensure that no significant information about the credit card account stays long enough for someone to steal for committing subsequent credit card frauds.

The system block diagram for the especially preferred embodiment of the present invention is shown in Figure 2. At the center of the system is a conventional 16-bit microprocessor 16 comprising a Central Processing Unit (CPU) 17, a Read-Only-Memory (ROM1) 18, a Random Access Memory (RAM1) 19, a 16-bit parallel Input Port (Input) 20 and a 16-bit parallel Output Port (Output)

21. The microprocessor 16 receives inputs through Input 20 from a bank of functional switches 22, which contains switches 4 through 8. The microprocessor also receives inputs from a 12-character keypad 9 through Input 20. Outputs from the microprocessor 16 emanate from Output 21 through a LCD display driver 23 to reach the 10- or more character alphanumeric LCD display 10 and also through an encoder driver 24 to reach a designated location of Track-2 15 of the magnetic stripe 12. Such a designated location of Track-2 15, where the encoder 25 is positioned, serves as a second RAM, RAM2, for the microprocessor 16. RAM2 stores the encoded ACCN needed for offline credit card transactions to be read by the merchant's standard decoding equipment very much like a conventional magnetic stripe credit card.

The software program is installed into ROM1 18 of the microprocessor 16 during production of the current UACC unit. Information pertaining to the cardholder is encoded onto Track-1 13 and Track-3 14 of the magnetic stripe 12 which serves as an independent ROM, ROM2, for the UACC unit. Since information stored in ROM2 will be read with a standard magnetic stripe reader, it operates independently of the microprocessor 16. A battery supply 26 with contacts 27, controlled by the ON/OFF switch 3, completes the UACC system. The battery supply provides power to all the components of the UACC system, including the microprocessor 16, LCD display driver 23, encoder driver 24, LCD display 10 and the keypad 9.

Figure 3 shows the physical layout and construction for the especially preferred embodiment of the present UACC device. All the electronic components of the system, namely the microprocessor 16, the LCD display 10, the keypad 9, LCD display driver 23, encoder driver 24, encoder 25, functional switches 4-8, ON/OFF switch 3 and battery contacts 27 with battery cell 26, are fabricated on a flexible multi-layered printed circuit board 28. The flexible printed circuit board 28 with all the loaded components is then encapsulated in plastic into thin 29 and thick 30 parallel sections as shown in Figure 3. The thickness of the thin section 29 where the conventional magnet stripe 12 will be fabricated on top of the encoder 25 (to be explained in more detail below) on the backside is about 0.030", the same thickness as the magnetic stripe credit cards in use today. The plastic encapsulated thick section 30 (see Figure 3), while holding the fully-loaded flexible

printed circuit board 28 in place, allows the ON/OFF switch 3, functional switches 4-8 and the keypad 9 to be physically accessible (e.g. by fingers) from the front side of the UACC device. The LCD display 10 is also directly visible from the front side. Note that the thickness of the plastic encapsulated section would also be 0.030" thick if a polymer-backed (e.g. Mylar®) ultra-thin LCD display (0.020" thick typical) is used.

1.2.1 Background discussion of magnetic stripe technology theory

A much simplified theory on magnetic stripe technology, especially on how to encode (write) and decode (read) digital data respectively on and off a magnetic stripe used in ordinary credit cards of today, will now be provided in order to better explain one way in which an encoder can be fabricated and work. A magnetic stripe is made out of a thin layer of very tiny ferromagnetic particles (typically 0.5 micron long) bound together with resin and subjected to a very strong magnetizing magnetic field (known as "coercivity") when such a stripe is printed onto a substrate. When the resin is cured or set, these tiny "magnets" are magnetically and permanently aligned (magnetized) into a series of South-North magnetic domains forming a chain of S-N, S-N ... interfaces. The adjacent N-S magnetic fluxes of these magnetic domains are normally linked together for the entire magnetic stripe to act like a single magnet with South and North poles at its ends. In other words, an un-encoded magnetic stripe is actually a series of aligned South-North magnetic domains (see Figure 4).

If a N-N interface (instead of the normal N-S interface for un-encoded magnetic domains) is created somewhere on the stripe, the magnetic fluxes at the N-N interface will repel each other, resulting in a concentration or increase of flux lines around the N-N interface called a "flux reversal". The same situation exists for a S-S interface as compared with a normal N-S interface. Such a situation will take place if a strong magnetizing magnet 31 having an opposite magnetic orientation, namely N-S, is suddenly introduced on top of one of the S-N magnetic domains 32 of the magnetic stripe as shown in Figure 5. The magnetic domain 32 will realign its magnetization as that of the strong magnet on top of it, namely N-S. Under this situation, two flux reversals have taken place, as illustrated in Figure 6.

The process of encoding or writing involves the creation of N-N and S-S magnetic domain interfaces, or flux reversals, and the process of decoding or

reading that of detecting them. Knowing that magnetic flux lines always emanate from the North pole and terminate on the South pole, a sudden introduction of a strong magnetic field (greater than the coercivity of the magnetic domains) having a N-S magnetic orientation can magnetize a normal S-N magnetic domain into N-S orientation, resulting in the creation of a pair of flux reversals S-S and N-N, much like that shown in Figure 6 above.

Before proceeding to explain how the encoder of the especially preferred embodiment writes the ACCN on Track-2 15 of the magnetic stripe 12, it is helpful to delve deeper into the data storage mechanics of the magnetic stripe 12 itself. As stated earlier, the magnetic stripe 12 has three tracks, namely Track-1 13, Track-2 15 and Track-3 14. Digital data are stored in these three tracks according to the American National Standards Institute (ANSI) and International Standards Organization (ISO) BCD (5-bit Binary Coded Decimal Format) or ALPHA (alphanumeric) standards. The ANSI/ISO standards for Tracks 1, 2 and 3 are summarized in Table I as follows:

Table I. ANSI/ISO Track 1, 2, 3 Standards

Track	Name	Density	Format	Characters	Function
1	IATA	210 bpi	ALPHA	79	Read Name & Account
2	ABA	75 bpi	BCD	40	Read Account
3	THRIFT	210 bpi	BCD	107	Read Account & Encode

Track-1 13, named after the "International Air Transport Association" (IATA), contains the cardholder's name as well as account and other discretionary data. Track-2 15, "American Banking Association" (ABA), is the most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA designed the specifications of this track and it is believed all major world banks abide by it. It contains the cardholder's account number, encrypted PIN, plus other discretionary data. Track-3 14 is unique and intended to have data read from and written on it. At present, it is an orphaned standard and has not been widely used to date.

Before the encoder can write on command the ACCN on Track-2 15 of the magnetic stripe, attention must be paid to the data layout for Track-2 15.

Encoding protocol specifies that each track must begin and end with a length of all Zero bits, called CLOCKING BITS. These are used to synchronize the self-clocking feature of bi-phase decoding, an industry standard. A typical Track-2 layout is shown as follows:

0000000000000000 ; 1111222233334444=9912****000000XXXX0000?

The symbol ";" after the "0's" is the "START SENTINEL" according to the BCD data format. The 4 digits "1111" following is the issuer or acquiring bank's identification number. The 12 digits following is the cardholder's account number. The symbol "=" following is the "FIELD SEPARATOR" according to BCD data format. The 4 digits "9912" following is the expiration date. The four characters following "****" are data reserved for private use. The data length "XXXX" after the string of 0's may vary and is the encrypted PIN offset. Finally the symbol "?" after another string of 0's is "END SENTINEL".

The location of the 12 digits that need to be encoded or written on command is represented by "2222 33334444" on Track-2 15 of the magnetic stripe 12 in the example cited above.

Next, it is helpful to have an understanding of how the 12 digits are represented in BCD data format on Track-2 15 of the magnetic stripe 12. According to the BCD data format, each decimal digit is coded by 5 bits. The ANSI/ISO BCD Data Format is reproduced in Table II below. Note that all 21 digits, including the field separator, namely "1111222233334444=9912", can also be encoded on command if so desired.

Table II. ANSI/ISO BCD Data Format

Data Bits				Parity	Character[1]	Function
b1	b2	b3	b4	b5		
0	0	0	0	1	0 (0H)	Data
1	0	0	0	0	1 (1H)	Data

0	1	0	0	0	2	(2H)	Data
1	1	0	0	1	3	(3H)	Data
0	0	1	0	0	4	(4H)	Data
1	0	1	0	1	5	(5H)	Data
0	1	1	0	1	6	(6H)	Data
1	1	1	0	0	7	(7H)	Data
0	0	0	1	0	8	(8H)	Data
1	0	0	1	1	9	(9H)	Data
0	1	0	1	1	:	(AH)	Control
1	1	0	1	0	;	(BH)	Start Sentinel
0	0	1	1	1	<	(CH)	Control
1	0	1	1	0	=	(DH)	Field Separator
0	1	1	1	0	>	(EH)	Control
1	1	1	1	1	?	(FH)	End Sentinel

Note 1. Hexadecimal conversions of the data bits are given in parenthesis (xH).

How BCD data is actually encoded onto Track-2 15 of the magnetic stripe 12 can now be explained. Table I above notes that Track-2 has a density of 75 bits per inch (bpi). According to the ANSI/ISO BCD data format, each character is represented by 5 bits. Thus, if the encoder needs to encode 12 digits (see "222233334444" in example above), it will require a total of 60 bits. Since the density is 75 bpi, the maximum physical space available for a stationary encoder head is 0.800". But the important dimension for the design of the encoder head is the space available for each BCD bit. In the present case, the bit dimension is 1,000 mils/75 bits or 13.33 mils (0.0133") per bit.

At this point, it is useful to explain with the help of Figures 7 A-D, how a single character or decimal digit comprising 5 bits in the ANSI/ISO BCD data format is encoded onto Track-2 15 of the magnetic stripe 12. Figure 7A shows an un-encoded strip of Track-2 long enough to accommodate 5 bits of data. The physical length of this strip is 5 x 0.0133" or 0.0667" (66.65 mils). This un-encoded strip is divided into five segments, each representing a single bit, and each is further represented by two magnetic domains as shown in Figure 7A. In

accordance with the industry standard of encoding called Aiken Biphase, or "two frequency coherent-phase encoding", data is encoded in "bit cells" defined above and the frequency of which is the frequency of the '0' signals. '1' signals are exactly twice the frequency of the '0' signals. So, at least from the conventional way of decoding, the actual frequency of the data passing the 'READ' head will vary with the swipe speed, for the data density, control functions etc., the '1' frequency, however, will always be twice the '0' frequency. This is illustrated in Figure 7B where the representation of all '1s' , all '0s' and how '1' and '0' data exist side by side. Note that in Figure 7B, the bit cell waveforms for '0' and '1' are the results of creating the so-called flux reversals of "N-N" or "S-S" at the magnetic domains interfaces of the un-encoded strip. For the stationary encoder of the present preferred embodiment, the encoding must be consistent with the Aiken Biphase convention because the same 'READ' heads will be used to decode the Track-2 data temporarily stored in UACC devices during offline (off the Internet) credit card transactions.

Consistent with the Aiken Biphase convention therefore, Figure 7C shows, as an illustration, how BCD decimal digits '0', '5' and '9' would appear referenced to the un-encoded 5-bit strip of Figure 7A. Also shown in Figure 7C are the orientation of the magnetic domains and the flux reversals at the domain interfaces. Thus, if an encoder head of the present preferred embodiment is designed to be on top of the 10 magnetic domains representing the 5-bit decimal digit, it would be possible to magnetize on command the individual domains in order to create the appropriate flux reversals corresponding to the desired decimal digit. This is illustrated in Figure 7D. The orientation of the magnetic domain 33 when un-coded is S-N as shown in Figure 7D. The two contact bits 34 and 35 control which direction the magnetizing current is flowing. When 34 and 35 are suddenly made "1" and "1", current I+ will flow in from contact 34 to ground resulting in flipping the orientation of magnetic domain 33 to N-S. Meanwhile the current I- from "+V" to contact 35 is zero. When contact 34 and 35 are suddenly left open circuited, both I+ and I- are zero and the orientation of magnetic domain 33 will stay as N-S. When contacts 34 and 35 are suddenly changed to "0" and "0", current I- will flow from "+V" to contact 35 and cause the magnetic domain to revert back to S-N while I+ is zero. No domain flipping occurs if the bits for

contacts 34 and 35 are either "1" "0" or "0" "1". In the former case, the magnetizing effect of I+ is neutralized by I-. Both I+ and I- are zero for the latter case. The magnitudes of currents I+ and I- needed to flip the magnetic domains with coercity of the order of 300-500 gausses ("soft" magnetic stripe found in conventional credit cards) for current carrying conductor of 1-2 microns thick are several hundred milliamperes. The electrical power required to encode or decode 12 decimal digits is of the order of tens microwatts.

In order to encode in the present example a total of 12 decimal digits, one would need to encode 5 x 12 or 60 bits of data. As shown in Figure 7D, the encoder has to have two micro-heads per bit of data. Furthermore, each micro-head has a PLUS or MINUS polarity. If the polarity is PLUS, current will flow in one direction so as to generate a N-S magnetizing magnet. Similarly, if the polarity is MINUS, current will flow in the opposite direction so as to generate a S-N magnetizing magnet. So the encoder of the present preferred embodiment will have 2 x 60 micro-heads each with a PLUS and MINUS polarity. An especially preferred embodiment of the encoder with the driver electronics and logic is shown schematically in Figure 8.

Figure 8 shows the 12 decimal digits divided up into 60 bit cells with each bit cell comprising two magnetic domains and each having a PLUS and MINUS polarity. There are therefore a total of 120 magnetic domains that have to be addressed, each with two polarities, making it a total of 240 address lines as shown in Figure 8. These addresses lines are accessed in bunches of 10 (5 magnetic domains or 21/2 bit cells). The address originates from using 10 bits of the 16-bit Output port 21 (see Figure 2 of system block diagram for UACC) and then through the encoder driver 24 (also see Figure 2) as current buffer before being connected to the 24 bunches of 10 address lines. Each of the 24 bunches of 10 address lines is accessed with a 32:1 decoder using five of the 16 bits of the Output parallel port 21. The decoder selects one of the 24 bunches of 10 address lines via switch bank 36 (there is a total of 24 switch banks similar to switch bank 36) comprising 10 switches each. In essence, it is the switch bank that selects which of the 10 address lines out of the 24 bunches that are being connected to the output of the encoder driver 24. Thus, it is possible to encode the 12 decimal digits into a designated location of Track-2 15 of the magnetic stripe with

commands from the microprocessor and outputted through the parallel port 21 through the encoder driver 24. Such a software command is stored in ROM1 (see Figure 2) of the microprocessor 16. The stored algorithm generates the ACCN or, in essence, a "Coupon" (Customer's one-time unique purchase order number), from the valid credit card number VCCN and the cardholder's PIN when inserted properly into part of the VCCN.

1.3 Additional details regarding use of the Universal Anonymous Credit Card

The manner in which the Universal Anonymous Credit Card (UACC) will work under different on and offline transaction circumstances will now be described in greater detail. It is first assumed that the cardholder has opened an UACC account with an issuer or acquiring bank. The cardholder has turned over a real name, address, personal and financial information to the issuer. In return, the cardholder is assigned a valid credit card number, VCCN, a credit limit, an Alias (chosen by the cardholder) and a proxy agent, and most importantly a cardholder UACC. The issuer has to assign the cardholder a proxy agent to use instead of giving out the cardholder's address in order to comply with the existing credit card transaction regulation. After obtaining a UACC from the issuer, the cardholder is now free to do anything and everything on and off the Internet safely with full assurance that nobody will find out what, where, when and how money is being spent with the UACC card, except its issuer.

The manner in which the cardholder can use his or her UACC to shop on the Internet will now be described. It is possible that not every online merchant will accept the UACC in the beginning, so the cardholder may have to identify those merchants that are partners with the UACC issuer bank. Otherwise, the transactions with the UACC will not be processed properly by the existing infrastructure that processes only conventional credit cards. Suppose the cardholder now wishes to purchase some merchandise from an online merchant who accepts UACC. All the cardholder has to send to the merchant's Web site online is his or her alias, a proxy agent's name assigned to the cardholder by the issuer bank, the ACCN or anonymous credit card number which will be obtained from the UACC (to be explained below), the merchandise and shipment choice. This is completely different from what the cardholder normally has to give out, viz.

a real name, address and the valid credit card number, should the cardholder use a regular credit card. To obtain the ACCN from his UACC device, all the cardholder has to do is to first push the button "CC", which is reserved for Anonymous Credit Card transactions, then to enter the cardholder's PIN using the keypad and then the "#" key. In the LCD display, the alias will first be scrolled across the display followed by the 10-digit ACCN. Note that the first six digits (four digits are used to identify the issuer bank and two more digits to designate a specific BIN number) and the last four digits of the ACCN always remain the same as those in the VCCN which signifies the issuer's identification and credit card BIN number, and the expiration date respectively. The cardholder can then use this ACCN to complete the transaction with the online merchant. After the cardholder finishes using the ACCN, he or she can either erase it from the LCD display by pressing "*" followed by "#" in the keypad, otherwise the ACCN will disappear from the LCD display automatically after approximately 2 minutes.

As one can see from this transaction on the Internet using the UACC, the real name and address of the cardholder, including the credit card number itself, never appear on the Internet or even are made known to the merchant. Even though the ACCN or Coupon does appear, together with the alias of the cardholder, across the Internet during the online transaction, this ACCN or Coupon number does not stay the same, but changes automatically after every transaction or use. Thus, unlike all the other credit card transactions on the Internet today, no valid credit card numbers are actually available in transmission for theft by anybody. Only the ACCN or Coupon number will appear on any or all transaction records and that number is useless for any subsequent transactions because it is time variant.

For off the Internet transactions, the UACC behaves just like an ordinary credit card. The only difference is that before one hands over the UACC to the merchant for charging the amount, one enters one's PIN after pushing first the "MC" button on the UACC device, which is reserved for magnetic stripe credit card transactions, and then follows it with a "#" key on the keypad. It is assumed here that the cardholder is satisfied with what is being charged on the credit card before the cardholder, in effect, "signs" it digitally in the transaction. Unlike ordinary magnetic stripe credit cards of today, no personal hand signature is

needed for off the Internet transactions with the UACC. By entering the PIN, the UACC automatically encodes temporarily the ACCN onto Track-2 of the magnetic stripe 12. The use of the resultant ACCN or Coupon is likened to the cardholder already signing the credit card with a personal digital signature for the transaction. The rest of the transaction simply follows that of a regular magnetic stripe credit card with the existing credit card processing infrastructure.

2. An alternative preferred embodiment of an electronic card

Another preferred embodiment with an alternative structure will now be described. In this embodiment, which is depicted in Figure 9, the electronic card does not have a display, such as the LCD; instead, the keypad has LEDs associated with its numeric keys. Otherwise, its structure is similar to prior preferred embodiment.

Figure 10 depicts a front side 2 of an electronic card 1. The electronic card 1 has a twelve key keypad 9. Ten of the keys are numeric, for numerals 0-9, and two are special function keys, namely an ENTER key and a CLEAR key. All of the keys are touch activated. In addition, keypad 9 has ten light-emitting diodes ("LEDs"), 101-110, one for each of the numeric keys. It is especially preferred that the LEDs be located in the same corner of each key, but it would also be possible, although less desirable, to make the LEDs a separate element, such as a separate array of LEDs. The electronic card 1 also contains two additional LEDs, 111 and 112, which function as a visual display device for indicating whether a personal identification number ("PIN") has been correctly entered into the card by designating whether the card is ready or whether there has been an error. If desired, the electronic card 1 can also contain one or more special function keys 113.

The purpose of the LEDs 101-110 is to allow a user to confirm correct entry of numbers into keypad 9. After card 1 is turned on by On/Off switch 3, once a numeric key is activated by touch, the LED associated with that LED will light up and remain lit for a specified time or until another key is activated by touch, whichever is shorter. The LEDs can be controlled by an LED driver (not shown). Because there may be times when the user does not want the LEDs to light up, or certain useres who do not want such a feature, the LEDs can be turned off by

entry of a specified preprogrammed code into card 1, and, if subsequently desired, reactivated. Thus, for example, a deactivate or reactivate sequence might be a series of key entries such as ENTER, ENTER, 7, 2, 5, ENTER, ENTER, 7, 2, 5, CLEAR. In addition, in a less desirable alternative embodiment, the LEDs could be deleted in their entirety, or there could be a less than one to one correlation between a key and an LED (for example, there might only be one LED, its only purpose being to confirm activation of any key).

This embodiment does not require any special function keys other than what may exist on keypad 9. By selection of a preprogrammed code into card 1, in the same manner as was just explained, the preprogrammed code can serve the same function as a special function key. For example, such a code might be used to select different uses for the card, such as accessing different accounts. It might also be used to send a special command to the computer to store specified data in a preselected portion of the magnetic storage medium.

Although this preferred embodiment does not require any special function keys other than what exist on keypad 9, it does not preclude their use. If optional special feature keys 113 are included in card 1, they could also trigger or be part of any sequence used to deactivate or reactivate the LEDs or any other function or operation that could be triggered by a special function key. For example, they could be used as a trigger, or be part of a triggering sequence or code, for changing a user identifier stored in the magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader.

It is also contemplated that this alternate preferred embodiment may require correct entry of a PIN before the card will function, or that a PIN be verified before it is used to generate a user one-time number through use of a card number generator. In either scenario, it is useful for the user to be able to determine whether the PIN has been correctly entered into the card. In either scenario, when the user is ready to enter a PIN into electronic card 1, the user presses the ENTER button. If the correct PIN for the card has been entered, the READY light 111 will light, but if the PIN is incorrect, the ERROR light 112 will light. The CLEAR key clears all entries of earlier information into keypad 9 and allows the user to begin reentering a PIN. If desired, the READY and ERROR

lights can be deactivated or reactivated in the same manner as described for the LEDs.

The versatility of this embodiment will now be illustrated by a theoretical example of how an electronic card in accordance with this embodiment could be used in a number of different situations.

First, assume that the user of the card wants to use the card for a company business expense. In this scenario, the user could select a company credit card, issued in the name of the company, by turning the card on, touching a special function button 113 followed by numeric key 1, then the ENTER key. This could tell the card to use an algorithm for a company account stored in the card's computer. Next, the user would enter the user's PIN for that company account. The card's computer would then generate a payment card number and temporarily store that number, and a user identifier representing the company name, in track 2 of the card's magnetic stripe, which could then be read by a magnetic stripe reader and sent to a verification agency for validation.

Second, assume that the user wants to use the card to charge a personal expense. In this scenario, the user could select a personal credit card by turning the card on, touching a special function button 113 followed by numeric key 2, then the ENTER key. This could tell the card to use an algorithm for a user credit card stored in the card's computer. Next, the user would enter the user's personal PIN. The card's computer would then generate a payment card number and temporarily store that number, and a user identifier representing the user's name (which would be different from the user identifier used in the first scenario), in track 2 of the card's magnetic stripe which could then be read by a magnetic stripe reader and sent to a verification agency for validation. The payment card number generated in this scenario would be different from the payment card number generated in the first scenario in two respects. First, the bank identification number would be different. This is a fixed variable portion of the payment card number (since many different cards for the same bank could have this number). Second, the account number would be different. This is a variable variable portion of the payment card number that changes each time the card is used (this is the same as the individual account portion of traditional credit card numbers).

Third, assume that the user wants to use the card to charge a personal expense, except the user wants to make a note that the expense is tax deductible. This scenario would proceed the same as the second scenario, except that a second personal PIN would be entered. In this example, the fixed variable portion of the payment card number would be the same as in the second scenario, but the variable variable portion would be different.

Fourth, assume that the user now wants to use the card to enter a parking garage controlled by an access card, and the requisite code has been stored in the card's memory. In this scenario, the user could access the requisite code by turning the card on, touching a special function button 113 followed by numeric keys 98, then the ENTER key. This could tell the card to temporarily store the requisite code in the card's magnetic stripe, which could then be read by a magnetic stripe reader.

Fifth, assume that the user now wants to use the card to enter the building of the parking garage, and this requires a PIN plus the requisite code of the fourth scenario. This would proceed the same as the fourth scenario, except that the user would enter the PIN into the card and it would be added to the magnetic stripe with the requisite code.

As should be apparent from these limited examples, there are many ways that an electronic card according to the present invention can be used.

3. A method for transferring a data packet from a user of an electronic card to a money source as part of a payment card transaction

The electronic cards of the preferred embodiments can be used to allow a standard magnetic stripe reader to read a data packet that is submitted to a money source for approval of a given payment card transaction associated with the data packet.

When such a data packet is read and transmitted to a money source, additional information can be conveyed within the data packet, as long as it can be conveniently read by the money source. This is why it is especially preferred that the data packet be encoded in the second track of the magnetic stripe within the field of data that can be read in a normal credit card transaction. Combination of this capacity for transmission of data with the flexibility provided by use of the

encoding technology opens a communication channel for data transmission that can be exploited every time such a transaction takes place.

One way to exploit the communication channel is to use it to directly convey information from the electronic card to the money source. This can be useful in synchronizing the electronic card with the money source. For example, it can be used to provide the money source with a current sequence number of the electronic card used in generating a one-time unique purchase order number. (The sequence number can be used in connection with an algorithm that is executed that uses the selected user key and a customer sequence number to generate the Coupon. The sequence number is changed after each Coupon is generated and a new Coupon can then be generated using the changed sequence number and a selected user key for the new Coupon.) It can also be useful in providing the money source with results of diagnostic test programs that are periodically run by the electronic card's computer, an important example of which is remaining battery capacity

Because of the limited capacity of current batteries that are useful in the type of electronic card described herein, it is possible that the battery will cease working before an expiration date of the card if the electronic card is heavily used. To solve this problem, the computer can run a program that measures remaining battery capacity or checks for a battery life parameter and generates a warning signal when a low battery condition is detected. The computer could even run a predictive program estimating when the useful battery capacity will expire based upon past usage, and this program could generate a battery life signal related to an estimated remaining battery life of the battery, which could be sent to the money source. The money source, in turn, can use such diagnostic information to send out a new electronic card to the user before the electronic card runs out of battery life. The same type of communication system can be used for other diagnostic programs that measure at least one parameter and generate a warning signal when a preselected threshold is exceeded.

Another way to exploit the communication channel is to use it to directly convey information that is generated by a user of the card to the money source. For example, the user could include a customization variable in the data packet.

4. A method for customizing use of an electronic card through a customization variable

Like a traditional payment card number, a one-time payment card number should be capable of being read by a standard magnetic stripe reader when it is part of a physical card used in traditional face-to-face transactions in which a user presents the physical card to a merchant for payment. However, like traditional payment card numbers, a one-time payment card number should also be capable of being used in a Mail Order Telephone Order ("MOTO") credit card transaction between the user and a merchant. Thus, like a traditional payment card number, the one-time payment card number should fit within, and work with, present platforms and protocols for financial transactions involving payment cards, such as traditional credit cards. This versatility allows the one-time payment card number to be used with electronic cards, software programs used in network applications, or telephones (especially telephones used in what is now being referred to as m-commerce, or mobile commerce).

A traditional payment card number can be characterized as having three parts. First, there is a set of fixed variables. This contains numerals that represent certain specified data fields, such as a bank identifier and a month and year expiration date for a given payment card. (The "bank" may be any "money source" as that term has been defined in U.S. Patent No. 5,937,394.) Second, there is a set of variable variables. This contains numerals that will vary for different payment cards issued by the same money source. In other words, this is the portion of the card number that will be specific to an individual entity or account for a given issuing money source. Third, there is a check sum digit. The value of the check sum digit is dictated by the other numerals in the card number.

In the context of the present invention, a user one-time payment card number is akin to a traditional payment card number, with certain exceptions. In a traditional payment card number, there might be a set of six fixed variables, followed by a set of nine variable variables, followed by a check sum digit and another set of four fixed variables representing the month and year. When a user uses this traditional payment card number to complete a given financial transaction, the transaction is always completed by using the same twenty digits for the payment card number. By contrast, if the user uses a one-time payment

card number to complete any such given financial transaction, the transaction will not be completed by always using the same twenty digits for the payment card number. Instead, the twenty digits of the one-time payment card number will vary, and the degree to which they vary may depend upon user selection of a customization parameter. In addition, because the one-time payment card number varies with successive usage, the check sum digit will not necessarily be the same with successive usage, although it may be. Thus, the check sum digit must be recalculated for each new one-time payment card number, and this is why it shall be referred to as a "check sum variable" in the context of a one-time payment card number according to the present invention.

Another difference between a traditional payment card number and a one-time payment card number is the way that a given transaction using either number is validated by a verification agency, which may be a money source or an entity who processes payment card transactions. When a transaction involving a one-time payment card number is processed, the verification agency must verify that the one-time payment card number is valid for the user identifier for the particular given transaction, as opposed to any given transaction involving the user identifier. (The verification process must take into account how selection of the customization parameter may affect what the verification agency will receive for verification.) This difference is a reason why use of the one-time payment card number provides greater security and anonymity than can be obtained through use of a traditional payment card.

A card number generator generates a one-time payment card number. No matter what method is used to generate a one-time payment card number, two successive one-time payment card numbers should be different. This can be accomplished by using a sequence number that is changed after each one-time payment card number is generated. (The present invention does not require that all theoretical possibilities will result in different one-time payment card numbers. Instead, it is preferred that there be a low probability of occurrence of identical one-time payment card numbers attributable to convergence of two different inputs leading to the same result due to operations performed on the inputs by the algorithm.)

A user can customize use of an electronic card having a card number that varies with each use by selecting at least one customization parameter to customize a given use of the electronic card. There are three general customization parameters that can be used to customize a given use.

First, the user can customize generation of the one-time card number. This can be done many different ways. An example of one way in which it can be done is to customize selection of a selected user key that is used to generate the one-time card number. Another way in which it can be done is to include a customization variable in the one-time card number, or as an input into the algorithm used to generate the one-time card number.

Second, the user can customize the user identifier that is used to validate the one-time card number. This can be done many different ways. One way is to choose one of two or more preselected identifiers as a selected user identifier. Another way is to modify the user identifier. Still another way is to add a customization variable, such as a numeric character, to the user identifier at a preselected location.

Third, the user can include a customization variable with information transmitted to a verification agency for validation of the given use. Unlike the first two customization parameters, this parameter relies upon use of an additional field of data collected as part of the validation process for a given transaction, and this may require a change in established validation protocols. It is especially preferred that any such change be technically feasible within the confines of hardware that is being used to process traditional payment card transactions. In the context of an electronic card with a magnetic stripe, this means that it is preferred that the additional customization variable be stored in the magnetic stripe, and it is especially preferred that it be stored in the second track of the magnetic stripe.

Once it is recognized that using one or more of the foregoing customization parameters will customize a given transaction involving use of a one-time payment card number, and that such customization will seamlessly allow a user to transmit additional information to the money source processing such transaction, without loss of desired security or anonymity, the options for using such customization are virtually limitless.

After a one-time payment card number is validated for a given transaction, the money source can determine what customization parameter(s) was selected by the user for the given transaction, which allows the money source to determine what handling option should be used for the transaction involving the one-time payment card number. (It also allows the money source to determine what sequence number is associated with the one-time payment card number, so that its records can be synchronized as part of the validation process.)

One use of multiple handling options is to allow the money source to access multiple accounts. For example, a user might use one account as a credit card, and another account as a debit or checking card. By choosing which account should be used for a given transaction, the user could determine, at the point of use, whether to charge the transaction, or have it deducted from an existing account balance. The same idea could be used for multiple credit cards, whether they are from the same issuer or different issuers, or even different cards, such as Visa®, MasterCard®, Diner's Card®, Discover® or American Express®. In addition, the user might elect to have separate billing statements for separate accounts, or have all billing consolidated in a single statement.

Another use of multiple handling options is to allow identification of the person completing a transaction, or to allow multiple persons access to a single account, or place different restrictions on multiple persons on a single account. For example, a single account might be opened with an issuing bank, but an entire family might be authorized to use the account. Thus, a father and a mother might have their own customization parameter, a teenage child might have another customization parameter and a lower authorized spending limit, and a preteen child might have a fourth customization parameter, but only be authorized to engage in a certain limited number of transactions per time period with a maximum spending limit for each transaction. All the members of this family could use the same card number generator embedded within a PDA or mobile phone, or on a computer or in an electronic card. At the end of a specified billing cycle, all transactions completed by any member of this family could be consolidated in a single bill, and that bill could indicate who spent what when during the billing cycle, and what it was spent on.

Still another use of multiple handling options is to allow a user to classify the nature of a particular transaction at the time it is completed. For example, suppose an individual uses a single credit card for personal expenditures and business expenditures. By assigning one customization parameter to personal transactions, and a second customization parameter to business transactions, the user can simplify accounting for such transactions without the necessity of having and carrying two separate cards. If desired, the user could even receive two separate statements for such expenditures so that the personal expenditures would not be discernable from the documentation associated with the business expenditures. Individual transactions could also be classified according to a preselected set of criteria, and such criteria could be used in various financial programs. For example, a user might include a code classification system used in a money management system to create various reports that itemize categories of spending or assist in budgeting of finances.

Yet another use of multiple handling options is to allow a user to preselect how a particular transaction is treated in a subsequent bill. For example, an individual user might not want a billing statement to include information about the identity of second entities who provide certain goods or services, or when transactions with such entities take place, but still want to have the billing statement include such information for other transactions. By selecting two different customization parameters with these two different handling options, the user has the option of controlling what information it receives in billing statements about individual transactions.

Multiple handling options can also be used to guard privacy, or for commercial purposes that do not presently exist. For example, the user and the money source might enter into an agreement about how, and under what circumstances, the money source can distribute information about transactions of the user, depending upon which customization parameter is used in a given transaction. The agreement might provide different levels of confidentiality, and set up different levels or types of compensation tied to transactions falling within the different levels for a given time period.

One level of confidentiality might restrict distribution of any information concerning a transaction by the money source to any third party. For example, a

user might want strict confidentiality of any transaction involving medical services, and would not want the money source to divulge that information to any party unless legally required to do so. Or, maybe the user does not want any third party to learn of any transaction that exceeds a certain dollar amount, for fear of a potential deluge of unsolicited advertising. A user might pay a monthly fee for use of this option, a transaction based fee, or no fee at all.

A second level of confidentiality might permit distribution of any information concerning a transaction by the money source to any third party. Such information is potentially valuable for purposes of advertising, and creating profiles for targeted marketing, and the money source might even pay the user for the right to sell such information.

Other levels of confidentiality might fall between those already noted. For example, a third level might permit distribution of certain information concerning a transaction (such as the payee, the amount of purchase, the date of purchase, and a profile of the user), but restrict distribution of other information concerning a transaction (such as the identity of the user). Another level of confidentiality might restrict distribution of information concerning a transaction to any third party, but allow the money source to use such information for its own marketing efforts directed to the user.

5. Anonymous delivery system

By using a customization parameter, use of a one-time payment card number can be customized for a desired delivery method, as will now be explained.

When a user purchases certain goods or services, the delivery or availability of such goods or services can be immediate and made at the time and point of purchase, and therefore can be anonymous. Examples of this include use of a payment card in a face-to-face transaction at a check out counter or use of a payment card to obtain immediate access to something, such as a service, information or a software program, that is delivered telephonically or over a computer network. In such situations, the user may not be required to provide the merchant with a user address. However, even if an address is required, it need not be used for delivery, so it need not be an actual address of the user or an

address for delivery of goods. Accordingly, in such situations, the user might want to provide a meaningless address to avoid undesired solicitation and junk mail, or an address of somebody who screens anything received at the address. Such an address could be a Proxy Agent.

When a user purchases goods that have to be delivered, the user is traditionally faced with a dilemma. Before the goods can be delivered, the user has to provide an address for delivery. If a home address is used, so the goods can be conveniently delivered to the home, anonymity is sacrificed. Once a merchant or marketer has a home address, the address is available for solicitation and, unfortunately for many consumers, junk mail. In addition, once a merchant or marketeer has a home address, it can be cross-referenced against available data bases, which can often reveal the true identity of the user, even if the transaction was otherwise conducted anonymously through use of a one-time payment card number and a fictitious user name. Once a true identity is obtained, that identity can be matched with the purchase, and this information can be used for all sorts of marketing purposes, including telemarketing. As is readily apparent, use of a real home address, even with an otherwise anonymous payment transaction, can lead to significant loss of a user's privacy and unwanted intrusions upon such privacy by a variety of marketing methods and practices.

To avoid such loss of privacy, a user might request that the goods be delivered to an address other than the user's home address, such as a work address or an address used for delivery of mail, such as a post office box. However, this option eliminates the convenience of a home delivery, and creates additional inconvenience. It is also not an option if the user making the purchase wants the goods sent to a third party, such as a relative, for a birthday or a holiday gift. This problem is aggravated when the desired delivery date is crucial and there is not sufficient time for delivery to a secondary address, and then a second delivery to the intended recipient. (In addition, this would involve extra cost and inconvenience associated with receiving the shipment at the secondary address, and then resending the package to the desired recipient.)

Even when a user is willing and able to put up with the inconvenience of delivery to a secondary address, there may be additional drawbacks with such a delivery.

The user may not want some goods delivered to the user's work address for a variety of reasons, including a resultant loss of privacy associated with such delivery. Not only may the user want to prevent colleagues from knowing what the user has purchased, but delivery to a work address may lead to junk mail being sent to the work address, or correlating the work address, in one fashion or another, to the true identity of the user. For example, assume that the user uses a fictitious name and a work address. The delivery agent may require proof that the user is entitled to receive the goods, and this proof could compromise the user's true identity. Alternatively, the user might not be able to claim goods delivered to the user's work address, or such goods, even if they have been delivered to the work address, may not reach the user due, for example, to theft by another employee.

Although delivery to an address designated for pick-up may avoid some of the problems associated with delivery to a work address, it has other drawbacks. For example, it requires that the user have an account with the delivery address, and pay for this service. In addition, it does not prevent the address from being used for junk mail. And, unless the user is careful with use of the address, and the service guarantees anonymity, it might still be possible for marketeers to use a database to cross-reference the delivery address to develop the true identity or address of the user.

To avoid the foregoing problems, the preferred embodiment of the present invention allows a user to select an anonymous delivery option when a one-time card number is used with a user identifier to complete a given commercial transaction. The mechanics of the anonymous delivery option can be triggered by use of a customization parameter associated with the anonymous delivery option. By selection of an appropriate customization parameter, a user can select from a variety of different, anonymous delivery options. For example, one option might be home delivery. Another option might be a pick-up by the user at a specified address. Another option might be a handling option by which the user selects a preselected delivery address. Still another option might be an alternative handling option by which the user provides a specified one-time delivery address for the specific transaction, and this might be provided before or after the actual transaction is completed with a merchant.

Once the anonymous delivery option is triggered, it can be implemented as follows.

When the commercial transaction is completed, whether it is a face-to-face transaction or a MOTO transaction, the user will provide the merchant with a one-time payment card number and a user identifier. As already noted, the user can customize the one-time payment card number so as to select the desired delivery method and address. Or, alternatively, the merchant could specify who the delivery agent will be, such as Federal Express® or UPS®, and the user could still specify a delivery option for such a carrier by selection of an appropriate customization variable. Once the merchant receives this information, it is sent to a money source to confirm the validity of the transaction. The communication from the merchant to the money source will also include an identification of the merchant and the amount of the transaction, and will also typically include the date of the transaction. When the money source confirms the validity of the transaction, the money source will send the merchant a confirmation number that can be used to identify the transaction. In other words, so far, this transaction proceeds in the same fashion as an ordinary credit card transaction, except that the merchant does not yet have a delivery address for the goods.

The delivery address can be provided to the delivery agent in a number of ways without allowing the merchant to learn the delivery address.

One way the delivery address can be kept from the merchant is for the money source to provide the delivery address to the delivery agent along with a tracking identifier. The money source can also give the tracking identifier to the merchant, so that it can serve as an identifier for the shipping process. The tracking identifier might simply be the confirmation number that the money source gave the merchant to confirm validation of the commercial transaction, or it might be another number specifically designated for this purpose. Once the merchant has the tracking identifier, the goods can be delivered to the delivery agent with the tracking identifier taking the place of a delivery address.

After the delivery agent receives the goods, the tracking identifier can be used to access the delivery address. Now the delivery agent to the delivery address can deliver the goods, and the delivery agent need not have any information about the addressee. To confirm delivery, and to verify that delivery

has been made to the right party, the delivery agent can be given a delivery code. This might be information about the commercial transaction, such as a merchant invoice number or the one-time payment card number used to complete the transaction, but it is preferably a separate code that the merchant, and the merchant's employees, would not have access to. The delivery code can be generated by the delivery agent or the money source, or even the user, as long as it is known by the delivery agent and the person who will pick up the goods, who will be designated the "addressee" (the addressee may be the user or a third party). By using the money source or another source as an intermediary, there need not be any direct contact between the delivery agent and the addressee until the time of delivery.

Another way the delivery address can be kept from the merchant is to use two delivery agents, or to deliver the goods to a destination address where the purchased item is held at a pick-up location for pick-up by the addressee. For example, the goods could be delivered to a local office of the delivery agent. In both of these cases, the first delivery agent will not have an address of the addressee, and the merchant could not get such an address from the first delivery agent. A variant on this method of delivery is to segregate knowledge of the delivery address within the delivery agent. For example, the delivery agent might use an internal delivery address for the first point of delivery. This might be a central location where a number of packages from a given collection zone are collected for sorting and subsequent distribution. Once the goods reach this central address, they could be processed according to special procedures to limit access to the correlation between the tracking identifier and the delivery address.

If the goods are not to be shipped by use of a delivery agent, but held for pick-up by the user or an authorized agent of the user, the delivery process can be modified in a number of ways to safeguard anonymity, while still providing security against fraud. For example, the money source can send a delivery code to the user and the merchant that the user must have at the time of pick-up. The user can also be required to provide an additional verification of identity, albeit anonymous to the merchant, at the time of pick-up. One way to do this is to require the user to provide a valid one-time payment card number at the time of pick-up, and it is especially preferred that this number be a dummy number that is

designated as such by using a customization variable designated as a dummy variable. When the dummy one-time payment card number is submitted for verification, the dummy variable tells the money source that this is not a commercial transaction, but rather, a request for verification of valid identity, and that it should be treated as such. Thus, the money source can use the dummy one-time payment card number to confirm that the person picking up the goods is authorized to pick them up, and then send a confirmation of the transaction to the merchant to verify that the party presenting the dummy one-time payment card number should be allowed to pick-up the goods. This confirmation also creates a record of receipt of the goods by the user. And, of course, all of these same methods could also be applied, if desired, to the situation of a delivery by the delivery agent to a delivery address.

In an alternative embodiment, the methods for anonymous delivery can be used to implement an anonymous "charge on delivery" that is somewhat akin to the concept of cash on delivery. In this embodiment, the money source can put a hold on charging or debiting the user's account (and, if desired, paying the merchant), until there has been an actual delivery of the goods. One way to establish such delivery is through use of a "dummy" one-time payment card number.

As described above, at least four parties are involved in completing an anonymous delivery of goods when the user does not pick up the goods from the merchant. In an alternative embodiment of the present invention, a fifth party is deliberately placed into the loop as an intermediary to act as a further safeguard against loss of anonymity. The fifth party, which shall be referred to as "Privacy Systems," can function as a further buffer and safeguard of the user's privacy. Using Privacy Systems as a payor to the merchant, a payee to the money source and the clearinghouse for all of the details of a given transaction, including the delivery address, does this. By adding this fifth party, who might be legally obligated not to divulge preselected details of a given transaction to third parties without consent of the user, the money source is taken out of the loop as a coordinating party with knowledge of all of the transaction details. Privacy Systems can also function as a clearinghouse for collecting, categorizing,

marketing and selling information about transactions in which it is serving as an intermediary.

Although the foregoing detailed description is illustrative of preferred embodiments of the present invention, it is to be understood that additional embodiments thereof will be obvious to those skilled in the art.

Accordingly, it will be readily apparent to those skilled in the art that still further changes and modifications in the actual concepts described herein can readily be made without departing from the spirit and scope of the disclosed inventions as defined by the following claims.

What is claimed is:

1. A method for transferring a data packet from a user of an electronic card to a money source as part of a payment card transaction, comprising the steps of:

executing a program on a computer of the electronic card to generate a data packet that can be read by a standard magnetic stripe reader;

using the standard magnetic stripe reader to read a payment card number, a user identifier and the data packet as part of a given payment card transaction; and

submitting the payment card number, the user identifier and the data packet to the money source for approval of the given payment card transaction.

2. A method as recited in claim 1, wherein the program is a diagnostic program that measures at least one parameter and generates a warning signal when a preselected threshold is exceeded.

3. A method as recited in claim 2, wherein the program checks for a battery life parameter and generates a warning signal when a low battery condition is detected.

4. A method as recited in claim 1, comprising the further steps of:

generating a user one-time payment card number through use of a card number generator; and

using the user one-time payment card number as the payment card number.

5. A method as recited in claim 4, wherein the one-time payment card number is correlated with a sequence number that indicates the relationship of the one-time payment card number to a sequence of one-time payment card numbers generated by the card number generator.

6. A method as recited in claim 5, wherein the data packet can be used to obtain the user sequence number.

7. A method for alerting a money source to a low battery condition of a battery used in an electronic card, comprising the steps of:

(1) using the electronic card to conduct a plurality of payment card transactions in which a payment card number and a user identifier are submitted to the money source as part of an approval process;

(2) executing a program on a computer of the electronic card to check for a battery life parameter and generate a warning signal when a low battery condition is detected; and

(3) when a warning signal is generated, submitting a low battery indicator to the money source in connection with the approval process.

8. A method as recited in claim 7, wherein the program is executed each time the electronic card seeks approval of a preselected number of payment card transactions.

9. A method as recited in claim 8, wherein the program generates a battery life signal related to an estimated remaining battery life of the battery.

10. A method as recited in claim 9, comprising the further step of:

(4) submitting a battery life indicator that is based upon the battery life signal to the money source in connection with the approval process.

11. A method as recited in recited in claim 10, comprising the further step of:

(4) providing a user of the electronic card with a replacement electronic card before the battery life parameter drops below a selected threshold.

12. A method for allowing customized use of an electronic card having a card number that varies with each use, comprising the steps of:

(1) allowing a user to select a customization parameter to customize a given use of the electronic card by at least one of the following steps:

(a) customizing generation of a one-time card number;

(b) customizing a user identifier; or

(c) inclusion of a customization variable with information transmitted to a verification agency for validation of the given use;

(2) generating a user one-time payment card number through use of a card number generator;

(3) submitting the user one-time payment card number and the user identifier to a verification agency for validation, and, if the user has selected step (1)(c), including the customization variable with the submission for the given use; and

(4) verifying that the one-time payment card number is valid for the given use.

13. A method as recited in claim 12, wherein the electronic card is a payment card and the one-time card number is a one-time payment card number.

14. A method as recited in claim 13, wherein the card number generator generates a new card number by executing an algorithm that uses a selected user key to generate the new card number.

15. A method as recited in claim 13, wherein the user can customize generation of the one-time card number by choosing either a first user key or a second user key as the selected user key, and wherein the algorithm will generate a first one-time card number if the selected user key is the first user key or a second one-time card number if the selected user key is the second user key, the first and the second one-time card numbers being different, but both valid with the user identifier.

16. A method as recited in claim 12, wherein the electronic card is comprised of:

a card base;

a computer affixed to the card;

an input mechanism;

a magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader;

an encoder for generating a data packet that is stored in a designated portion of the magnetic storage medium and is readable by a standard magnetic stripe reader; and

a power source for supplying power to the computer and the encoder;

wherein the electronic card is sized such that the magnetic storage medium can be read by the standard magnetic stripe reader.

17. A method as recited in claim 16, wherein the data packet is further comprised of the customization variable.

18. A method for processing a plurality of payment card transactions based upon a user's selection of a customization variable for each of the transactions, comprising the steps of:

(1) establishing a plurality of handling options between a money source and the user;

(2) providing the user with a card number generator;

(3) allowing the user to complete a plurality of payment card transactions within a time period in accordance with the following steps:

(a) allowing the user to select a customization parameter to customize a given use of the card number generator by at least one of the following steps:

(i) customizing generation of a one-time payment card number;

(ii) customizing a user identifier; or

(iii) inclusion of a customization variable with information transmitted to a verification agency for validation of the given use;

(b) generating a user one-time payment card number through use of the card number generator;

(c) verifying the validity of the given use by submitting the user one-time payment card number and the user identifier to a verification agency for validation, and, if the user has selected step (3)(a)(iii), including the customization variable with the submission; and

(d) repeating steps (a) through (c) at least once within the time period; and

(4) processing each of the plurality of payment card transactions in accordance with one of the plurality of handling options based upon the customization parameter selected for each of the plurality of payment card transactions.

19. A method as recited in claim 18, wherein the card number generator is included within an electronic payment card.

20. A method as recited in claim 19, wherein the electronic payment card is comprised of:

a card base;

a computer affixed to the card;

a keypad for providing input to the computer, the keypad having ten numeric keys and at least one special function key that are touch-activated;

a magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader;

an encoder controlled by the computer for generating a data packet that is stored in a designated portion of the magnetic storage medium; and

a power source for supplying power to the computer and the encoder;

wherein the electronic card is sized such that the magnetic storage medium can be read by a standard magnetic stripe reader.

21. A method as recited in claim 18, wherein the first and the second handling options are mechanisms to bill two separate accounts.

22. A method as recited in claim 19, wherein the user is sent a single bill for charges to the two separate accounts.

23. A method as recited in claim 22, wherein the user is sent a first bill for the first account and a separate bill for the second account.

24. A method as recited in claim 18, wherein the first and the second handling options are a first and a second mechanism for dealing with distribution of information concerning the plurality of payment card transactions.

25. A method as recited in claim 24, wherein the first mechanism restricts the distribution from the money source to a third party of information relating to any payment card transaction in which the user payment card number was generated by use of the first user key.

26. A method as recited in claim 24, wherein the first mechanism restricts the distribution from the money source to the second entity of personal information of the user relating to any payment card transaction in which the user payment card number was generated by use of the first user key.

27. A method as recited in claim 25, wherein the user provides the money source with consideration for use of the first mechanism.

28. A method as recited in claim 24, wherein the second mechanism permits the distribution from the money source to a third party of information relating to any payment card transaction in which the user payment card number was generated by use of the second user key.

29. A method as recited in claim 28, wherein the second mechanism permits the distribution from the money source to the second entity of personal information of the user relating to any payment card transaction in which the user payment card number was generated by use of the second user key.

30. A method as recited in claim 28, wherein the money source provides the user with consideration for use of the second mechanism.

31. A method as recited in claim 18, wherein the first and the second handling options provide a mechanism for classifying the nature of the plurality of payment card transactions.

32. A method as recited in claim 31, wherein the first handling option is used for business transactions and the second handling option is used for personal transactions.

33. A method as recited in claim 18, wherein the first and the second handling options provide a mechanism for identifying either a first user or a second user as the user.

34. A method as recited in claim 33, wherein approval of a payment card transaction for the first user is subject to different restrictions than approval of a payment card transaction for the second user.

35. A method as recited in claim 18, wherein the first and the second handling options provide a mechanism for controlling what information is reported about the plurality of payment card transactions in a billing statement.

36. An electronic card, comprising:

a card base;

a computer affixed to the card;

a display mechanism controlled by the computer;

an input mechanism;

a magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader;

an encoder for generating a data packet that is stored in a designated portion of the magnetic storage medium; and

a power source for supplying power to the computer and the encoder;

wherein the electronic card is sized such that the magnetic storage medium can be read by a standard magnetic stripe reader.

37. An electronic card as recited in claim 36, wherein the magnetic storage medium is a magnetic stripe.

38. A method for providing a secure and anonymous transaction between a user and a merchant with subsequent delivery of a purchased item, comprising the steps of:

(1) establishing a user account between a money source and the user which is associated with a fictitious user identifier, a user account number, and a user settlement mechanism through which the user and the money source can settle payment card transactions involving the user account;

(2) providing the user with a card number generator;

(3) completing a payment card transaction between the user and the merchant in which the user account is charged a monetary value for the purchased item, comprising the following steps:

(a) allowing the user to select a customization parameter associated with an anonymous delivery option for subsequent delivery of the purchased item to customize the payment card transaction by at least one of the following steps:

(i) customizing generation of a user one-time payment card number;

(ii) customizing the user identifier; or

(iii) inclusion of a customization variable in a user transaction data packet that includes the user one-time payment card number and the user identifier;

(b) generating the user one-time payment card number through use of the card number generator; and

(c) providing the merchant with the user transaction data packet;

(4) submitting a merchant transaction data packet to the money source, wherein the merchant transaction data packet includes the user transaction data packet, the monetary value, a merchant identifier and a purchased item identifier;

(5) providing the merchant with a confirmation that the transaction is valid after the money source verifies that the user one-time payment card number is valid for the user identifier and the transaction;

(6) sending a tracking identifier from the money source to the merchant;

(7) sending the tracking identifier and a delivery address from the money source to a delivery agent;

(8) invoking the settlement mechanism to charge or debit the user account for a transaction amount correlated to the monetary value;

(9) delivering the purchased item to the delivery agent with the tracking identifier; and

(10) delivering the purchased item from the delivery agent to the delivery address.

39. A method as recited in claim 38, wherein the merchant is not provided with the delivery address.

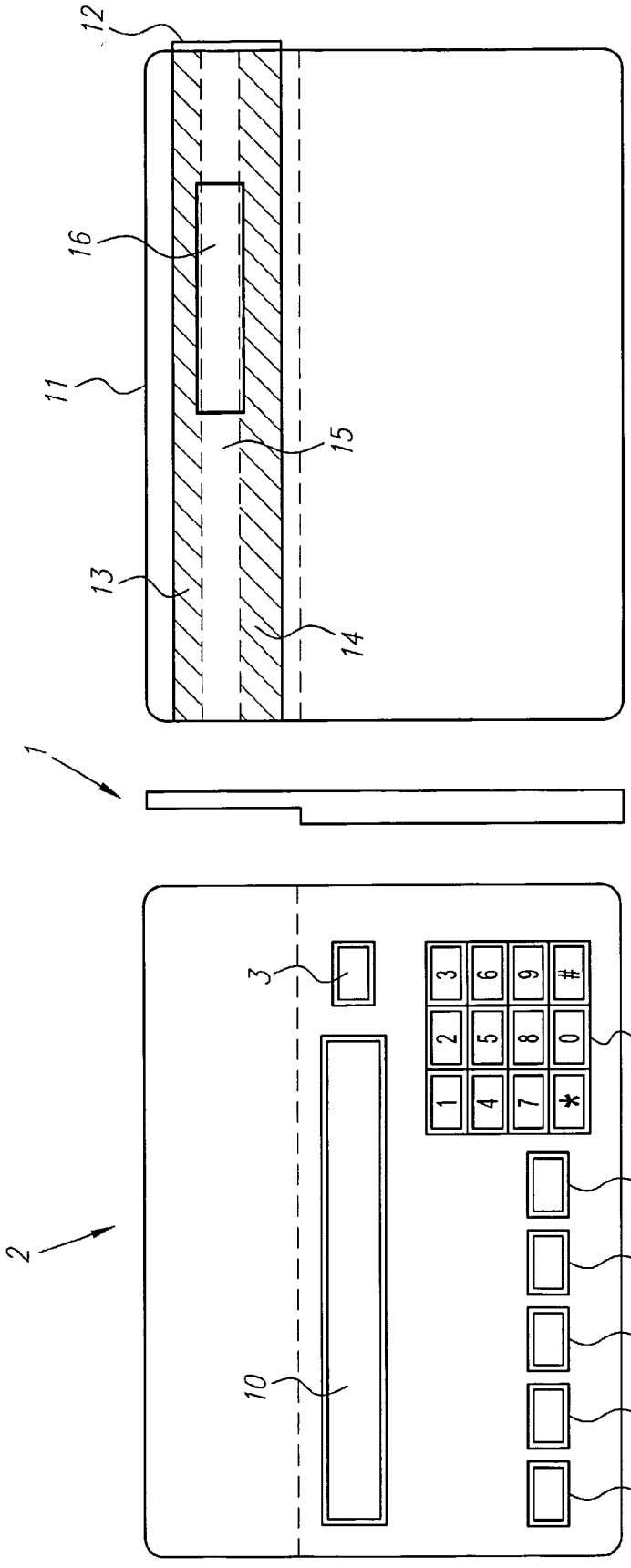


FIG. 1C

FIG. 1B

FIG. 1A

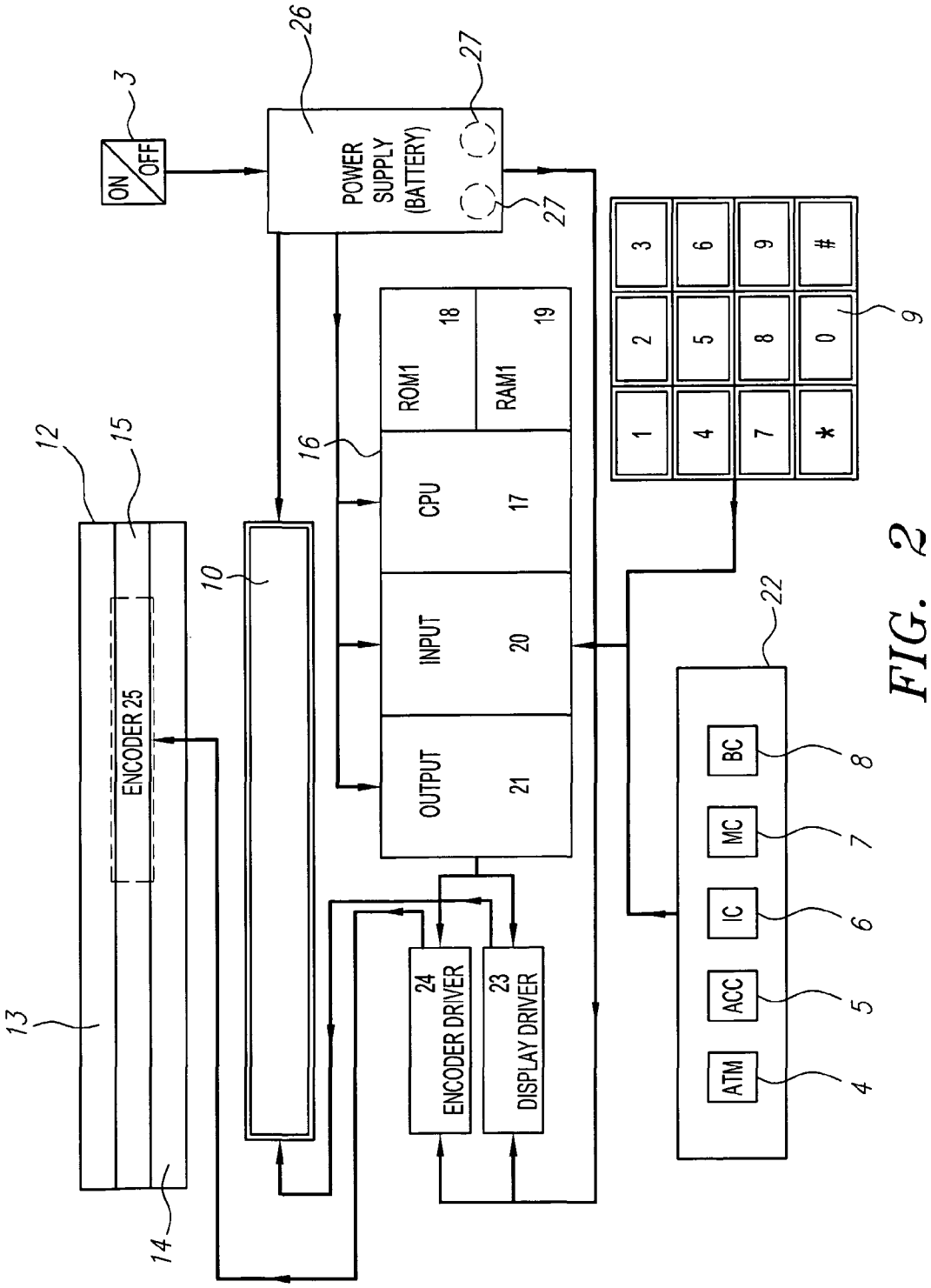

3
ON
OFF
26
POWER SUPPLY (BATTERY)
27
27
ROM1
18
RAM1
19
CPU
17
INPUT
20
OUTPUT
21
16
12
15
10
ENCODER 25
13
14
24
ENCODER DRIVER
23
DISPLAY DRIVER
22
BC
8
MC
7
IC
6
ACC
5
ATM
4
1
2
3
4
5
6
7
8
9
*
0
#
9

FIG. 2

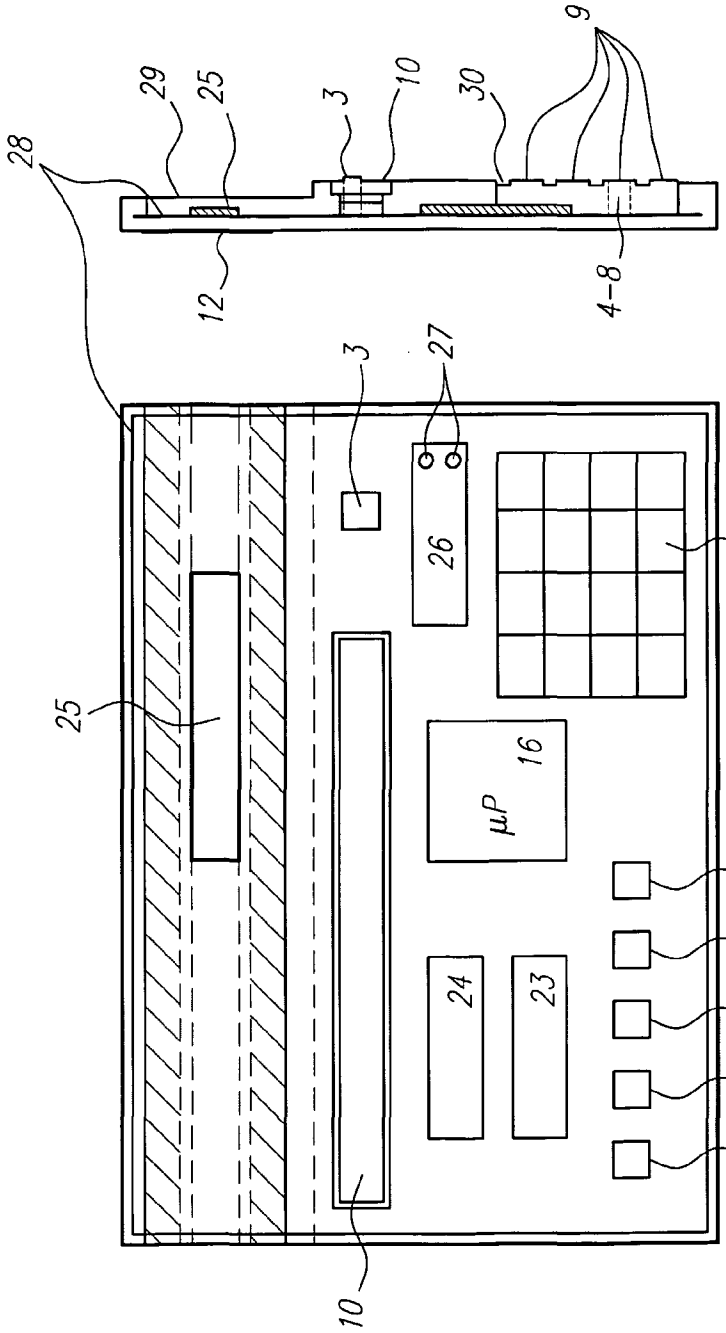


FIG. 3B

FIG. 3A

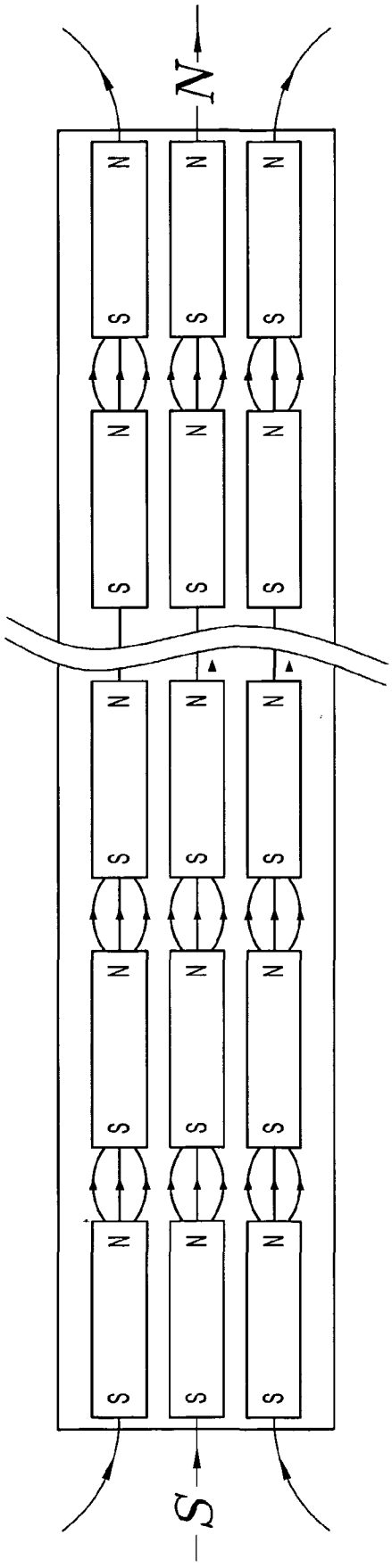


FIG. 4

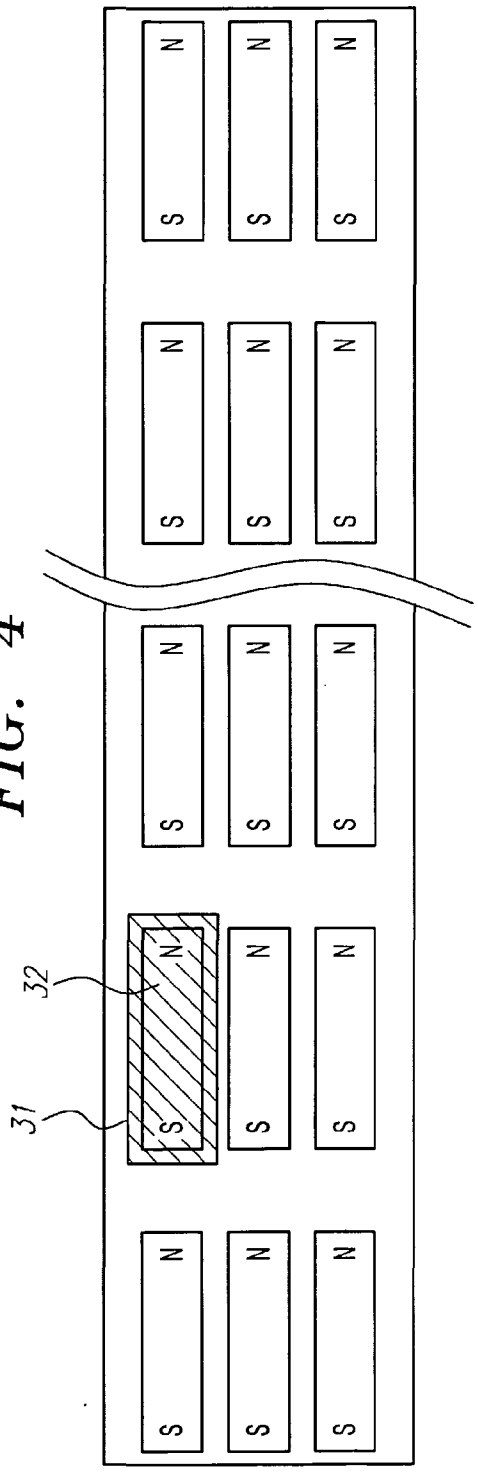


FIG. 5

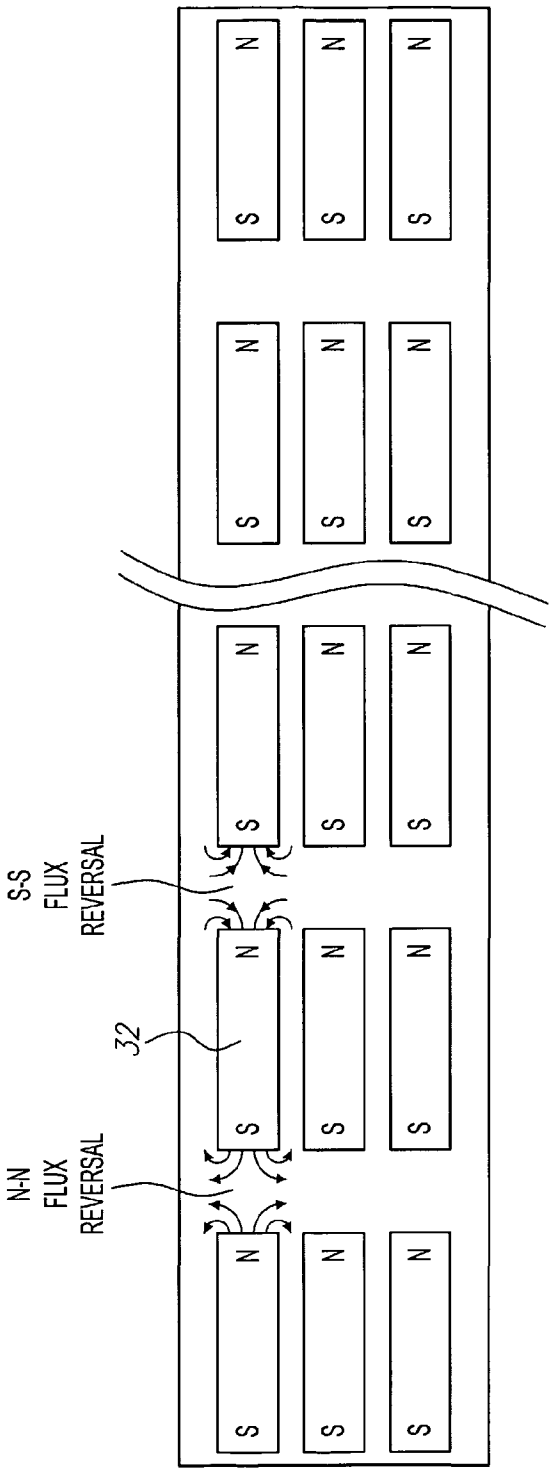


FIG. 6

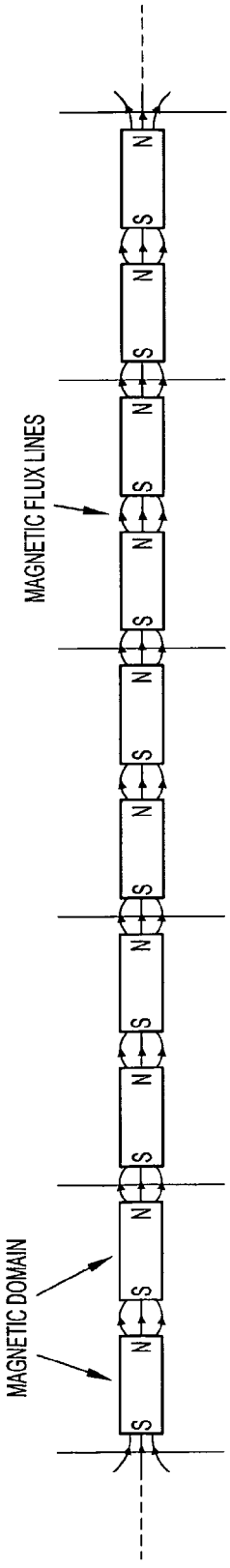


FIG. 7A

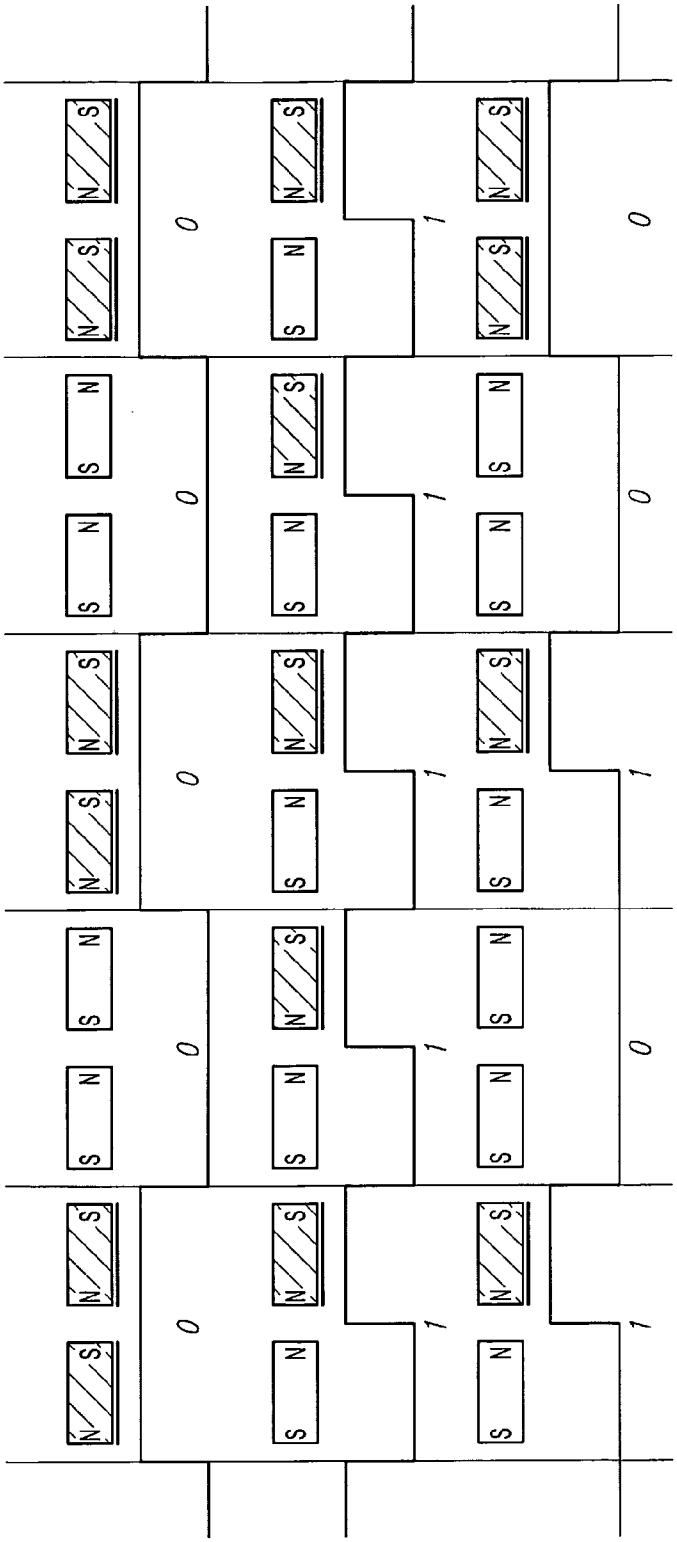


FIG. 7B

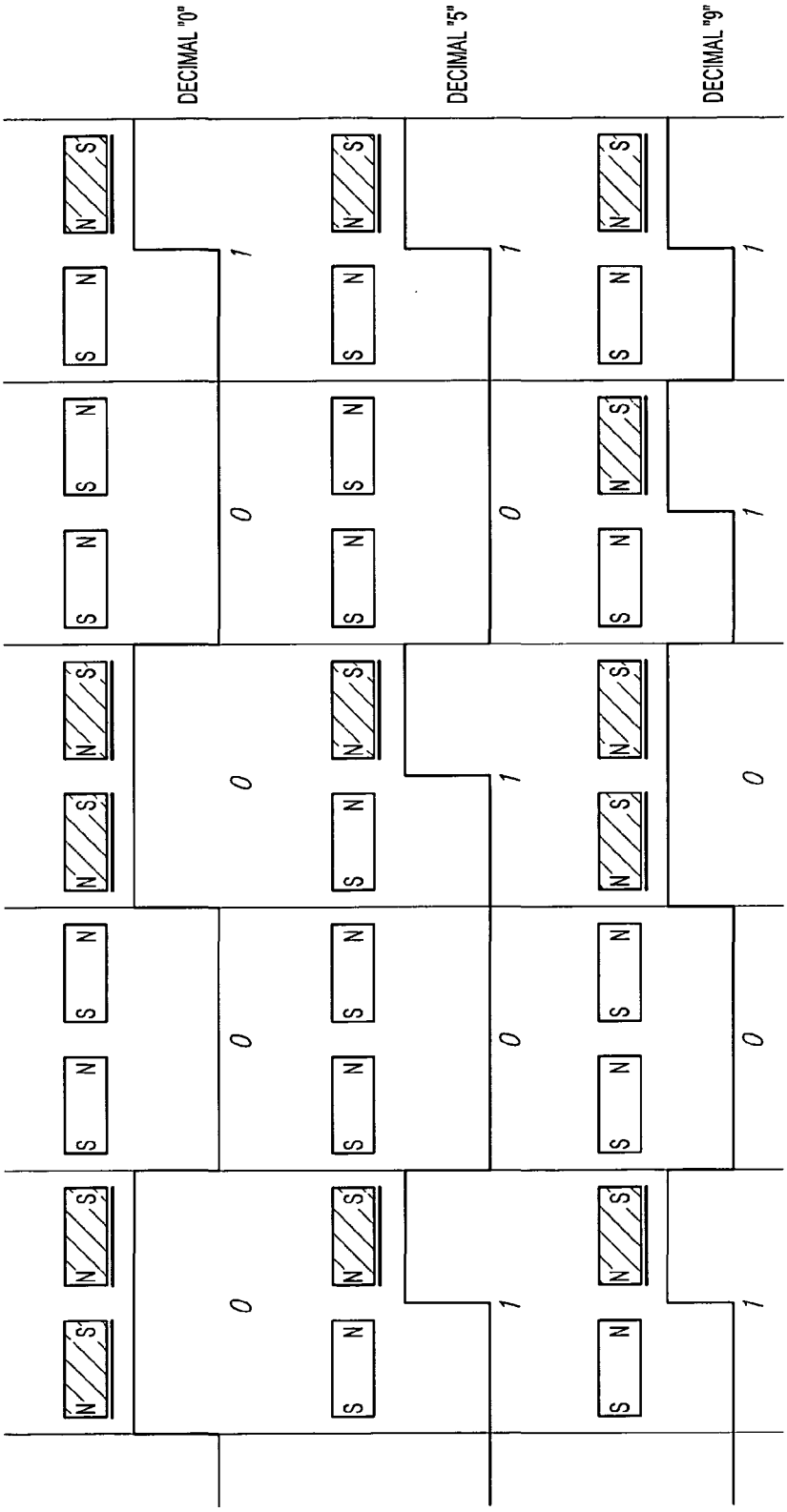


FIG. 7C

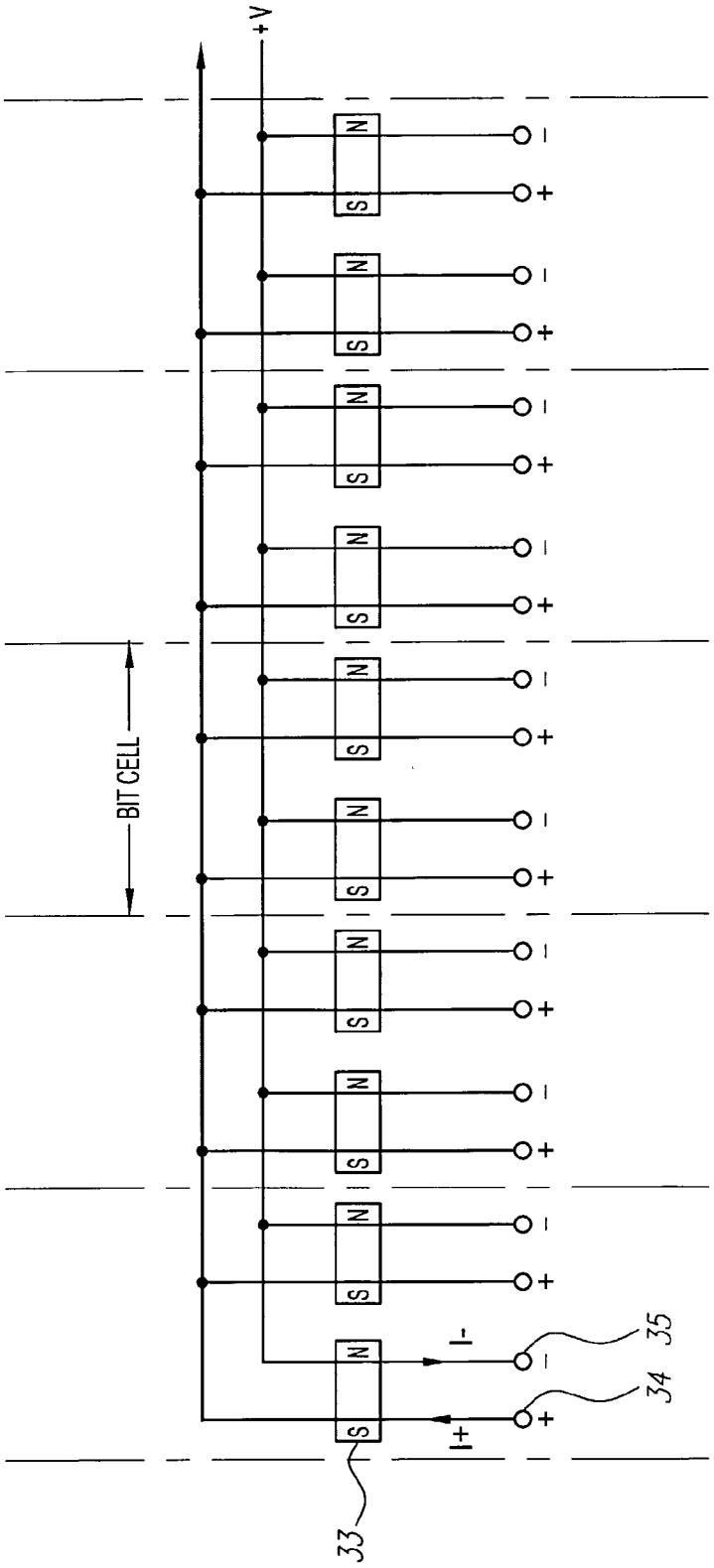


FIG. 7D

IPR2025-00645 Page 00441

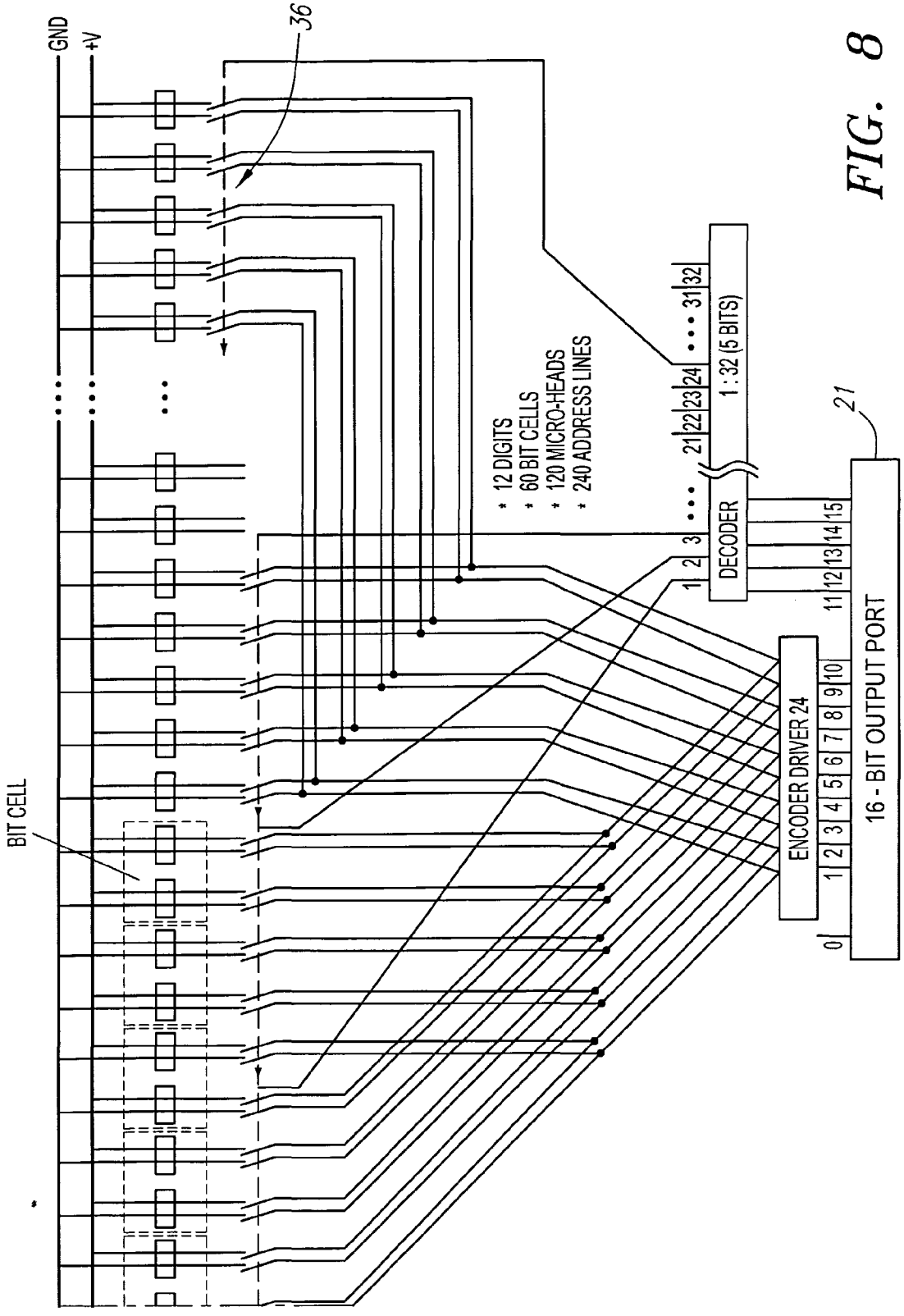


FIG. 8

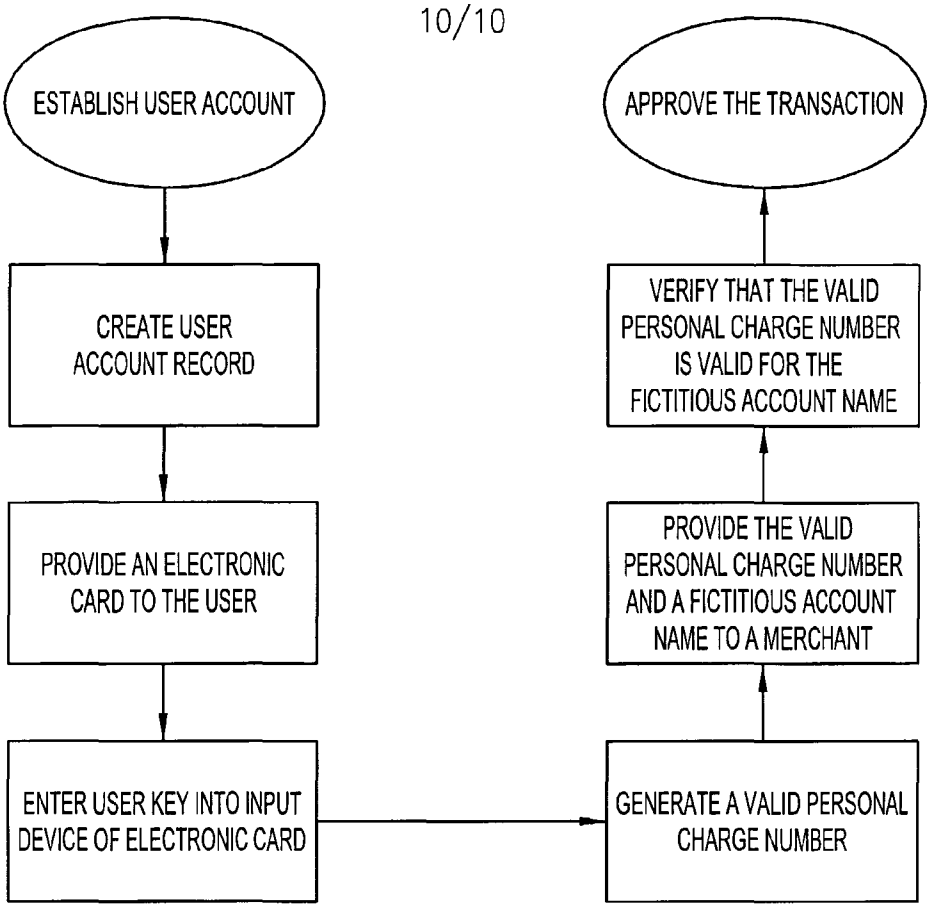

ESTABLISH USER ACCOUNT
CREATE USER ACCOUNT RECORD
PROVIDE AN ELECTRONIC CARD TO THE USER
ENTER USER KEY INTO INPUT DEVICE OF ELECTRONIC CARD
GENERATE A VALID PERSONAL CHARGE NUMBER
PROVIDE THE VALID PERSONAL CHARGE NUMBER AND A FICTITIOUS ACCOUNT NAME TO A MERCHANT
VERIFY THAT THE VALID PERSONAL CHARGE NUMBER IS VALID FOR THE FICTITIOUS ACCOUNT NAME
APPROVE THE TRANSACTION

FIG. 9

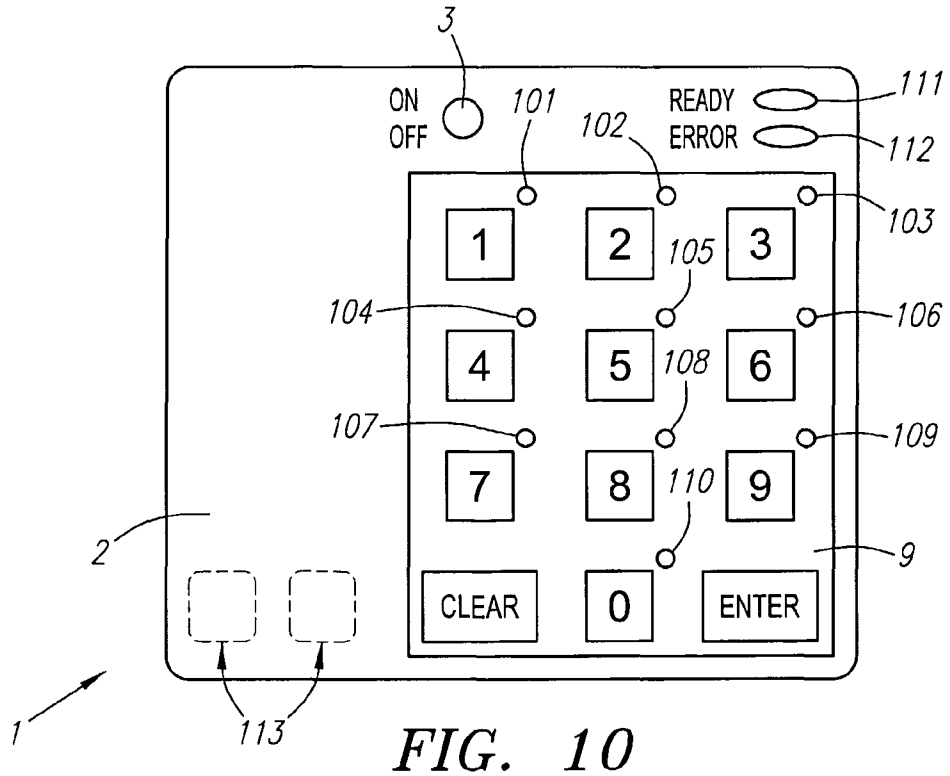

3
ON
OFF
101
102
READY
ERROR
111
112
103
1
2
3
105
104
106
4
5
6
108
107
109
7
8
9
110
2
9
CLEAR
0
ENTER
1
113

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/15612

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/00, 17/60; G06K 5/00, 7/01
US CL : 235/375, 379, 380, 382.5; 705/50, 64, 67, 72, 74

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)
U.S. : 235/375, 379, 380, 382.5; 705/50, 64, 67, 72, 74

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 practicable, 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 --- Y	US 4,918,631 A (HARA et al.) 17 April 1990 (17.04.1990), figures 1 and 2 and columns 2-4.	36, 37 --- 16-17, 19-20
Y	US 5,884, 271 A (PITRODA) 16 March 1999 (16.03.1999), figures 1, 3, summary of invention, col. 11, lines 30-57, col. 17, lines 10-44.	3, 7-11, 18-19, 21-35
X, P --- Y, P	US 6,163,771 A (WALKER et al.) 19 December 2000 (19.12.2000), figures 1-3, entire patent.	1-2, 4-6, 12-15, 38-39 --- 3, 7-11, 16-35

☐ 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 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
04 February 2002 (04.02.2002)	13 FEB 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Larry D Taylor Telephone No. (703) 306-5867

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/029942 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/31335

(22) International Filing Date: 1 October 2002 (01.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/968,628 1 October 2001 (01.10.2001) US

(71) Applicant: CHAMELEON NETWORK, INC. [US/US]; 950 Winter Street, Suite 1400, Waltham, MA 02451 (US).

(72) Inventors: BURGER, Todd, O.; 386 Lincoln Street, Lexington, MA 02421 (US). COHEN, Robert, M.; 119 Bent Road, Sudbury, MA 01776 (US).

(74) Agent: PRITZKER, Randy, J.; Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210 (US).

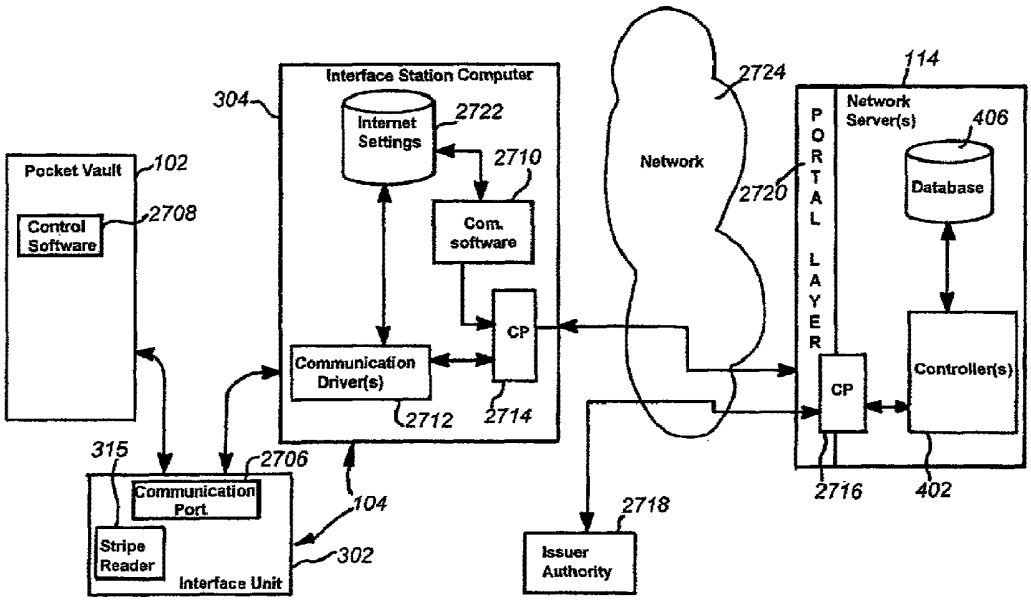
(81) Designated State *(national)*: CA.

(84) Designated States *(regional)*: 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).

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: PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD



(57) Abstract: In one embodiment, an electronic device is used to authenticate an identity of a user to determine that the user is permitted to access restricted information on a server. In response to the electronic device authenticating the identity of the user, a software module on a computer operated by the user is permitted to access the restricted information. In another embodiment, an electronic device is used to authenticate an identity of a user. In response to the electronic device authenticating the identity of the user, the settings on a computer are altered to correspond to settings on the electronic device.

WO 03/029942 A2

PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD

RELATED APPLICATIONS

This is a Continuation-in-Part (CIP) of U.S. Application Serial No. 09/675,438, filed September 28, 2000, and now pending, which claims the benefit of each of: (1) Application Serial No. 60/156,356, filed September 28, 1999; (2) Application Serial No. 60/167,050, filed November 23, 1999; (3) Application Serial No. 60/184,425, filed February 23, 2000; and (4) Application Serial No. 60/217,542, filed July 12, 2000.

FIELD OF THE INVENTION

The present inventions are directed to novel systems and methods for engaging in transactions involving financial and/or non-financial media.

BACKGROUND OF THE INVENTION

People often times carry wallets with them when they engage in their day to day activities. A typical wallet is made of leather or other suitable material, and is generally a foldable structure that readily fits into a pocket or purse. A wallet typically includes a number of pockets, pouches, or the like for storing items such as a driver's license, a social security card, identification cards, credit cards, debit cards, membership cards, commuter passes, access tools, business cards, cash, coupons, event tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipts, photographs, etc.

Wallets are frequently stolen, lost, or misplaced. When any of these events occurs, not only must the wallet itself be replaced, but all of the contents of the wallet must be replaced as well. As anyone who has lost a wallet can testify, replacing the contents of a wallet can be cumbersome and expensive. In addition, if a wallet is stolen or if a lost wallet falls into the wrong hands, the contents of the wallet may be used to engage in unauthorized activities which financially detriment the wallet owner, as well as any banks, credit issuers, and/or other institutions that issued financial media to the wallet owner.

While the wallet owner is generally able to "cancel" financial media in such situations by contacting the respective financial media issuers, often times this is done too late, i.e., after one or more media have been exploited by the unauthorized user. In some cases, the

wallet owner may not recall all of the contents of the now stolen wallet, and so may fail to report theft of one or more items. Further, in addition to any cash contained in a lost or stolen wallet, many media issued by non-financial media issuers have a significant cash value, e.g., transportation tickets, event tickets, commuter passes, and the like, and therefore represent an immediate (and often times unrecoverable) financial loss to the wallet owner. Moreover, the misappropriation of media issued by non-financial media issuers that contain personal information, e.g., a drivers license, social security card, identification card, etc., present the opportunity for an unauthorized possessor of a wallet to engage in the practice known as "identity theft," whereby the possessor may assume the identity of the wallet owner for various fraudulent purposes, e.g., using the assumed identity to obtain and exploit one or more new financial media.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, a method is disclosed for enabling a software module on a computer operated by a user to access restricted information on a server. With an electronic device distinct from the computer, an identity of the user is authenticated to determine that the user is permitted to access the restricted information on the server. In response to the electronic device authenticating the identity of the user, the software module on the computer is permitted to access the restricted information on the server.

According to another aspect, a method is disclosed for altering settings on a computer to correspond to settings on an electronic device distinct from the computer. With the electronic device, an identity of a user is authenticated to determine that the user is authorized to use the electronic device. In response to authenticating the identity of the user, the settings on the computer are altered to correspond to settings on the electronic device.

According to another aspect of the invention, a system for enabling a software module on a computer operated by a user to access restricted information on a server includes an electronic device which includes a user-authenticator to authenticate an identity of the user to determine that the user is permitted to access the restricted information on the server. The system further comprises means for, in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

According to yet another aspect, a system for altering settings on a computer to correspond to settings on an electronic device distinct from the computer comprises a user authenticator included in the electronic device to authenticate an identity of a user to determine that the user is authorized to use the electronic device. The system further comprises means for, in response to authenticating the identity of the user, altering the settings on the computer to correspond to settings on the electronic device.

According to another aspect, an apparatus includes a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory, supported by the housing, that stores transaction information for at least first and second media; and at least one output, supported by the housing, that releases at least a portion of the transaction information to a point-of-sale (POS) terminal after the user authenticator has authenticated the identity of the user.

According to another aspect of the present invention, a method involves steps of: (a) storing transaction information for at least first and second media in a memory of a device (b) using the device to authenticate an identity of a user; and (c) after authenticating the identity of the user with the device, transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect of the present invention, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus.

According to another aspect of the present invention, a method involves steps of: storing transaction information for at least one media in a memory of a first device; using the first device to authenticate an identity of a user; and after authenticating the identity of the user with the first device, releasing an embedded identification code of the apparatus from the housing that enables a second device receiving the embedded identification code to authenticate the identity of the first device.

According to another aspect of the present invention, an apparatus includes: at least one memory that stores transaction information for at least first and second media; at least

one input that enables a user to select one of the at least first and second media; a display that provides a visual indication to the user regarding which of the at least first and second media has been selected with the at least one input; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect of the present invention, a method involves steps of: storing transaction information for at least first and second media in a memory of a device; receiving as input a user's selection of one of the at least first and second media; displaying a visual indication to the user regarding which of the at least first and second media has been selected; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect of the present invention, an apparatus includes: at least one memory that stores transaction information for at least one financial media and at least one non-financial media; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect of the present invention, a method involves steps of: storing transaction information for at least one financial media and at least one non-financial media in a memory of a device; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect of the present invention, a system includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a device releasably attached to the housing; and configuring means, supported by the housing, for selectively configuring the device to hold the transaction information so that the device may be used to engage in a transaction involving the at least one media.

According to another aspect of the present invention, a method involves steps of: (a) storing transaction information for at least one media in a memory of a first device, the first device having a second device releasably attached thereto; (b) while the second device is attached to the first device, configuring the second device to hold the transaction information for the at least one media based on the contents of the memory; (c) detaching the second device from the first device; and (d) using the second device to engage in a transaction involving the at least one media.

According to another aspect of the present invention, a system includes: a first device including a user authenticator that authenticates an identity of a user; and a second device

releasably attached to the first device, wherein the second device holds transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media, and wherein the second device is detached from the first device after the user authenticator has authenticated the identity of the user.

According to another aspect of the present invention, a method involves steps of: with a first device, authenticating an identity of a user; and after authenticating the identity of a user with the first device, detaching a second device from the first device, the second device holding transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media.

According to another aspect of the present invention, a system includes: a first device; a second device that has the first device releasably attached thereto, the second device including means for selectively configuring the first device to hold transaction information for a first media but not for a second media so that the first device may be used to engage in a transaction involving the first media but not the second media, and the second device further including means for selectively configuring the first device to hold transaction information for the second media but not for the first media so that the first device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect of the present invention, a method involves steps of: selectively configuring a device to hold transaction information for a first media but not for a second media so that the device may be used to engage in a transaction involving the first media but not the second media; and selectively configuring the device to hold transaction information for the second media but not the first media so that the device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect of the present invention, a system includes: at least one memory that stores first transaction information for a first media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively add second transaction information for a second media to the memory.

According to another aspect of the present invention, a method involves steps of: storing first transaction information for a first media in a memory of a device; releasing at least a portion of the first transaction information to a point-of-sale (POS) terminal; and in

response to a request by the person to whom the first transaction information is issued, adding second transaction information for a second media to the memory.

According to another aspect of the present invention, a system includes: at least one memory that stores first transaction information for a first media and second transaction information for a second media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively remove at least a portion of the second transaction information from the memory.

According to another aspect of the present invention, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in a memory of a device; releasing at least a portion of the first transaction information to a point-of-sale (POS) terminal; and, in response to a request by the person to whom the second media is issued, removing at least a portion of the second transaction information from the memory.

According to another aspect of the present invention, a system includes: at least one memory that stores transaction information for at least one media; at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal; and means for enabling at least one functional characteristic of the at least one media to be altered by altering the contents of the least one memory.

According to another aspect of the present invention, a method involves: storing transaction information for at least one media in a memory of a device; releasing at least a portion of the transaction information to a point-of-sale (POS) terminal; and altering at least one functional characteristic of the at least one media by altering the contents of the least one memory.

According to another aspect of the present invention, an apparatus includes: a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory that, supported by the housing, stores first transaction information for a first media and second transaction information for a second media; and at least one output, supported by the housing, that releases the first transaction information only after the user authenticator has authenticated the identity of the user, and that releases the second information without requiring the user authenticator to have authenticated the identity of the user.

According to another aspect of the present invention, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in at least one memory of a device; using the device to authenticate an identity of a user; releasing the first transaction information only after the identity of the user has been authenticated; and releasing the second transaction information without requiring the identity of the user to be authenticated.

According to another aspect of the present invention, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device causes the first device to generate a machine-readable code for only a predetermined, finite period of time after the first device is detached from the second device.

According to another aspect of the present invention, a method involves a step of generating a machine-readable code on a device for only a predetermined, finite period of time.

According to another aspect of the present invention, an apparatus includes: a portable substrate; a power supply supported by the substrate; and at least one controller supported by the substrate and powered by the power supply, the at least one controller being configured to generate a simulated magnetic stripe on the substrate.

According to another aspect of the present invention, an method involves a step of generating a simulated magnetic stripe on a portable device.

According to another aspect of the present invention, a system includes: at least one memory that stores transaction information for at least one media; a user authenticator that authenticates an identity of the user; and a display that provides a visual indication to the user regarding the at least one media, the visual indication being displayed for only a predetermined, finite period of time after the user authenticator has authenticated the identity of the user.

According to another aspect of the present invention, a method involves steps of: authenticating an identity of a user; and displaying a visual indication to the user regarding the at least one media for only a predetermined, finite period of time after authenticating the identity of the user.

According to another aspect of the present invention, a system includes a portable device that can be used to engage in point-of-sale (POS) transactions; and a device remote

from the portable device, that can disable an ability of the portable device to engage in POS transactions.

According to another aspect of the present invention, a method involves steps of: providing a portable device that can be used to engage in point-of-sale transactions; and at a location remote from the portable device, disabling an ability of the portable device to engage in POS transactions.

According to another aspect of the present invention, a method involves steps of: storing transaction authorization information for at least two media in a first memory of a first device; and storing the transaction authorization information for the at least two media in a second memory, which is disposed at a location remote from the first device.

According to another aspect of the present invention, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device can cause the first device to generate a machine-readable code after the first device is detached from the second device, the second device including at least one controller configured so as to be capable of causing the first device to generate the machine-readable code only for a finite, predetermined period of time.

According to another aspect of the present invention, a method involves a step of configuring a first device such that the first device is capable, for only a predetermined, finite period of time, of generating a machine-readable code on a second device.

According to another aspect of the present invention, a method involves steps of: receiving information at a first device that has been transmitted over an electronic communication link; and after receiving the information at the first device, using a media at the first device to access a quantity of credit or cash reserves that could not be accessed prior to the first device receiving the information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating an example of a network system in which a portable electronic authorization device (also referred to herein as a "Pocket Vault") may be employed according to one embodiment of the invention;

Fig. 2 is a block diagram showing an illustrative embodiment of the Pocket Vault shown in Fig. 1;

Fig. 3 is a block diagram showing an illustrative embodiment of one of the interface stations shown in Fig. 1;

Fig. 4 is a block diagram showing an illustrative embodiment of the network server(s) shown in Fig. 1;

Fig. 5 is a diagram showing an example of how the memory of the Pocket Vault shown in Fig. 2 may be configured in accordance with one embodiment of the invention;

Fig. 6 is a block diagram showing an illustrative embodiment of the token (e.g., a card) associated with the Pocket Vault shown in Fig. 2;

Fig. 7 is a flow diagram illustrating a primary routine that may be executed by the controller of the Pocket Vault shown in Fig. 2;

Fig. 8 is a flow diagram illustrating an example implementation of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7;

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine shown in Fig. 10;

Fig. 12 is a flow diagram illustrating an example implementation of the VERIFY CARD RETURN routine shown in Fig. 7;

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the pocket vault interface unit shown in Fig. 3;

Fig. 14 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the interface station computer shown in Fig. 3;

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine shown in Fig. 14;

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 14;

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine in Fig. 14;

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine shown in Fig. 14;

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller(s) of the network server(s) shown in Fig. 4;

Fig. 20 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO REGISTER NEW POCKET VAULT HOLDER routine shown in Fig. 19;

Fig. 21 is a flow diagram illustrating an example implementation of the PROCESS REQUEST BY MEDIA ISSUER/ADVERTISER TO UPDATE NETWORK SERVER routine shown in Fig. 19;

Fig. 22 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 19;

Fig. 23 is a flow diagram illustrating an example implementation of the PROCESS REQUEST FROM HOLDER TO LOAD NEW FILE ONTO NETWORK SERVER routine shown in Fig. 19;

Fig. 24 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine shown in Fig. 19;

Fig. 25 is a flow diagram illustrating an example implementation of the AUTHORIZED POCKET VAULT USE? routine shown in each of Figs. 20, 22, and 24; and

Figs 26a-26p are illustrations of the portable electronic authorization device, as well as the token (e.g., a card) associated therewith, as these items may appear when in use;

Fig. 27 is a block diagram illustrating several additional features that may optionally be added to a network system such as that shown in Fig. 1 so as to enhance the functionality of the network;

Fig 28 is a block diagram illustrating example components that may optionally be added to software executing on a controller of the Pocket Vault, such as the software described in connection with Figs. 7-12, so as to enhance the functionality of the Pocket Vault in a network environment;

Fig 29 is a data flow diagram illustrating an example of how data may flow between the Pocket Vault and a user interface of an interface station computer to which the Pocket Vault is interfaced/docked;

Fig. 30 is a flow diagram illustrating an example of a primary routine that may be executed by a website on the network server(s) shown in Fig. 27, which website may be accessed, for example, by a browser executing on the interface station computer shown in Fig. 27;

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine shown in Fig. 30;

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine shown in Fig. 33;

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine shown in Fig. 33;

Fig. 36 is a flow diagram illustrating an example implementation of the RECOVERY routine shown in Fig. 33;

Fig. 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine shown in Fig. 33;

Fig. 38 is a flow diagram illustrating an example implementation of the BACKUP routine shown in Fig. 33; and

Fig. 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine shown in Fig. 33.

DETAILED DESCRIPTION

A new method and system for producing, distributing, storing, and using the typical contents of an individual's wallet is disclosed herein. Essentially, the system may enable individuals to replace nearly all of the paper and plastic contents of their wallets with a single, hand-held portable electronic authorization device. The system may include the portable electronic authorization devices, removable morphing tokens or cards associated with such devices, associated computer peripherals, software and certain network capabilities. As a whole, the system may eliminate virtually all of the distribution costs and security concerns associated with paper and plastic media.

Because the device may incorporate many different media that are commonly stored in a person's wallet, possibly including both financial and non-financial media, it is much more than a simple point-of-sale (POS) device. Therefore, the device may be more appropriately referred to as a multi-purpose, "point-of-transaction" device. In any situation

of presentment, whether for purposes such as building security, demonstrating membership or using credit or debit capacity, the system is designed to perform tasks more safely, securely and with greater ease than is possible with prior art systems. Further, while certain computer technologies are involved, the preferred embodiment is such that some people may barely recognize it as a computer, seeing instead a more comfortable to carry, easier-to-use, safer and more securely packaged means of transporting typical wallet contents.

The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various financial and non-financial media, that also may enable individuals and retailers to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns.

A network system 100 configured according to one illustrative embodiment of the invention is shown in Fig. 1. As shown, the network system 100 may include a portable electronic authorization device 102 (alternatively referred to herein as a "Pocket Vault") and an associated token 102a (alternatively referred to herein as a "Chameleon Card"). Each person desiring to use the network system 100 may possess his or her own the Pocket Vault 102 and associated token 102a. Some individuals may choose to own multiple Pocket Vaults or Chameleon Cards. The system and software therefore may accommodate the use of multiple Pocket Vaults and multiple Chameleon Cards by one individual.

Referring to Fig. 1, in addition to the Pocket Vault 102, the network system 100 may include one or more network servers 114 to which various other network components are coupled. Although multiple, load-sharing network servers 114 may be employed in a typical application, the network server(s) 114 will hereinafter, for convenience, occasionally be referred to as a single network server 114. Coupled to the network server 114 are: several different types of interface stations 104 (i.e., a validation interface station 104a , a personal interface station 104b, and a commercial interface station 104c), one or more commercial card readers 106, one or more commercial bar code readers 107, and several computers 108, 110, and 112 operated by one or more advertisers, non-financial media issuers, and financial

media issuers, respectively. The structure and functionality of each of the components of the network system 100 in accordance with illustrative embodiments of the invention are described below.

As shown in Fig. 1, the network server 114 may form the hub of the network system 100, with each of the interface stations 104, the commercial card reader 106, the commercial bar code reader 107, and the computers 108, 110, and 112 being coupled thereto. As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders.

Any of a number of techniques may be used to interconnect the various elements of the network system 100, and the invention is not limited to any particular networking technique. In one illustrative embodiment, for example, the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links).

As shown in Fig. 1, the Pocket Vault 102 may be interfaced with any of the interface stations 104a-c so as to permit information to be uploaded from the network server 114 to the Pocket Vault 102, or to be downloaded from the Pocket Vault 102 to the network server 114. In one illustrative embodiment, each of the interface stations 104 includes a docking mechanism that permits a Pocket Vault 102 to be physically, as well as electronically, interfaced therewith. In such an embodiment, once the Pocket Vault 102 is physically "docked" with an interface station 104, the Pocket Vault 102 may communicate with the interface station 104 using any now known or later discovered technique. For example, physical contact may be made between respective electrodes or plugs, a line of sight (e.g., infrared) wireless link may be established, or any other interfacing technique may be employed.

The Pocket Vault 102 may additionally or alternatively be configured such that it need not be physically docked with or even in the same room as the interface station 104, as a

wireless network such as Bluetooth may be employed to permit communication between devices on the network system 100. In fact, in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114, without the interface stations 104a-c facilitating communication therebetween. In addition, in some embodiments, Pocket Vaults 102 may communicate directly with one another. In such embodiments, such inter-device communication may permit value to be exchanged directly between Pocket Vaults 102.

The personal docking station 104b may allow setting or changing of user preferences, recording of miscellaneous information by the Pocket Vault holder, replenishment or deletion of information regarding particular media, and may also permit additional media (e.g., a library card) to be added to the device. The Pocket Vault holder may, for example, directly add non-value-based media (e.g., a membership number for the local Historical Society) and notes to the Pocket Vault 102. In one embodiment, value-based and certain identification media (a driver's license, passport, building security ID, etc.) may be added or reinstated only through a secure connection to the network server 114 (as described below), in response to an update request from the Pocket Vault holder. In addition, the personal interface station may provide a mechanism to download transaction activity involving the Pocket Vault 102 into an individual's home computer. There are many users of home finance software. These applications can be relatively "data hungry," and commonly require users to download checking and debit card data from their banks (or key it in manually) and to key in the details of credit card and cash purchases. All of this keying and internet file downloading from third parties may be replaced by a simple docking procedure, i.e., when the Pocket Vault 102 is interfaced with the personal docking station 102b.

As shown in Fig. 1, and as described below in more detail, the Pocket Vault 102 may be equipped to generate the token 102a such that the token 102a has transactional information regarding a media (e.g., a simulated magnetic stripe or a bar code) produced thereon. In such an embodiment, after the token 102a has been generated, the token 102a may be used by the Pocket Vault holder to engage in a transaction wherein an entity swipes the simulated magnetic stripe of the token 102a through a card reader 106 or scans the bar code on the token 102a using a bar code reader 107. Additionally or alternatively, the token 102a may include a suitable Smartcard interface so that the Chameleon Card 102 may be used with Smartcard compatible devices.

Because the token 102a may be caused to take on a different personality each time it is released from the Pocket Vault 102, a plurality of media may be stored electronically in memory of the Pocket Vault 102, and the token 102a may, upon request, be generated to take on the personality selected by the Pocket Vault holder. The respective media stored on the Pocket Vault 102 may be issued by different and unrelated media issuers. As used herein, two media issuers are "unrelated" if there exists no legal relationship between them. The token 102a may also have display capacity, sufficient to indicate the media personality that it has taken on. This may or may not include display of the specific identity that is temporarily encoded on the token 102a. In some embodiments, value may be exchanged between two Pocket Vaults 102 when one the Pocket Vault 102 generates a token 102a having a value-based or value-linked media stored thereon, and the token 102a so generated is passed to the other the Pocket Vault 102, which then may then access the media and extract value therefrom or add value thereto. As mentioned above, this sort of value exchange may also be accomplished directly between two Pocket Vaults 102 over a wireless network, such as Bluetooth.

As discussed in more detail below, in addition to or in lieu of the token 102a, the Pocket Vault 102 may also generate a bar code for a selected media on the Pocket Vault's display (not shown in Fig. 1), and the bar code reader 107 may be used to scan the displayed bar code to process a transaction. Further, a transaction may be processed via a commercial interface station 104c either by use of a docking terminal or via a wireless network scheme such a Bluetooth. In one embodiment, some commercial interface stations 104c may comprise an interface station linked to a standard commercial card reader 106 or commercial bar code reader 107, with the card reader 106 or bar code reader 107 being modified to accept input from the station.

To permit the Pocket Vault holder to select from among the various media stored in memory of the Pocket Vault 102, the Pocket Vault 102 may comprise a display (not shown in Fig. 1). By employing either a display having a user-manipulable touch screen or a separate user input device (not shown in Fig. 1), a Pocket Vault holder can effectively flip through the contents of the Pocket Vault 102 to locate and select a desired media (e.g., a credit card, driver's license, library card, frequent flier card, etc.) much like a person can flip through the contents of his or her wallet to do the same.

The use of a display on the Pocket Vault 102 also creates an opportunity for media providers to go from a static presentation of their brand (logo, etc.) to having the option of dynamic branding and messaging. In addition, using the display, the presentment of active marketing at the "moment of buying decision" is possible. Specifically, the logo and message displayed to the Pocket Vault holder may incorporate motion, moving images and messages. To conserve power, moving images may be presented only at certain times, e.g., in response to internal or external events or communications.

In the embodiment of Fig. 1, the computers 108, 110, and 112, together with the network server 114, may represent a secure infrastructure of server databases capable of storing information for purposes of delivering personalized services to holders of Pocket Vaults 102. The network server 114 may also track activity of Pocket Vault holders and compile marketing information based thereupon that may prove useful to media issuers and/or advertisers. The Pocket Vault holder may have control over the ability of the network server 114 to track activity. The information maintained on the network system 100 may originate with the holders of Pocket Vaults 102 and/or may originate with the other entities having access to the network system 100 (e.g., advertisers and media issuers).

As discussed below in more detail, in some embodiments of the invention, certain uses of the Pocket Vault 102, as well as each of the interface stations 104a-c, may be permitted only by pre-authorized individuals. To this end, a suitable user authentication technique may be employed in connection with each attempted use of any of these devices. One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis. Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder's identity. In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly.

It should be appreciated that, for some applications, it may be desirable to receive and store authentication information (e.g., fingerprint data) of some or all Pocket Vault holders in the network server 114. Accordingly, in some embodiments, such authentication information may be maintained by the network server 114. This authentication information may be transmitted to the network server 114, for example, when Pocket Vaults 102 are first validated.

As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information.

A similar level of care may also be taken to ensure that only authorized individuals are permitted to validate interface stations 104a-c by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, as with the Pocket Vaults 102, after it has been confirmed that each interface station's authorization information has been properly stored in the interface station 104, a trust relationship may be set up between the network server 114 and the interface station 104. This relationship may also involve, for example, the registration of a unique encrypted chip ID of the interface station 104 with the network server 114 through a secure Internet connection, the distribution of a digital certificate to the interface station 104, and the grant authority to the interface station 104 to permanently store the interface station operator's authentication information. While, in some embodiments, the Pocket Vault 102 and/or the interface stations 104 are each permitted to store authentication information for only one individual, it should be appreciated that, in alternative embodiments, the Pocket Vault 102 and/or the interface stations 104 may each store authentication information for more than one individual, thereby permitting multiple people to use them.

Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114, as well as with any other networked devices or sites that require a high level of trust. Also, the existence of these trust relationships enable individual Pocket Vaults 102 to accept other services provided by the network servers 114, such as the backup and recovery of information stored within the Pocket Vaults 102. That is, the network servers 114 can serve as a repository for all of the information stored on every validated Pocket Vault 102 (except the holder's authentication information – which, in some embodiments, is stored only in the Pocket Vault 102). To ensure that the network server 114 stores an accurate version of the contents of each Pocket Vault 102, information may, for example, be uploaded from the network server 114 to a Pocket Vault 102 or downloaded from the Pocket Vault 102 to the network server 114 each time the Pocket Vault 102 is interfaced with any of the interface stations 104a-c. Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault 102, and the entire contents of the lost Pocket Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card.

In addition to serving as a repository for Pocket Vault information, the network server 114 may also serve as a repository for information regarding media issuers or advertisers, and may further provide various services to these entities. For example, the network server 114 may facilitate transactions involving media issued by media issuers, and may permit new media to be issued or lost media to be replaced at a fraction of the cost of generating new physical tokens or replacing lost ones. Additionally, the network server 114 may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them. The network server 114 may also function as an advocate for Pocket Vault holders, advertisers, and/or media issuers when it utilizes its portfolio of Pocket Vault holders, media issuers, and/or advertisers to secure privileges. Examples of such advocacy include the ability to secure buying power for Pocket Vault holders as a group or to provide

media issuers and advertisers with a highly efficient tool for generating awareness for affinities or causes that fit appropriate holder markets. In sum, the services provided by the network server 114 enable Pocket Vault holders to combine and manage their media data using a single, hand-held device, and enables advertisers and media issuers to understand more about, and more readily reach more of, their customers than ever before.

Fig. 2 shows an example embodiment of the Pocket Vault 102 of Fig. 1. The Pocket Vault 102 may employ components similar to those used in modern personal digital assistants (PDAs) and palm top computers. Examples of such products include PDAs such as the "Palm Pilot" from Palm, Inc. (www.palm.com), and the "Casiopedia" from Casio, Inc. of Dover, New Jersey (www.casio.com). As shown, the Pocket Vault 102 may include a controller 202, as well as a transceiver 204, a user input device 206, a docking interface 208, a read/write memory 210, a write-once memory 212, a power manager 214, an indicator 215, a display 216, a token port 218, and a fingerprint scanner 220, all coupled to the controller 202. In addition, the Pocket Vault 102 may include a hard-wired memory (not shown) to store device serial numbers and key operating system and encryption software components.

Actual views of an example embodiment of the Pocket Vault 102, as well as the token 102a associated therewith, are shown in Figs. 26A-26P. The views of Figs. 26A-P, including the items displayed on the display 216, are discussed in more detail below in connection with the flow diagrams of Figs. 7-12. At this point, however, with reference to Figs. 26A-L and 26O, it may be noted that the Pocket Vault 102 may comprise a housing 2602 in which the components shown in Fig. 2 may be disposed. As illustrated in Figs. 26E and 26F, the housing 2602 may be approximately seventy millimeters wide, approximately one hundred millimeters long, and approximately fifteen millimeters deep. Thus, in the embodiment shown, the housing 2602 has an internal volume of less than 105 cubic centimeters. Of course, in alternative embodiments, the housing 2602 may be slightly larger or smaller than that shown. For example, in different embodiments, the housing 2602 may have an internal volume of less than five hundred cubic centimeters, or less than four hundred cubic centimeters, or less than three hundred cubic centimeters, or less than two hundred cubic centimeters, or less than one hundred cubic centimeters, or less than any other volume value that falls between one hundred and five hundred centimeters. In one embodiment, the housing 2602 is sized so that the Pocket Vault 102 may readily fit into the rear pocket of a pair of pants. One feature of the illustrative embodiment of the Pocket Vault 102 shown in

Fig. 2 which may permit its size to be reduced below that of a standard personal computer is the fact that the embodiment shown lacks a disk drive (either hard or floppy) or any similar memory storage device (e.g., a tape drive) that consumes a significant volume within the housing 2602. It should be appreciated, of course, that alternative embodiments may include such memory devices, and that the invention is not necessarily limited to embodiments that exclude them. In addition to the lack of a disk drive or the like, in some embodiments, the power manager 214 may reduce the power consumption of the active components of the Pocket Vault 102 well below that of a standard personal computer, thereby enabling a very small and light weight battery to be employed, as opposed to the relatively large and heavy batteries typically employed in personal computers.

The housing 2602 may provide a water-resistant or waterproof environment for the components housed thereby. The housing materials of Pocket Vaults 102 may be brightly colored, in addition to traditional black or brown, thereby helping their holders to make a fashion statement and/or permitting them to be readily spotted if misplaced. Deluxe versions may be clad in leather, Kevlar™, Gortex™, aluminum and/or stainless steel. In some embodiments, the housing 2602 may even be woven into garments.

Referring again to Fig. 2, any of a number of devices may be used to implement the controller 202, and the invention is not limited to any particular type of controller. In one illustrative embodiment, for example, the controller 202 comprises a low-power multiprocessor or microcomputer having an on-board SRAM and/or flash memory and a real time clock calendar. One example of a suitable controller is the "Motorola Dragonball" Processor from Motorola, Inc. (www.motorola.com). The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID is released from the Pocket Vault 102 only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder. A signal processor for Bluetooth or another wireless connection may also be employed within or along with the controller 202.

The transceiver 204 may be any type of transceiver (or separate transmitter and receiver) capable of communicating with the other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may, in fact, include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface

the Pocket Vault with a "docking station" type interface unit, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth.

In one illustrative embodiment, the user input device 206 is implemented as part of a touch-screen display used as the display 216 (described below). Additionally or alternatively, the user input device 206 may include dedicated buttons, a keypad, a touch pad, a microphone and speech recognition software, a wand or joystick, or any other suitable implement that permits a person to provide input to the controller 202. The user input device 206 may also be integrated into the fingerprint scanner 220 or into an alternative bio-metric input device. By manipulating the user input device 206, a Pocket Vault holder may select one of a number of media stored in memory of the Pocket Vault 102 for display and/or use in connection with a transaction, and may otherwise control or provide input to software executing on the controller 202. In one embodiment, a keypad is employed as the user input device 206, thereby permitting the holder to input a PIN code as a means of authenticating the holder's identity.

The docking interface 208 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 208 may, for example, include a multi-pin plug adapted to mate with a receptacle disposed on the interface units 104a-c, or vice versa. The docking interface 208 may also comprise one or more implements (e.g., grooves or keys) to ensure that the plug or other docking interface 208 mates correctly with the reciprocal device on an interface unit 104 when the two are physically mated together.

The read/write memory 210 may take on any of a number of forms, and the invention is not limited to any particular type of memory. The memory 210 may, for example, comprise a suitable non-volatile SRAM. Similarly, any suitable memory device that permits a only single write operation to take place may be employed as the write-once memory 212. The memory 210 may have instructions stored therein which, when executed by the controller 202, cause the controller 202 to implement the routines/software described below in connection with Figs. 7-12 and/or Fig. 28. Of course, the memory 210 may also contain a suitable operating system (e.g., Palm OS, Microsoft's Windows CE, Microsoft's Windows for Smartcards, or some similar offering), appropriate device drivers, and other software employed in connection with the controller 202 and/or the peripherals thereof. The memory 210 may also be used to store the various media and personal information retained by the

Pocket Vault 102. In one illustrative embodiment, the memory 210 stores a plurality of different media issued by different and unrelated media issuers, including both financial (e.g., a credit or debit card) and non-financial media (e.g., a drivers license or a library card). Other examples of media or information that may be stored in the memory 210 include: a social security card, identification cards, membership cards, discount cards, commuter passes, toll passes, transit cards, access tools such as hotel keys, business cards, coupons, concert and theatre tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipt information, photographs, etc.

As used herein, "financial media" refers to any media which can, as a matter of course, be used to purchase goods or services, whereas "non-financial media" refers to any media which, while possibly having some value to the Pocket Vault holder, cannot, as a matter of course, be used to purchase goods or services. Examples of financial media include value-linked and value-based media such as debit or credit cards issued by a bank or other financial institution, telephone calling cards, etc. Examples of non-financial media include: library cards, driver's licenses, building access cards, etc. In one embodiment, the memory 210 is large enough to store as many as one hundred compressed graphic image files, and full data sets for as many as one hundred types of media.

In addition, the memory 210 may store status information, where useful, for each type of media. Examples of this sort of status information include: information regarding the value remaining on a pre-paid phone card, information regarding an accumulated number of frequent flier miles, information regarding a total number of cups of coffee that have been purchased at a particular coffee shop (e.g., in connection with a buy-ten-get-one-free special), etc. The portion of the memory 210 devoted to memory storage may be divided into three sections: (1) a high-security section, (2) a medium security section, and (3) a non-secure section. The high security section may be used to store value-based or value-linked media such as debit and credit cards and certain ID information such as driver's licenses, passports, building security passes, etc. The medium security section may be used to store low-value, limited use media that may be accessed, for example, by retailers to keep track of frequent purchase credits or the like. The non-secure section may, for example, be used to store notes, membership ID records, emergency contact information, etc. Access to the information included in the various sections may require security or user authentication procedures commensurate with the indicated security level. For example, an accurate fingerprint scan

and an accurate pin code entry may be required to access the high-security section, only an accurate PIN code entry (even by the retailer) may be required to access the medium-security section, and anyone may be permitted to access the non-secure section.

The power manager 214 may comprise any of numerous devices, and the invention is not limited to any particular type of power supply/management device. The power manager may, for example, employ a flat, rechargeable, lithium battery, and associated regulator and power management software. Alternatively, the battery used may be non-rechargeable and/or coin cell-shaped. Solar powered cells may also be a viable option as at least a supplement to battery power, if not a primary source of power for the Pocket Vault 102. This may be made possible because of the typically modest on-time requirements for a Pocket Vault 102. Power management software may also assist in minimizing the power consumption of the Pocket Vault 102. Such software may, for example, invoke an auto-shutdown feature after a preference-set number of seconds, may control the level of screen back-lighting in response to feedback received from a photo-sensor that registers ambient light, and/or may provide battery charge level warnings to Pocket Vault holders.

The indicator 215 may be any device capable of generating a perceptible indication to the holder such as a bell, chime, buzzer, light, vibration, etc., and the invention is not limited to any particular type of device for accomplishing such a result. In one embodiment, for example, the indicator is a chime generator that generates a "chime" sound that can be heard by the Pocket Vault holder.

Any of a number of devices may also be used for the display 216, and the invention is not limited to any particular type of display. As mentioned above, in one embodiment, a touch-screen display may be employed such that at least a portion of the functionality of the user input device 206 may be incorporated therein. Suitable displays may, for example, include any of a black & white, gray-scaled, or color LCD display, or an LCD bi-stable display.

As mentioned above, the use of the display 216, together with the user input device 206 (which may constitute the touch-screen functionality of the display 216) permits the Pocket Vault holder to flip or scroll through the various media stored in the memory 210 in much the same way as a person flips through the contents of his or her wallet. As mentioned above in connection with the description of the indicator 215, in addition to or in lieu of the display 216, other user output devices may also be employed to provide information to the

Pocket Vault holder. For example, light emitting diodes (LEDs), a beeper or buzzer, a speech synthesizer, a vibrator, etc., may be employed in some embodiments of the Pocket Vault 102.

The token port 218 of the Pocket Vault 102 may comprise a cavity or slot in which the token 102a is retained until it is released to be used to engage in a transaction, as well as the hardware employed to secure the token 102a in place when the token 102a has not been authorized to be released. In one embodiment, the token 102a stores a unique (and possibly encrypted) chip ID which is accessible to another device only when the token 102a is successfully released form the token port 218. In addition to the elements described above, the card port 218 may include additional hardware employed in connection with properly generating or configuring the token 102a prior to its release. This hardware is discussed in more detail below in connection with Fig. 6.

The fingerprint scanner 220 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 220 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and from Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner 220 may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is employed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in Fig. 2.

Fig. 3 is a block diagram showing an example embodiment of one of the interface stations 104a-c shown in Fig. 1. The hardware employed to implement each of the stations 104a-c may be identical to the others or may be substantially different, depending on the environment in which the station 104 is to be used, as well as the functional requirements of

the particular station. Therefore, while the example embodiment described herein may be suitable for use as any of the stations, it should be appreciated that each of the stations may, in fact, be configured quite differently than the others.

As shown in Fig. 3, each interface station 104 may include both an the interface station computer 304 and a pocket vault interface unit 302. The interface station computer 304, for example, may be a standard desktop personal computer (PC), and may, as shown, comprise a controller 308, a user input device 318, a memory 320, a modem 322, and a display 324. These components are well known in the art and therefore will not be described in detail herein. The memory 320 of the interface station computer 304 may have instructions stored therein which, when executed by the controller 308, cause the controller to implement the routine described below in connection with Figs. 14-18 as well as any other software, e.g., a browser, drivers, etc., executing on the interface station computer 304.

The pocket vault interface unit 302 is coupled to the interface station computer 304 such that a controller 306 of the pocket vault interface unit 302 can communicate with the controller 308 of the interface station computer 304. The communications interface between these devices may, for example, comprise a Smartcard, Bluetooth or USB interface. As shown, in addition to the controller 306, the pocket vault interface unit 302 may comprise a transceiver 310, a docking interface 312, a finger print scanner 316, a stripe reader 315, and a memory 314. Further, although not shown in Fig. 3, the pocket vault interface unit 302 may also comprise a display and/or another device used to provide feedback to the operator, e.g., an audio indicator or LED.

The stripe reader 315 may be any conventional device for electronically reading the magnetic stripe on a token card such as a credit/debit card or drivers license. The stripe reader 315 may be used, for example, to read information from a token card so that such information can be downloaded to the network server 114 or the Pocket Vault 102.

The memory 314 may be any conventional memory suitable to store the software executed by the controller 306, as well as any data, e.g., stored fingerprint data, used in connection therewith. For example, the memory 314 of the pocket vault interface unit 302 may have instructions stored therein which, when executed by the controller 306, cause the controller 306 to implement the routine described below in connection with Fig. 13.

As with the transceiver 204 of the Pocket Vault 102, the transceiver 310 of the pocket vault interface unit 302 may be any type of transceiver (or separate transmitter and receiver)

capable of communicating with the other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may even include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface the pocket vault interface unit 302 with a Pocket Vault 102, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth.

As with the docking interface 208 of the Pocket Vault 102, the docking interface 312 of the pocket vault interface unit 302 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 312 may, for example, include a multi-pin plug adapted to mate with a receptacle used as the docking interface 208 of a Pocket Vault 102, or vice versa. The docking interface 312 may also comprise one or more implements (e.g., keys or grooves) to ensure that the plug or the like of the docking interface 208 of the Pocket Vault 102 mates correctly with the corresponding implement of the docking interface 312 when the Pocket Vault 102 and pocket vault interface unit 302 are physically mated together.

Finally, as with the fingerprint scanner 220 of the Pocket Vault 102, the fingerprint scanner 316 of the pocket vault interface unit 302 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 316 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and by Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is performed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the interface station operator. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the operator. Although not shown, the pocket vault interface unit 302 may

additionally comprise one or more user input devices enabling the operator to control or provide input to the pocket vault interface unit 302 or the software executing thereon. The fingerprint scanner 316 and/or other bio-metric scanners may, for example, have touch pad capability capabilities built into them, thereby permitting them to constitute such a user input device. Separate user input devices may also be employed.

Fig. 4 shows an example embodiment of the network server 114 shown in Fig. 1. As shown, the network server 114 may comprise one or more controllers 402, as well as a local memory 404, a database 406, and a transceiver 408 coupled thereto. The illustrated components of the network server 114 are well known, and therefore will not be described in detail. The transceiver 408 may, for example, be used to communicate with other devices in the network system 100 (Fig. 1) using a wireless network such as Bluetooth. The controller 404 may also communicate with other network devices via the Internet or a direct connection such as the type established using a dial up modem.

The local memory 404 may have instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement the routines described below in connection with Figs. 19-25 and/or Figs. 30-39. In some embodiments, the local memory 404 and/or database 406 act as a website and execute software which may be accessed by a browser or similar software module operating on a computer. One such embodiment is described below in connection with Figs. 28-39.

The database 406 may, for example, comprise a relational database, and may be used to store the majority, if not all, of the data maintained by the network server 114. The database 406 may, for example, keep a real-time record of critical reference data along with transaction histories, back-up files, and security audit trail information for key events. Examples of specific items that may be stored in the database 406 include: a list of current Pocket Vault holders and appropriate contact information for each; records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304; a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list; a list of currently authorized locations for interface stations 104 and telephone or other access lines therefor, including business information for each such location and an indication as to the type of interface station 104 it is (e.g., a validation interface station, a personal interface station, or a

commercial interface station); a list of currently authorized or registered interface station operators and the interface stations 104 with which they are associated; a list of currently authorized or registered interface stations 104, identified by chip ID and linked to the list of authorized operators therefor, as well as encrypted cookie ID information (if any) for the respective interface stations 104; authorized media data received from media issuers that has not yet been downloaded to individual Pocket Vaults 102; backup data sets for individual Pocket Vault holders; detailed transaction histories for Pocket Vault registrations indicating where each Pocket Vault 102 was shipped from and to, where each Pocket Vault 102 was registered, which authorized interface station operator conducted the registration process, when that authorized operator was added to the list of authorized operators at a particular location, who submitted the key information to add the operator, which corporate representative associated with the network server 114 met with which representative associated with the interface station in establishing each new location for a validation interface station 104a, to whom and when each Pocket Vault 102 was issued; and communication encryption protocols. Each Pocket Vault account defined on the network server 114 may be defined to support multiple Pocket Vaults 102, as well as to identify other family members who may share certain contents of the Pocket Vaults 102 (e.g., family membership in a local museum).

The network server 114 may analyze data regarding consumer transactions, and thereby accumulate demographic information. Using this information, merchants, media issuers, and/or advertisers may, for example, define targeted marketing programs, which the network server 114 may then deliver to Pocket Vault holders that meet particular demographic profiles.

Fig. 5 shows how the memory 210 of the Pocket Vault 102 (Fig. 2) may be organized (conceptually) in accordance with one embodiment of the invention. The purpose of each of the illustrated memory components will be readily understood by those skilled in the art of the invention, and therefore will not be explained in detail.

Fig. 6 is a block diagram showing an example embodiment of the token 102a shown in Figs. 1 and 2. As shown, the token 102 may be equipped with a controller 602. In the embodiment shown, the controller 602 may be selectively programmed, for example, via interface terminals 606 to generate a current in a wire loop 608 so as to generate a magnetic field about the wire loop 608 that simulates a magnetic stripe of a standard credit card-like

token. In other words, a magnetic field may be generated along the edge of the token 102a as if a magnetic stripe were present on that edge. The location of the simulated magnetic stripe on the token 102a is identified in Fig. 6 as a virtual magnetic stripe 610.

Appropriate software may be loaded onto the controller 602 (e.g., in an on-board memory of the controller 602) so as to enable the controller to generate the virtual magnetic stripe 610. When the token 102a is disposed in the token port 218, the terminals 606 of the token 102a may engage corresponding terminals of the token port 218, thereby enabling the controller 602 to be programmed appropriately. The programming of the controller 602 may be effected, for example, in response to commands from the controller 202 of the Pocket Vault 102, which commands may be generated in response to software executing on the controller 202.

As shown, the controller 602 may be powered by an appropriate resistor-capacitor (RC) circuit which stores a charge that decays over time. The RC circuit may be initially charged via the terminals 606 when the token 102a is disposed in the token port 218 and the controller 602 is being programmed. After the token 102a is removed from the token port 218, the controller 602 will remain powered only so long as sufficient charge remains stored by the RC circuit 604. Because the controller 602 can generate the virtual magnetic stripe 610 only when it is driven by an adequate power supply, the virtual magnetic stripe will disappear after the charge in the RC circuit 604 has decayed beyond a certain threshold level. Because the decay of an RC circuit is reasonably predictable, the virtual magnetic stripe 610 is disposed on the token 102a only for a finite, predetermined period of time after the token 102a is removed from the token port 218. In one embodiment, after the controller 602 loses power, the information with which it was programmed to enable it to generate the virtual magnetic stripe 610 is also lost. Therefore, the virtual magnetic stripe 610 of the token 102a cannot be used again until the controller 602 is again powered up and reprogrammed. Alternatively, the controller 602 may cut off the power to the wire loop 608 after a preset amount of time or an amount of time determined by the Pocket Vault holder (possibly within preset limits). Additionally or alternatively, the token 102a may have its own embedded chip ID, which may be accessible only when the token 102a is successfully released form the token port 218.

In some embodiments, the token 102a may possess the characteristics of a bank-issued Smartcard, either in addition to or in lieu of the virtual magnetic stripe 610.

Accordingly, the token 102a may include a specialized Smartcard chip or the controller 602 may be programmed to mimic such a chip. In any event, the token 102a may be preloaded with the bank's chip operating system (OS) and possibly customer-specific secure information. In such embodiments, the functionality of the Smartcard components may, for example, be enabled only in response to successful authentication of the Pocket Vault holder, e.g., using the fingerprint scanner 220 of the Pocket Vault 102. Therefore, the customer-specific "Smartcard" information may remain inaccessible so long as the Pocket Vault holder's identity has not been authenticated using the Pocket Vault 102.

As mentioned above, Figs. 7-12 are flow diagrams illustrating an example implementation of software that may be executed by the controller 202 of the Pocket Vault 102. As described below, this or additional proprietary software may enable menu structures, handle preference management, provide the data on and safeguard the programmability of the virtual magnetic stripe 610 (if so equipped), and ensure proper encryption data management. In one embodiment, local software for each Pocket Vault 102 and pocket vault interface station 104 may be upgraded from time to time by automatic download from the network server 114.

During execution of the routines of Figs. 7-12, various items may be displayed on the display 216, including prompts or icons regarding user input options (when a touch-screen display is employed as the display 216 or a point and click mechanism is employed herewith), and various items may also be displayed on the token 102a when the token 102a is ejected from the token port 218 of the Pocket Vault 102. Figs. 26A-P show examples of how the display 216 and the token 102a may appear as the routines of Figs. 7-12 are executed, and therefore will be discussed in connection with the description of these routines.

Fig. 7 is a flow diagram illustrating an example implementation of a primary routine 700 that may be executed by the controller 202 of the Pocket Vault 102. Instructions for the routine 700 may be stored, for example, in the "applications" section 508 of the memory 210 of the Pocket Vault 102.

As shown, the routine 700 begins at a step 702, wherein it is determined whether the Pocket Vault holder has applied his/her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102. At the step 702, the display 216 of the Pocket Vault 102 may appear as shown in Fig. 26A. That is, the display 216 may be blank at the step 702, as the Pocket Vault 102 is currently powered down.

When, at the step 702, it is determined that the holder has applied his/her fingerprint to the fingerprint scanner 220, the routine 700 proceeds to a step 704, wherein the power manager 214 powers on the Pocket Vault 102. The routine 700 otherwise waits at the step 702 until the Pocket Vault holder has applied a fingerprint to the fingerprint scanner 220. Is should be appreciated, however, that, in some embodiments, the step 702 may not represent an instruction set executed by the processor 202. Instead, the step 702 may represent the detection of the occurrence of a physical action, e.g., the activation of a hardware switch, and the power manager 214 may be activated in response to the detection of such an action, without requiring intervention by the processor 202.

After the step 704, the routine 700 proceeds to a step 706, wherein the fingerprint scanner 220 scans the applied fingerprint of the Pocket Vault holder.

After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. In one embodiment, the Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of Fig. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114, as described below.

When, at the step 708, it is determined that the Pocket Vault 102 has not yet been validated, the routine 700 proceeds to a step 710, wherein a PROCESS POCKET VAULT VALIDATION routine (described below in connection with Fig. 8) is executed.

When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212.

When, at the step 712, it is determined that the Pocket Vault has not been properly authenticated, the routine 700 proceeds to a step 714, wherein an UNAUTHORIZED HOLDER routine (discussed below in connection with Fig. 9) is executed. Figs. 26B-D show how the display 216 of the Pocket Vault 102 may appear during the UNAUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Fig. 9.

When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit

302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device.

In some embodiments, before a Pocket Vault holder is granted access to the contents of his or her Pocket Vault 102, a check may be made to ensure that the components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly, and have not been compromised. Alternatively, the operability and integrity of such components may be checked just prior to their use.

Moreover, in some embodiments, prior to granting a holder access to the contents of the Pocket Vault 102, a check may be made to ensure that the contents of the Pocket Vault 102 have been updated recently. For example, the Pocket Vault 102 may forbid its holder from accessing its contents if the Pocket Vault 102 has not been updated at least 48 hours (or some other specified time period) prior to the attempted use. Updating of the Pocket Vault 102 may be accomplished, for example, using the synchronization or backup and recovery methods described herein.

After the step 713, the routine 700 proceeds to a step 716, wherein it is determined whether the Chameleon Card (i.e., the token 102a) is presently on-board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the card port 218 of Fig. 2).

When, at the step 716, it is determined that the token 102a is not on-board the Pocket Vault 102, the routine 700 proceeds to a step 718, wherein the Pocket Vault holder is informed that the Chameleon Card is not on board, and is asked whether he/she wants to engage in a non-card transaction (i.e., a transaction not involving the token 102a).

After the step 718, the routine 700 proceeds to a step 720, wherein it is determined whether the holder has selected to engage in a non-card transaction.

When, at the step 720, it is determined that the holder has selected not to engage in a non-card transaction, routine 700 returns to the step 716 (described above), wherein it is again determined whether the Chameleon Card is on board the Pocket Vault 102. Therefore, the holder is permitted to engage in a transaction involving the Chameleon Card only when it has been confirmed that the Chameleon Card is on board the Pocket Vault 102.

When, at the step 720, it is determined that the holder has selected to engage in a non-card transaction, the routine 700 proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed.

When, at the step 716, it is determined that the Chameleon Card is on-board the Pocket Vault 102, the routine 700 also proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed. Figs. 26G-N and 26P show how the display 216 of the Pocket Vault 102 and the token 102a ejected therefrom may appear (when employed) during the AUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Figs. 10 and 11.

After each of the steps 710, 714, and 720 (only one of which is executed during each iteration of the routine 700), the routine 700 proceeds to a step 724, wherein the VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed. Fig. 26O shows how the display 216 of the Pocket Vault 102 may appear during the VERIFY CARD RETURN routine, and therefore is also discussed below in connection with Fig. 12.

After the step 724, the routine 700 proceeds to a step 726, wherein the screen of the display 216 is caused to flash to indicate that the Pocket Vault 102 is being shut down.

After the step 726, the routine 700 proceeds to a step 728, wherein the Pocket Vault 102 is powered down.

After the step 728, the routine 700 returns to the step 702, wherein the Pocket Vault 102 again waits for a fingerprint to be applied to the fingerprint scanner 220, and wherein the display 216 may again appear as shown in Fig. 26A.

Fig. 8 is a flow diagram illustrating an example embodiment of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7 (step 710).

As shown, the routine 710 begins at a step 801, wherein the holder is informed (e.g., on the display 216) that the Pocket Vault 102 is not currently validated, and that the holder must interface the Pocket Vault 102 with an interface unit 302 of an appropriate interface station 104 (e.g., a validation interface station 104a) if the holder desires to validate the Pocket Vault 102.

After the step 801, the routine 710 proceeds to step 802, wherein it is determined whether the Pocket Vault 102 has been interfaced with an appropriate interface unit 302.

When, at the step 802, it is determined that the pocket vault 102 has not yet been interfaced with an appropriate interface unit 302, the routine 710 returns to the step 801 (discussed above).

When, at the step 802, it is determined that the Pocket Vault 102 has been interfaced with an appropriate interface unit 302, the routine 710 proceeds to a step 803, wherein it is determined whether the fingerprint memory, e.g., the write-once memory 212, is empty.

When, at the step 803, it is determined that the fingerprint memory is empty, the routine 710 proceeds to a step 804a, wherein the holder is prompted to apply a fingerprint from one finger of his or her left hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806a – 810a, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After the steps 806a-810a, the routine proceeds to a step 804b, wherein the holder is prompted to apply a fingerprint from one finger of his or her right hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806b – 810b, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After completing the steps 806b-810b, when a total of six fingerprints have been stored in memory, the routine 710 proceeds to a step 812, wherein an encrypted message including the pocket vault ID is transmitted to the interface unit 302, for ultimate transmission to the network server 114.

When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (Fig. 7) matches one of the stored fingerprints.

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does match one of the stored fingerprints, the routine 710 proceeds to the step 812 (discussed above).

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does not match any of the stored fingerprints, the routine 710 proceeds to a step 818, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215) is generated to inform the holder that the validation attempt was unsuccessful.

After the step 818, the routine 710 terminates.

After the step 812, the routine 710 waits at steps 814 and 816 to determine whether an encrypted message including validation information (e.g., a PKI certificate) has been received from the interface unit 302. This encrypted validation information may, for example, be received by the Pocket Vault 102 via either the docking interface 208 or the transceiver 204 of the pocket vault interface unit 302 of a validation interface station 104a. As discussed in more detail below, this encrypted validation information may, for example, be generated by the network server 114 and forwarded to the pocket vault interface unit 302 of a validation interface station 104a (via the interface station computer 304 of the validation interface station 104a) after certain conditions have been met. The network server 114 may therefore ultimately determine whether each Pocket Vault 102 is permitted to receive this validation information.

When, at the step 816, it is determined that the time-out period has elapsed, the routine 710 proceeds to the step 818 (discussed above).

When, at the step 814, it is determined that encrypted validation information has been received before the timeout period of the step 816 has elapsed, the routine 710 proceeds to a step 820, wherein the validation information is stored in memory.

After the step 820, the routine 710 proceeds to a step 822, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215 of the Pocket Vault 102) is generated to inform the holder that the Pocket Vault 102 has been successfully validated.

After the step 822, the routine 710 terminates.

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7 (step 714).

As shown, the routine 714 begins at a step 902, wherein a menu is displayed on the display 216 that permits the holder to select one of several options: (1) TRY AGAIN, (2) POCKET VAULT RETURN INFORMATION, (3) EMERGENCY INFORMATION, or (4) END SESSION. Fig. 26B shows how the display 216 may appear when the step 902 is reached. As shown, textual information and/or icons representing the various menu options may be displayed to the holder.

After the step 902, the routine 714 proceeds to a step 904, wherein the routine 714 waits for one of the displayed menu items to be selected by the holder (e.g., when the holder touches the location on the screen of the display 216 at which the menu item is displayed).

After one of the menu items has been selected at the step 904, the routine 714 proceeds to a step 906, wherein it is determined whether the TRY AGAIN option was selected. By selecting TRY AGAIN, the holder may request that the holder again be permitted to attempt to access the secure contents of the Pocket Vault 102 by reapplying the holder's fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the user has selected the TRY AGAIN option, the routine 714 proceeds to a step 912, wherein it is determined whether this is the third sequential time that the scanned fingerprint has failed to match the fingerprint stored in memory.

When, at the step 912, it is determined that three sequential failed matches have occurred, the routine 714 proceeds to a step 914, wherein certain security precautions are taken in light of the multiple failed attempts to match the holder's fingerprint with that stored in the Pocket Vault 102. For example, when multiple failed matches have occurred, the Pocket Vault's secure memory may be erased, a security alert message may be broadcast by the transceiver 204 and/or any other prudent steps may be taken to ensure that an unauthorized user does not access the Pocket Vault's sensitive contents.

After the step 914, the routine 714 terminates.

When, at the step 912, it is determined that this is not the third consecutive time that the holder's fingerprint has failed to match that stored in the Pocket Vault's memory, the routine 714 terminates, and the holder may then again attempt (at the step 702) to access the Pocket Vault 102 by reapplying his/her fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the TRY AGAIN option has not been selected, the routine 714 proceeds to a step 908, wherein it is determined whether there exist any nested menu items for the menu item selected at the step 904.

When, at the step 908, it is determined that nested menu items do exist for the selected menu item, the routine 714 proceeds to a step 910, wherein the nested menu items for the selected menu item are displayed to the holder on the display 216.

After the step 910, the routine 714 returns to the step 904, wherein the routine 714 again waits for the holder to select one of the displayed menu items.

When, at the step 908, it is determined that no nested menu items exist for the selected menu item, the routine 714 proceeds to a step 916, wherein it is determined whether the END SESSION option has been selected.

When, at the step 916, it is determined that the END SESSION option has been selected, the routine 714 terminates.

When, at the step 916, it is determined that the END SESSION option has not been selected, the routine 714 proceeds to a step 918, wherein the information, if any, for the selected menu item is displayed to the holder on the display 216. Because the step 918 is reached only after a failed attempt to match the holder's fingerprint with that stored in the memory of the Pocket Vault 102, the information displayed at the step 918 may, for example, include information as to where the Pocket Vault 102 may be returned if it is found by someone other than the Pocket Vault holder (see Fig. 26C), or may be emergency information regarding the holder such as the holder's blood type, allergies, persons to contact in case of an emergency, etc. (see Fig. 26D). It should be appreciated that any of a number of non-secure media may be selected using the menu access routine discussed above in connection with steps 904-910, and may be displayed to the person accessing the Pocket Vault 102, regardless of the identity of that person. Of course, this non-secure information may be information that the holder would not mind falling into the hands of a stranger should the holder misplace or have his/her Pocket Vault 102 stolen.

After the step 918, the routine 714 proceeds to a step 920, wherein after a delay of a certain period of time (e.g., thirty seconds), the holder is prompted to reapply his/her fingerprint within a particular period of time (e.g., ten seconds) to avoid shut down of the Pocket Vault 102.

After the step 920, the routine 714 proceeds to a step 922, wherein it is determined whether a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds.

When, at the step 922, it is determined that a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 returns to the step 918 (discussed above), wherein the selected information is again displayed to the user.

When, at the step 922, it is determined that a fingerprint has not been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 terminates.

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine of Fig. 7 (step 722).

As shown, the routine 722 begins at a step 1002, wherein it is determined whether an advertisement is scheduled for display on the Pocket Vault 102. Information regarding whether certain advertisements are to be displayed by the Pocket Vault 102 may have been

uploaded, for example, from the personal interface station 104b in response to the holder previously interfacing the Pocket Vault 102 with the personal interface station 104b to synchronize the contents of the Pocket Vault 102 with information stored on the network server 114. The advertiser 108 (Fig. 1) may, for example, have made arrangements with the company operating the network server 114 to have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b.

When, at the step 1002, it is determined that an advertisement has been scheduled, the routine 722 proceeds to a step 1004, wherein the scheduled advertisement is displayed, for example, for approximately two seconds. Fig. 26I shows an example of how the display 216 may appear when such an advertisement is displayed.

After the step 1004, the routine 722 proceeds to a step 1006, wherein a "welcome screen" is displayed for a brief period (e.g., one second). Fig. 26G shows an example of how the display 216 may appear when such a welcome screen is displayed.

When, at the step 1002, it is determined that an advertisement is not scheduled, the routine 722 proceeds immediately to the step 1006, and no advertisement is displayed to the Pocket Vault holder.

After the step 1006, the routine 722 proceeds to a step 1008, wherein it is determined whether a "preferred" menu has been selected or pre-set for initial display to the Pocket Vault holder.

When, at the step 1008, it is determined that a preferred menu has been selected or pre-set, the routine 722 proceeds to a step 1012, wherein the display 216 fades to the preferred menu. Figs. 26H and 26J show examples of how the display 216 may appear when such a preferred menu is displayed. In the example of Fig. 26H, the preferred menu immediately shows the holder's preferred credit card as the selected menu item. Should the holder opt to use this media to engage in a transaction, the holder can simply choose the media directly. Alternatively, the holder may opt to access the HOME menu or other menu items by selecting appropriate icons displayed on the screen. In the example of Fig. 26J, the preferred menu immediately shows, perhaps, a selected group of the holder's most frequently used menu items.

When, at the step 1008, it is determined that a preferred menu has not been selected or pre-set, the routine 722 proceeds to a step 1010, wherein the display 216 fades to a standard

HOME menu of secure items. Fig. 26L shows an example of how the display 216 may appear when the HOME menu is displayed.

After either one of the steps 1010 and 1012 has been executed, the routine 722 proceeds to a step 1014, wherein the routine 722 waits for the holder to select one of the displayed menu items.

When, at the step 1014, it is determined that the holder has selected a particular menu item, the routine 722 proceeds to a step 1016, wherein it is determined whether the holder has selected to enter or return to the HOME menu.

When, at the step 1016, it is determined that the holder has selected the HOME option, the routine 722 proceeds to the step 1010, wherein the HOME menu of secure items is displayed.

When, at the step 1016, it is determined that the holder has selected a menu item other than the HOME option, the routine 722 proceeds to a step 1018, wherein it is determined whether there exist any nested menu items for the selected menu item.

When, at the step 1018, it is determined that nested menu items do exist for the selected menu item, the routine 722 proceeds to a step 1020, wherein the nested menu items for the selected menu item are displayed. Thus, the holder may work his/her way through various layers of menu items until the desired menu item is reached. It should be appreciated that the menu items on the higher-level layers therefore may be categorized so as to enable the holder to quickly reach the desired media or other menu option.

When, at the step 1018, it is determined that no nested menu items exist for the selected menu item, the routine 722 proceeds to a step 1022, wherein it is determined whether the holder has selected a media from among the available menu items.

When, at the step 1022, it is determined that the holder has not selected a media, the routine 722 proceeds to a step 1040, wherein information relating to the selected non-media item may be displayed, or some other function may performed in accordance with the holder's selection. A non-media menu selection may involve, for example, preference settings for certain functional aspects of the Pocket Vault 102, e.g., whether the holder has a preferred secure menu (see step 1008). Preferences for the services or the device can be selected and, as appropriate, distributed to the Pocket Vault 102 either on the spot or the next time the Pocket Vault 102 is interfaced with an appropriate interface station 104. Preferences may, for example, include definition of home pages, connection of secure and non-secure

media, order of media presentment, sort orders, user interface options, synchronization defaults, etc. Preferences that determine which items are displayed on the home page or on other pages may be defined. For example, a Pocket Vault holder may set up three preference sets: one for "business," one for "personal," and one for "vacation." The "personal" and "business" preference sets may be set to be effective at different times of the day and/or different days of the week. The "vacation" preference set may be made effective for specific blocks of time determined by the Pocket Vault holder, possibly overriding the normal timing of the "personal" and "business" sets. The Pocket Vault holder may choose to establish the various preference settings based on his or her judgment or he or she may choose to allow the network server 114, supported by various databases, knowledge of the Pocket vault holder's various media and goals set by the Pocket Vault holder (e.g., minimize interest cost on credit cards or maximize frequent flyer miles, etc.), to determine optimal media use patterns and resulting media menu contents for a particular Pocket Vault holder. Preferences may also be defined between media that will link them for: (a) affiliate credits (like frequent flyer miles) that may be automatically presented to a merchant and tracked for a holder, (b) available discounts afforded by a membership (like senior citizen or AAA discounts), and/or (c) process improvement purposes (e.g., when information needs to be presented in a certain order to work properly). For example, a linkage preference may facilitate presentation of a discount card before presentation of a payment card when buying groceries.

After the step 1040, the routine 722 proceeds to a step 1042, wherein the holder is prompted either to END the session, or to return to the HOME menu.

After the step 1042, the routine 722 proceeds to a step 1044, wherein it is determined whether the holder has opted to END the session or to return to the HOME menu.

When, at the step 1044, it is determined that the holder has selected to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1044, it is determined that the holder has opted to END the session, the routine 722 terminates.

When, at the step 1022, it is determined that the holder has selected a media from the displayed menu items, the routine 722 proceeds to a step 1024, wherein the selected media is displayed to the holder on the display 216. The selected media may, for example, be a particular credit card, in which case the name of the credit card and/or the logo for the credit

card and any preferred advertisement, specials, etc., for the selected media may be displayed to the holder as well.

After the step 1024, the routine 722 proceeds to a step 1026, wherein the holder is prompted to choose to: (1) EJECT the card, (2) to invoke a WIRELESS transaction, or (3) to return to the HOME menu.

After the step 1026, the routine 722 proceeds to a step 1028, wherein it is determined which of these three options has been selected by the holder.

When, at the step 1028, it is determined that the holder has opted to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1028, it is determined that the holder has selected the EJECT card option, the routine 722 proceeds to a step 1032, wherein it is determined whether the Chameleon Card is on board the Pocket Vault 102 (i.e., whether the token 102a is disposed in the token port 218).

When, at the step 1032, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 722 proceeds to a step 1034, wherein the holder is informed that the Chameleon Card is not on board the Pocket Vault 102.

After the step 1034, the routine 722 proceeds to the step 1026 (discussed above).

When, at the step 1032, it is determined that the Chameleon Card is on board the Pocket Vault 102, the routine 722 proceeds to a step 1036, wherein the PROCESS CARD TRANSACTION routine (discussed below in connection with Fig. 11) is executed.

After the step 1036, the routine 722 proceeds to a step 1038, wherein the VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed.

After the step 1038, the routine 722 proceeds to the step 1042 (discussed above).

When, at the step 1028, it is determined that the holder has opted to invoke a wireless transaction, the routine 722 proceeds to a step 1030, wherein the wireless transaction involving the selected media is executed. This wireless transaction may be invoked, for example, using the transceiver 204 of the Pocket Vault 102 to communicate with the transceiver 310 (Fig. 3) of a commercial interface station 104c (Fig. 1) over a wireless network, such as Bluetooth. As mentioned above, in embodiments that permit wireless transactions, a check of the wireless components may be made (e.g., verifying that an internal antenna (not shown) is in place and connected, and that related circuitry is not defeated or compromised in any way), prior to granting the holder access to the contents of the Pocket

Vault 102. Alternatively, such a check may be made in response to such a wireless transaction being requested, e.g., at the step 1030.

After the step 1030, the routine 722 proceeds to the step 1042 (discussed above).

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine of Fig. 10 (step 1036).

As shown, the routine 1036 begins at a step 1102, wherein the Chameleon Card is configured to carry the selected media, and is ejected from the card port 218 (Fig. 2). As discussed above, the token 102a may be configured to carry the selected media in any of a number of ways, and the invention is not limited to any particular type of configuration technique. The card may be configured, for example, by causing it to generate a simulated magnetic stripe for a limited period of time, by causing it to have a bar code disposed on it for a limited period of time, or simply by causing a card number to be visibly disposed on it for a limited period of time. One example of technology that may be employed to cause information to appear temporarily on the token 102a is available from E-ink (www.Eink.com). It should be appreciated, of course, that the card need not be temporarily configured in all embodiments, and may alternatively be configured in a more permanent manner in some embodiments.

After the step 1102, the routine 1036 proceeds to a step 1104, wherein the selected media is grayed out on the display 216 to indicate that the media is currently in use by the Chameleon Card. When the selected media is grayed out, the Pocket Vault's ability to configure another Chameleon Card with the grayed out media may also be disabled. Therefore, in such an embodiment, even if the Pocket Vault holder had an additional Chameleon Card available, the Pocket Vault 102 would be incapable of loading that media onto that Chameleon Card.

After the step 1104, the routine 1036 proceeds to a step 1106, wherein it is determined whether the selected media has stored value associated with it. The selected media may, for example, represent a pre-paid calling card from which value is deducted each time the media is used in a particular transaction, or a frequent flier card to which value (e.g., miles) is added in connection with each airline ticket purchased.

When, at the step 1106, it is determined that the selected media does have stored value associated with it, the routine 1036 proceeds to a step 1108, wherein a "stored value

flag" (discussed below in connection with step 1126 of routine 1036 (Fig. 11) and step 1212 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1108, the routine 1036 proceeds to a step 1110, wherein it is determined whether the holder has set a default option so as to permit the holder to maintain expense records by recording transactions into registers assigned to expense categories.

When, at the step 1106, it is determined that the selected media does not have stored value associated with it, the routine 1036 proceeds immediately to the step 1110.

When, at the step 1110, it is determined that the holder has not opted for the ability to maintain expense records, the routine 1036 terminates.

When, at the step 1110, it is determined that the holder has opted for the ability to maintain expense records, the routine 1036 proceeds to a step 1112, wherein the holder is prompted to decide whether to record the currently-pending transaction.

After the step 1112, the routine 1036 proceeds to a step 1114, wherein it is determined whether the holder has opted to record the pending transaction.

When, at the step 1114, it is determined that the holder has not opted to record the transaction, the routine 1036 terminates.

When, at the step 1114, it is determined that the holder has opted to record the transaction, the routine 1036 proceeds to a step 1116, wherein a menu including a number of options involving expense categories are displayed to the holder on the display 216.

After the step 1116, the routine 1036 proceeds to a step 1118, wherein the routine 1036 waits for the holder to select one of the displayed menu options.

When, at the step 1118, it is determined that the holder has selected a menu item, the routine 1036 proceeds to a step 1120, wherein it is determined whether the holder selected the SKIP RECORD option, e.g., when the holder has changed his or her mind and opted not to record a particular transaction.

When, at the step 1120, it is determined that the holder has selected the SKIP RECORD option, the routine 1036 terminates.

When, at the step 1120, it is determined that holder has not selected the SKIP RECORD option, the routine 1036 proceeds to a step 1122, wherein it is determined whether any nested menu items exist for the selected menu item.

When, at the step 1122, it is determined that nested menu items do exist for the selected menu item, the routine 1036 proceeds to a step 1124, wherein the nested menu items are displayed to the holder on the display 216.

After the step 1124, the routine 1036 returns to the step 1118 (discussed above).

When, at the step 1122, it is determined that no nested menu items exist for the selected menu item, the routine 1036 proceeds to a step 1126, wherein it is determined whether the stored value flag was set to TRUE at the step 1108 (discussed above).

When, at the step 1126, it is determined that the stored value flag is set to TRUE, the routine 1036 proceeds to a step 1128, wherein a "record stored value transaction" flag (discussed below in connection with step 1216 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1128, the routine 1036 terminates.

When, at the step 1126, it is determined that the "stored value" flag is not TRUE, the routine 1036 proceeds to a step 1130, wherein the holder is prompted to enter a dollar amount to be recorded for the transaction.

After the step 1130, the routine 1036 proceeds to a step 1132, wherein the routine 1036 waits for the holder to enter a transaction amount. After the holder has entered a transaction amount, the routine 1036 proceeds to a step 1134, wherein a "transaction summary approval" menu is displayed to the holder on the display 216. In the example shown, this menu permits the holder to select (1) to APPROVE the recordation, (2) to change the expense CATEGORY for the transaction, or (3) to change the AMOUNT to be recorded.

After the step 1134, the routine 1036 proceeds to a step 1136, wherein it is determined which of the menu items displayed in step 1134 the holder has selected.

When, at the step 1136, it is determined that the holder has selected to change the transaction AMOUNT, the routine 1036 returns to the step 1130 (discussed above).

When, at the step 1136, it is determined that the holder has opted to change the expense CATEGORY, the routine 1036 returns to the step 1116 (discussed above).

When, at the step 1132, it is determined that the holder has opted to APPROVE the recordation, the routine 1036 proceeds to a step 1138, wherein the entered transaction amount is added to the expense register for the selected category, and the balances associated therewith are updated accordingly.

After the step 1138, the routine 1036 terminates.

Fig. 12 is a flow diagram illustrating the VERIFY CARD RETURN routine of Fig. 7 (step 724).

As shown, the routine 724 begins at a step 1202, wherein it is determined whether the Chameleon Card is currently on board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the token port 218).

When, at the step 1202, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 724 proceeds to a step 1204, wherein the holder is prompted to return the Chameleon Card to the token port 218 (see Fig. 260).

After the step 1204, the routine 724 proceeds to a step 1206, wherein it is determined whether a timeout period (e.g., ten seconds) has elapsed since the user was last prompted to return the Chameleon Card to the token port 218.

When, at the step 1206, it is determined that the timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1206, it is determined that the timeout period has elapsed, the routine 724 proceeds to a step 1208, wherein the user is again prompted to return the Chameleon Card, this time with an audio indication (e.g., a "chime" sound generated by the indicator 215 of Fig. 2).

After the step 1208, the routine 724 proceeds to a step 1210, wherein it is determined whether an extended timeout period (e.g., 10 minutes) has elapsed since the user was first prompted to return the Chameleon Card to the token port 218.

When, at the step 1210, it is determined that the extended timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1210, it is determined that the extended timeout period has elapsed, the routine 724 terminates.

When, at the step 1202, it is determined that the Chameleon Card is on board the Pocket Vault 102 (i.e., the token 102a is disposed within the token port 218), the routine 724 proceeds to a step 1212, wherein it is determined whether the "stored value" flag was set to TRUE in step 1108 of the routine 1036 (Fig. 11).

When, at the step 1212, it is determined that the "stored value" flag is not TRUE, the routine 724 terminates.

When, at the step 1212, it is determined that the "stored value" flag is TRUE, the routine 724 proceeds to a step 1214, wherein the stored value for the selected media is updated based on the amount deducted from the Chameleon Card during its use.

After the step 1214, the routine 724 proceeds to a step 1216, wherein it is determined whether the "record stored value transaction" flag was set to TRUE in the step 1128 of the routine 1036 (Fig. 11).

When, at the step 1216, it is determined that the "record stored value transaction" flag is FALSE, the routine 724 proceeds to a step 1222, wherein the "stored value" flag is set to FALSE.

When, at the step 1216, it is determined that the "record stored value transaction" flag is TRUE, the routine 724 proceeds to a step 1218, wherein the dollar amount of the transaction is added to the selected expense register (i.e., the expense register selected at the step 1118 of the routine 1036 (Fig. 11)). The dollar amount entered is determined based on the dollar amount that was deducted from the stored value on the Chameleon Card as a result of the transaction.

After the step 1218, the routine 724 proceeds to a step 1220, wherein the "record stored value transaction" flag is set to FALSE.

After the step 1220, the routine 724 proceeds to the step 1222 (discussed above)

After the step 1222, the routine 724 terminates.

In addition to a routine such as that discussed above in connection with Figs. 7-12, certain software enhancements may also be disposed in the memory 210 of a Pocket Vault 102 for use with the controller 202. One such software enhancement involves the use of "system preference file" software. This software may establish certain preferences that cannot be altered on the Pocket Vault 102 by the holder, and which may be stored in encrypted form, along with certain information regarding value-based media. For example, Pocket Vaults 102 may be sold with a choice of two or three advertising profiles. During the Pocket Vault registration and validation process (described below), an encrypted system preference file may be created that indicates whether the device was, for example, subject to a "Premium," "Plus" or "Base" profile status. This status may have been selected, for example, on the Pocket Vault 102 itself, or using one of the interface stations 104a-c when the Pocket Vault 102 was interfaced therewith.

Under the "Premium" profile, the Pocket Vault 102 may be advertising-free, but cost a significant amount. Under the "Plus" profile, the Pocket Vault 102 may display only advertising related to shops or services you currently patronize, but cost significantly less than the "Premium" version. Under the "Base" profile, the Pocket Vault 102 may have a variety of advertising on a regular basis, subject only to network "saturation effectiveness" limitations, and the Pocket Vault 102 may be free, or nearly so (e.g., a small purchase charge to generate in-store revenue for the retailer may be charged).

A holder's choice about participation in specific promotional campaigns linked to the holder's buying behavior may also be part of the registration process and affect retail pricing. Once chosen, the network server 114 may send a message to the Pocket Vault 102, e.g., via the validation interface station 104a, and direct the storage of necessary encrypted information on the Pocket Vault 102 (e.g., "Buyer Profile Participant").

The advertising and marketing choices may be changed at a date after purchase and result in a changed set of costs (either credits or debits) to the Pocket Vault holder. Other system preference data may include the "saturation effectiveness" limitations on the amount of advertising that can appear during any given single use window (a particular period during which the device is powered on), any given hour, any given day and/or any given month. The limitations may control both the number of advertisements permitted and the amounts of advertisement time permissible (e.g., seconds per advertisement), by category (e.g., such limitations may, for example, based on categories of advertisements be imposed general advertising, advertising from retailers that the Pocket Vault holder already patronizes and advisory notices from the network server 114. For example, these limits may be set to balance the need for advertising revenue with the need to not overwhelm or annoy Pocket Vault holders. This preference file may, for example, limit all advertising to one advertisement per "on-session," two advertisements per hour, four advertisements per day and/or twenty advertisements per month. General advertisements might get priority claim on this time up to a set limit (say 75% of all advertisement time), with targeted advertisements next, and advisory messages last.

Another software enhancement that may be employed is software used for preference file management. Such "preference file management" software may, for example, include a default file which is periodically updated from the network server 114, and a Pocket Vault holder custom file. Using this software, the holder may, for example, be able to modify: (1)

the initial on-screen backdrop and message greeting; (2) the menu structure and media order within menu screens; (3) some (but not all) of the bio-metric input requirement parameters; (4) the amount of on-time after the bio-metric data is confirmed (within pre-set limits); (5) the ability to conceal all or part of the credit or debit account information on the Chameleon Card display area; (6) the normal restaurant tip percentage; (7) the links between certain media; and/or oversight preference restrictions.

For example, some of the menu tree structures for the Pocket Vault 102 may be set by the holder. This may include the sequence in which certain screens appear (e.g., debit screens before credit screens), among credit screens (e.g., Visa before MasterCard) and media order-of-appearance within a screen (e.g., FirstCard Visa before ChaseVisa).

Generally, a retailer does not need to see a credit or debit account number, while the approving entity contacted on the dialup modem does. Today, credit and debit cards have this information embossed on the card and recorded in the magnetic stripe on the back of the card. If the magnetically encoded information is unreadable due to mechanical wear of the magnetic stripe or for other reasons, the embossed image can always be read by the clerk and manually keyed in. There is no way for this embossing to disappear when it is not needed and appear at just the right time, either with a standard card or a Smartcard. As a result, such numbers are generally in view and this visibility may lead to fraud. In one embodiment, the Pocket Vault 102 may be programmed to conceal this number, unless prompted to the contrary by the holder. A retailer may confirm the kind of credit or debit being presented and the full name on the card, without having to see or be told the account number. On the rare occasion when the number itself is needed, the holder may, for example, repeat the bio-metric input to the Pocket Vault 102 to reveal the card account number. If placed in the personal interface station 104c, such account numbers may be automatically revealed (e.g., through detection of an encrypted cookie on the interface station computer 304 of the personal interface station 104c).

If the holder establishes a preferred tip percentage, this preferred tip amount may be automatically applied to restaurant checks. This may eliminate a step in restaurant check close-out and reduce the hassle of calculating an appropriate tip and eliminate the need for waitstaff to return to pick up the credit receipt with the tip.

The holder may also choose to link certain media on the Pocket Vault 102 to reduce selection tasks at the point-of-transaction. For example, the holder may link certain credit or

debit cards to certain frequent buyer ID cards, thereby enabling the holder to pick a grocery store frequent buyer card (which would be linked to a debit card and brought up automatically after the grocery store card).

At the point of registration or issuance, a Pocket Vault holder may be asked if there is to be any transaction oversight security. If the answer is yes, a second bio-metric input may be required from the individual endowed with that oversight role. For example, a parent may choose to get a Pocket Vault 102 for a child or other relative who may lack certain fiscal discipline. At issuance, and prior to any credit or debit media being added to the Pocket Vault 102, the oversight authority may need to be established. The person having such oversight authority may then have sole access to a profile of transaction preference data. The person having the oversight authority may therefore create and modify this profile any time after issuance. This data set may limit one or more of the following: (1) debit and credit transaction dollar volume per day, per week and/or per month; (2) certain purchase restrictions such as the types of retailers to whom payments are permitted, such as exclusion of gambling establishments or liquor stores; and (3) geographic restrictions such as payments within 10 miles of a son's or daughter's college campus, but not beyond).

Another software enhancement that may be employed is software for managing media image libraries. Every media image sent to the display 216 may actually be a composite of from two to five layers of graphics files. Layers one, two and four may, for example, be stored in media library files while layers three and five may include text and data files stored in memory on the Pocket Vault 102. For example, a credit card image may comprise separate layers for: (1) the standard credit card background and icon; (2) the issuing bank's overlay icons and text; (3) the individual's account number; and (4) customized advertising from the issuing bank and/or credit card company.

Layering the image in this fashion may minimize data transmission requirements, reduce memory storage requirements, and speed up screen display. For example, Pocket Vaults 102 may be preloaded at point of manufacture with background images of the top ten credit images, three passport images (e.g., EU, US, Japan), and a handful of other globally-relevant backgrounds. When, for example, a Pocket Vault holder living in Boston initially registers a device, it may trigger downloading of the top five additional background images prevalent in that area. When the individual applies for and is electronically issued a new credit card over the network system 100, the download from the network server 114 may

include a second layer credit card company overlay for the credit card, along with the third layer of account and name information, and the fourth layer of the most recent customized advertisement from the credit card company related to a seasonal promotion of card usage.

The advertisement layer may be temporary in nature. This layer may, for example, remain on-screen for a given number of seconds, predetermined by the time period of the advertisement paid for by the advertiser. Underneath such an advertisement, a fifth layer of Pocket Vault holder-determined data may appear, also for a temporary period, in this case for privacy reasons and for a period set by the holder. This positioning of the holder's data below the advertising data increase the value of the advertisement time, since holders will be likely to view the display 216 awaiting the appearance of their data, which may also remain on-screen for only a set number of second. For example, such holder-specific data may include the last date of the next billing period, or the total charges since the last billing period on this particular card or on all of the holder's credit cards. Such balance information may be generated, for example, by the financial management software. The initial on-screen image may also be layered, for example, with a market-tailored backdrop and a sign-on message, both of which possibly being modifiable could be modified by the appropriate setting of user preferences.

Another software enhancement that may be employed is software to manage memos. Certain screen choices may, for example, result in the viewing of memos created by and for the Pocket Vault holder. These memos may be written on a home PC and transferred to a Pocket Vault 102 when the Pocket Vault 102 is interfaced with the personal interface station 104c for an update/download session. Alternatively, such memos may be created on the Pocket Vault 102 using a screen-based keyboard function similar to that of a Palm Pilot. The memo template software may provide certain standard backgrounds and layouts to support this feature. This feature may help to eliminate the need for scraps of various notes now found in most wallets.

Yet another software enhancement that may be employed is software to manage advertising messages. Such advertising message management software may, for example, perform several noteworthy functions: (1) limiting the appearance of advertising in accordance with the advertising profile (e.g., stored in the network server 114) of the particular Pocket Vault holder; (2) limiting the appearance of advertising to a certain number of times per on-session, per hour, per day, per week and/or per month; (3) tracking the

number of times each advertisement appears since the last download/update session (since the number of on-sessions during any period will govern the number of opportunities certain advertisements have to run, this tracking may be necessary to enable billing of advertisers for actual advertisement exposure levels; (4) generating reminder advertisements for frequent buyer cards (e.g., a message such as "Ten weeks since your last car wash! One more and the next is free!"); and (5) tracking the effectiveness of advertising through linkage to the transaction files (e.g., the ability to build more accurate, comprehensive buying profiles since all of an individual's media are now "under one roof").

Another software enhancement that may be employed is software to process transaction data. Such transaction processing software may, for example, include the ability to track total outstanding transactions on particular media and compare those to media limits at the time of the next transaction, along with date validity of the media. If a particular piece of media is no longer valid, selection of this item from a menu may produce a message such as "expired," or "requires update to extend period of validity," or "payment of balance required before re-use."

Another software enhancement that may be employed is software to manage frequent buyer data. Such frequent buyer data management software may, for example, track purchases at stores with frequent buying programs that participate in the network system 100. This software may also indicate any frequent buyer credits that are about to expire or create advertisements that remind their Pocket Vault holders that they are about to qualify for a free item. For example, a tenth gasoline purchase at a service station/car wash may generate a message indicating that the holder is "now entitled to free car wash."

Yet another software enhancement that may be employed is software for managing financial information. This type of software may, for example, enable easy download advertisements into personal finance software used by some PC owners. It may also support certain on-board functionality in the Pocket Vault, such as charge card management, automatically shifting from the preferred credit card to another credit card, for example: (1) when a transaction would cause a credit limit to be exceeded, (2) when using a different card would lengthen the time after which actual payment would be due, (3) when using another card would garner desired contest eligibility, or maximize cash back points for a particular period, and/or (4) when use of another card would preclude having to pay annual dues.

Another software enhancement that may be employed is Global Positioning Software. Integration of this functionality with memo information and frequent buyer information may induce visits to nearby stores at convenient times to take advantage of sales, frequent buyer credits, etc.

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine 1300 that may be executed by the controller 306 of the pocket vault interface unit 302 (Fig. 3).

As shown, the routine 1300 begins at a step 1346, wherein it is determined whether a card has been swiped through the stripe reader 315 of the interface unit 302.

When, at the step 1346, it is determined that a card has been swiped, the routine 1300 proceeds to a step 1348, wherein information from the swiped card read by the stripe reader 315 is transmitted to the interface station computer 304.

After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match).

When, at the step 1346, it is determined that a card has not been swiped, the routine 1300 proceeds directly to the step 1302 (discussed above).

When, at the step 1302, it is determined that such a first encrypted message has not been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1338, wherein it is determined whether any encrypted information and/or commands have been received from the interface station computer 304.

When, at the step 1338, it is determined that information and/or commands have been received from the interface station computer 304, the routine 1300 proceeds to a step 1340, wherein the received information and/or commands are forwarded to the Pocket Vault 102.

After the step 1340, the routine 1330 proceeds to a step 1342, wherein it is determined whether any information and/or commands have been received from the Pocket Vault 102.

When, at the step 1338, it is determined that no information or commands have been received from the interface station computer 304, the routine 1300 proceeds directly to the step 1342 (discussed above).

When, at the step 1342, it is determined that information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1344, wherein the received information and/or commands are forwarded to the interface station computer 304.

After the step 1344, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1342, it is determined that no information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds directly to the step 1346.

When, at the step 1302, it is determined that a first encrypted message including a Pocket Vault ID has been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1304, wherein the first encrypted message is forwarded to the interface station computer 304 (Fig. 3).

After the step 1304, the routine 1300 proceeds to steps 1306 and 1308, wherein it is determined whether a fingerprint has been scanned by the fingerprint scanner 316 of the pocket vault interface unit 302 before a timeout period measured by the step 1308 has elapsed.

When, at the steps 1306 and 1308, it is determined that a fingerprint has not been scanned within the timeout period of step 1308, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302.

When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304.

After the step 1312, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1310, it is determined that the scanned fingerprint does not match any fingerprint stored in the memory 314 of the pocket vault interface unit 302, the routine 1300 proceeds to a step 1314, wherein a message is transmitted to the interface station computer 304 indicating there has been an unsuccessful attempt to authenticate an operator of the pocket vault interface unit 302.

After the step 1314, the routine 1300 proceeds to steps 1316 and 1318, wherein it is determined whether, before the expiration of a timeout period measured by the step 1318, a request has been received from the interface station computer 304 to add a new operator to the pocket vault interface unit 302.

When, at the steps 1316 and 1318, it is determined that such a request has not been received from the interface station computer 304 in a timely manner, the routine 1300 returns to the step 1302 (discussed above).

When, at the steps 1316 and 1318, it is determined that a request to add a new operator to the pocket vault interface unit 302 has been received from the interface station computer 304 in a timely manner, the routine 1300 proceeds to steps 1320 and 1322.

At the steps 1320 and 1322, it is determined whether three identical fingerprints have been stored in the interface unit 302 for each of the operator's two hands before the expiration of a timeout period measured by the step 1322. The operator may be prompted, e.g., on the display 324 of the interface station computer 304, to take appropriate steps to ensure his or her fingerprints are properly scanned. An example routine for obtaining the requisite fingerprint data from a user is discussed above in connection with steps 804a-810a and 804b-810b (for the Pocket Vault 102), and therefore will not be repeated here.

When, at the steps 1320 and 1322, it is determined that the requisite fingerprint information has not been stored in a timely manner, the routine 1300 proceeds to a step 1336, wherein an indication (e.g., a message or an audio tone) regarding the unsuccessful new operator validation attempt is generated.

After the step 1336, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1320 and 1322, it is determined that the fingerprint information has been successfully stored in the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1324, wherein an encrypted message including an ID unique to the interface unit 302 is transmitted to the interface station computer 304 for ultimate registration with the network server 114.

After the step 1324, the routine 1300 proceeds to step 1326 and 1328, wherein is determined whether a message including validation information (e.g., a PKI certificate for the interface unit 302) has been received from the network server 114 (via the interface station computer 304) before the expiration of a timeout period.

When, at the steps 1326 and 1328, the validation information is not received by the interface unit 302 in a timely manner, the routine 1300 proceeds to the step 1336 (discussed above).

When, at the steps 1326 and 1328, it is determined that the validation information is received by the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1330, wherein the validation information is stored for the new operator.

After the step 1330, the routine 1300 proceeds to a step 1332, wherein an indication (e.g., a message or an audio tone) regarding the successful validation of the new operator is generated.

After the step 1332, the routine 1300 returns to the step 1346 (discussed above).

Fig. 14 is a flow diagram illustrating example implementation of a primary routine 1400 that may be executed by the controller 308 of the interface station computer 304 of Fig. 3.

As shown, the routine 1400 begins at a step 1402, wherein a menu is displayed on the display 324 of the interface station computer 304 that gives the operator of the interface station computer 304 several options to choose from. These options may, for example, include: (1) the option to request that a Pocket Vault 102 be validated (i.e., permitted to store a new finger print), (2) the option to request that the information currently stored on a Pocket Vault 102 be updated (e.g., information may be uploaded from the network server 114), (3) the option to request that a transaction involving a Pocket Vault 102 be authorized, and/or (4) the option to access a website on the network server 114 and take advantage of the functionality thereof.

It should be appreciated that the foregoing are only examples of menu options that may be provided to the operator of the interface station computer 304, and that the invention is not limited to the particular examples described. It should also be appreciated that fewer than all of the options shown may be provided in connection with different types of interface stations. For example, a validation interface station 104a may be provided only with option (1), a personal interface station may be provided only with option (2), and a commercial interface station may be provided only with option (3). In many instances, option (4) may be the only option required or desired to be employed by the user, as the website may itself provide all of the functionality of the other options (1)-(3). If fact, in such circumstances, the user need not be provided with a menu at all, as the user could simply log on the website

using a browser. An embodiment of a network system in which a website may be accessed by a server in this manner is discussed below in connection with Figs. 28-39.

After displaying the menu at the step 1402, the routine 1400 proceeds to a step 1404, wherein it is determined whether any requests to validate Pocket Vaults 102 have been received.

When, at the step 1404, it is determined that no request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1408, wherein it is determined whether any requests to update information on Pocket Vaults 102 have been received.

When, at the step 1408, it is determined that no request to update the information on a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1412, wherein it is determined whether any requests to authorize transactions involving Pocket Vaults 102 have been received.

When, at the step 1412, it is determined that no request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1416, wherein it is determined whether the interface station computer has received any messages from Pocket Vault interface units 302 indicating that an unsuccessful operator authentication has occurred (i.e., the fingerprint of an operator scanned by the fingerprint scanner 316 has failed to match a fingerprint stored in the memory 314).

When, at the step 1416, it is determined that no such messages have been received, the routine 1400 proceeds to a step 1420, wherein it is determined whether a request to access a website on the network server 114 has been received.

When at the step 1420, it is determined that no request to access the website on the network server 114 has been received, the routine 1400 returns to the step 1402, wherein the menu of the various options for the operator is again displayed. Thus, the menu 1402 is displayed until one of the various options is selected in accordance with any of the steps 1404, 1408, 1412, 1416, or 1420.

When, at the step 1404, it is determined that a request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1406, wherein the PROCESS REQUEST TO VALIDATE POCKET VAULT routine (discussed below in connection with Fig. 15) is executed.

After the step 1406, the routine 1400 proceeds to the step 1408 (discussed above).

When, at the step 1408, it is determined that a request to update the information on a Pocket Vault 102 has been received, the routine 1410 proceeds to a step 1410, wherein the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine (discussed below in connection with Fig. 16) is executed.

After the step 1410, the routine 1400 proceeds to the step 1412 (discussed above).

When, at the step 1412, it is determined that a request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1414, wherein the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine (discussed below in connection with Fig. 17) is executed.

After the routine 1414, the routine 1400 proceeds to the step 1416 (discussed above).

When, at the step 1416, it is determined that a message has been received from an the interface station computer 304 indicating that an attempted fingerprint match of an operator has failed, the routine 1400 proceeds to a step 1418, wherein the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine (discussed below in connection with Fig. 18) is executed.

After the routine 1418, the routine 1400 proceeds to the step 1420 (discussed above).

When, at the step 1420, it is determined that a request to access a website on the network server 114 has been received, the routine 1400 proceeds to a step 1422, wherein the PROCESS REQUEST TO ACCESS WEBSITE routine (discussed below in connection with Figs. 30-39) is executed.

After the step 1422, the routine 1400 returns to the step 1402 (discussed above).

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine of Fig. 14 (step 1406).

As shown, the routine 1406 begins at a step 1502, wherein the potential new Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302. This may be accomplished, for example, by interfacing the docking interface 208 of the Pocket Vault 102 with the docking interface 312 of the pocket vault interface unit 302.

After the step 1502, the routine 1406 proceeds to steps 1504 and 1506, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1506.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that an error has occurred in the Pocket Vault validation process.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1506, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1506, the routine 1406 proceeds to steps 1508 and 1510, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1510.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to the step 1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1526, the routine 1406 terminates.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1512, wherein the interface station operator is prompted to input information regarding the new Pocket Vault holder into the interface station computer 304.

After the step 1512, the routine 1406 proceeds to a step 1514, whereat the routine 1406 waits until all of the requisite information regarding the new Pocket Vault holder has been entered properly (e.g., via the user input device 318 of the interface station computer 304).

After the step 1514, the routine 1406 proceeds to a step 1516, wherein the network server 114 (Fig. 1) is contacted.

After the step 1516, the routine 1406 proceeds to a step 1518, wherein the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with a request that the new Pocket Vault holder be validated.

After the step 1518, the routine 1406 proceeds to steps 1520 and 1522, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1522.

When, at the steps 1520 and 1522, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1524, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1520 and 1522, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1528, wherein, in an encrypted format, the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1528, the routine 1406 proceeds to steps 1530 and 1532, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1532, and prior to receiving a message from the network server 114 indicating that the request to validate the new Pocket Vault holder has been denied.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, or it is determined that a message has been received indicating that the request to validate the new Pocket Vault holder has been denied, the routine 1406 proceeds to a step 1538, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was unsuccessful.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine 1406 proceeds to a step 1534, wherein the encrypted validation information (e.g., a PKI certificate) from the network server 114 is forwarded to the pocket vault interface unit 302 for forwarding on to the Pocket Vault 102.

After the step 1534, the routine 1406 proceeds to a step 1536, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was successful. In addition to this message, when the pocket vault interface unit 302 forwards this message on to the Pocket Vault 102, the Pocket Vault 102 itself may provide, for example, an audio indication such as a chime, indicating that the Pocket Vault 102 has been successfully validated.

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine of Fig. 14 (step 1410).

As shown, the routine 1410 begins at a step 1602, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302.

After the step 1602, the routine 1410 proceeds to steps 1604 and 1606, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1606.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1634, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1606, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1606, the routine 1410 proceeds to steps 1608 and 1610, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1610.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to the step 1634,

wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1634, the routine 1410 terminates.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1612, wherein the network server 114 is contacted.

After the step 1612, the routine 1410 proceeds to a step 1614, wherein a request to update the information on the Pocket Vault 102 is transmitted to the network server 114.

After the step 1614, the routine 1410 proceeds to steps 1616 and 1618, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1618.

When, at the steps 1616 and 1618, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1620, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1616 and 1618, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1622, wherein, in an encrypted manner, the interface station operator ID, the interface unit ID, and the Pocket Vault ID are transmitted to the network server 114.

After the step 1622, the routine 1410 proceeds to steps 1624 and 1626, wherein it is determined whether encrypted updates have been received from the network server 114 for loading onto the Pocket Vault 102 prior to the expiration of a timeout period measured by the step 1620, and prior to the network server 114 denying the requested attempt to upload information.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have been received in a timely manner, the routine 1410 proceed to a step 1630, wherein the received updates are transmitted to the pocket vault interface unit 302 so that they may be subsequently forwarded to the Pocket Vault 102 for uploading thereto.

After the step 1630, the routine 1410 proceeds to a step 1632, wherein a message is displayed to the holder indicating that the requested updates have been successfully uploaded to the Pocket Vault 102.

After the step 1632, the routine 1410 terminates.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have not been received from the network server 114 in a timely manner, or that the network server 114 has denied the request to upload information onto the Pocket Vault 102, the routine 1410 proceeds to a step 1628, wherein a message is displayed on the display 324 indicating that the attempt to update the information on the Pocket Vault 102 was unsuccessful.

After the step 1628, the routine 1410 terminates.

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine of Fig. 14 (step 1414).

As shown, the routine 1414 begins at a step 1702, wherein the operator of the interface station computer 304 is prompted to input information regarding the proposed transaction involving the Pocket Vault 102.

After the step 1702, the routine 1414 waits at a step 1704 until all of the information regarding the requested transaction has been entered.

After, at the step 1704, it is determined that all of information regarding the requested transaction has been entered, the routine 1414 proceeds to a step 1706, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault with the pocket vault interface unit 302.

After the step 1706, the routine 1414 proceeds to steps 1708 and 1710, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1710.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1726, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface

unit 302 in a timely manner, the routine 1414 proceeds to a step 1712, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1712, the routine 1414 proceeds to steps 1714 and 1715, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1715.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to the step 1726, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1726, the routine 1414 terminates.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1716, wherein the network server 114 is contacted.

After the step 1716, the routine 1414 proceeds to a step 1718, wherein the request regarding the proposed transaction involving the Pocket Vault 102 is transmitted to the network server 114.

After the step 1718, the routine 1414 proceeds to step 1720 and 1722, wherein it is determined whether the transaction request has been acknowledged by the network server 114 before the expiration of a timeout period measured by the step 1722.

When, at the steps 1720 and 1722, it is determined that the request has not been acknowledged in a timely manner, the routine 1414 proceeds to a step 1724, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

After the steps 1724, the routine 1414 terminates.

When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732.

When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed.

When , at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has been received in a timely manner, the routine 1414 proceeds to a step 1734, wherein a message is forwarded to the pocket vault interface unit 302 indicating that the requested transaction has been approved. This message may also be used to update information on the Pocket Vault 102, and/or to cause the Pocket Vault 102 to generate an indication (e.g., an audio tone) that the transaction has been approved.

After the step 1734, the routine proceeds to a step 1738, wherein a message is displayed on the display 324 indicating that the requested transaction has been approved.

After the step 1738, the routine 1414 terminates.

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine of Fig. 14 (step 1418).

As shown, the routine 1418 begins at a step 1802, wherein the operator of the interface station computer 304 is informed that the attempted use the pocket vault interface unit 302 (when the operator applied his or her finger print to the fingerprint scanner 316) was not authorized.

After the step 1802, the routine 1418 proceeds to a step 1804, wherein the operator is prompted to either: (1) add a NEW OPERATOR to the interface unit 302, or (2) ABORT the attempt to use the interface unit 302.

When, at the step 1806, it is determined that the operator has chosen to ABORT the attempt to use the interface unit 302, the routine 1418 terminates.

When, at the step 1806, it is determined that the operator has chosen to add a NEW OPERATOR, the routine 1418 proceeds to a step 1808, wherein a message is transmitted to the pocket vault interface unit 302 indicating the operator's desire to add a new operator to the pocket vault interface unit 302.

After the step 1808, the routine 1418 proceeds to a step 1810, wherein the operator is prompted to input information regarding the proposed new operator into the interface station computer 304 (e.g., using the user input device 318), and is provided with instructions as to the application of three identical fingerprints from each of his or her two hands to the fingerprint scanner 316 of the interface unit 302.

After the step 1810, the routine 1418 proceeds to a step 1812 wherein the routine 1418 waits until all of the requisite information regarding the proposed new interface station operator has been entered properly.

When, at the step 1812, it is determined that all of the requisite information regarding the proposed new operator has been entered properly, the routine 1418 proceeds to a step 1814, wherein the network server 114 is contacted.

After the step 1814, the routine 1418 proceeds to a step 1816, wherein the request to add the new operator to the pocket vault interface unit 302 is transmitted to the network server 114.

After the step 1816, the routine 1418 proceeds to steps 1818 and 1820, wherein it is determined whether the request by the interface station computer has been acknowledged by the network server 114 prior to the expiration of a timeout period measured by the step 1820.

When, at the steps 1818 and 1820, it is determined that the request has not been acknowledged in a timely manner, the routine 1418 proceeds to the step 1822, wherein a transmission failure message is displayed.

After the step 1822, routine 1418 terminates.

When, at the steps 1818 and 1820, it is determined that the request has been acknowledged in a timely manner, the routine 1418 proceeds to the step 1824, wherein a message, including the information regarding the proposed new operator and the interface unit ID, is transmitted to the network server 114 in an encrypted manner.

After the step 1824, the routine 1418 proceeds to steps 1826 and 1828, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1828, and prior to the network server 114 denying the addition of the new interface station operator.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine

1418 proceeds to a step 1830, wherein the encrypted validation information (e.g., a PKI certificate) is forwarded from the interface station computer 304 to the pocket vault interface unit 302.

After the step 1830, the routine 1418 proceeds to a step 1834, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was successful.

After the step 1834, the routine 1418 terminates.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, the routine 1418 proceeds to a step 1832, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was unsuccessful.

After the step 1832, routine 1418 terminates.

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine 1900 that may be executed by the network server 114 of Fig. 1.

As shown, the routine 1900 may begin at a step 1902, wherein it is determined whether any requests have been received to register new Pocket Vault holders.

When, at the step 1902, it is determined that a request has been received to register a new Pocket Vault holder, the routine 1900 proceeds to a step 1904, wherein the request to register the new Pocket Vault holder is processed. An example of a routine that may be employed to implement the step 1904 is discussed in more detail below in connection with Fig. 20.

When, at the step 1902, it is determined that no request to register a new Pocket Vault holder has been received, the routine 1900 proceeds to a step 1906, wherein consumer marketing information is compiled and transmitted to subscribing media issuers and advertisers.

After the step 1906, the routine 1900 proceeds to a step 1908, wherein it is determined whether any requests from media issuers or advertisers have been received to update the network server 114.

According to one aspect of the invention, media issuers and advertisers may have the option to utilize the functionality of the network server 114 to update the account characteristics of authenticated Pocket Vault holders. These updates may, for example, be delivered from the computers 108, 110, and 112 to a secure location within the database 406.

When each selected holder next synchronizes with network server 114 (e.g., as described below in connection with routine 1914 of Fig. 22), any media characteristics updated by the media issuers or advertisers may be uploaded to that holder's the Pocket Vault 102. The database of account updates may be revised periodically based on the media issuer's systems (e.g., pursuant to the routine 1910 of Fig. 21 - described below). Confirmation of the update process may be provided to the issuer after a synchronization session is complete for a particular Pocket Vault holder (see step 2206 of routine 1914 (Fig. 22) below).

When, at the step 1908, it is determined that a request to update the network server 114 has been received from a media issuer or advertiser, the routine 1900 proceeds to a step 1910, wherein the request from the media issuer or advertiser is processed. An example of a routine that may be employed to implement the step 1910 is discussed in more detail below in connection with Fig. 21.

When, at the step 1908, it is determined that no request from a media issuer or advertiser to update the network server 114 has been received, the routine 1900 proceeds to a step 1912, wherein it is determined whether any requests have been received from holders to update information on their Pocket Vaults.

When, at the step 1912, it is determined that such a request has been received, the routine 1900 proceeds to a step 1914, wherein the request to update the Pocket Vault information is processed. An example of a routine that may be employed to implement the step 1914 is described in more detail below in connection with Fig. 22.

When, at the step 1912, it is determined that no request from a holder to update information on a Pocket Vault 102 has been received, the routine 1900 proceeds to a step 1916, wherein it is determined whether any holders have requested that new files be loaded onto the network server 114.

When, at the step 1916, it is determined that a holder has requested that a new file be loaded onto the network server 114, the routine 1900 proceeds to a step 1918, wherein the holder's request to load the new file onto the network server 114 is processed. An example of a routine that may be employed to implement the step 1918 is described in more detail below in connection with Fig. 23.

When, at the step 1916, it is determined that no request by a holder to load a file onto the network server 114 has been received, the routine 1900 proceeds to a step 1920, wherein it is determined whether any requests have been made to authorize transactions. Such a

request may be made, for example, by a merchant operating a commercial interface station 104c. In this regard, it should be appreciated that, when a token 102a is employed to engage in a transaction with a commercial card reader 106 or a commercial bar code reader 107, a request for transaction approval may not be made to the network server 114. Instead such a transaction approval request may be made through conventional, existing communication and approval channels for such devices. Therefore, it should be understood that the step 1922 is generally reached only when it is possible for the network server 114 to check the identity of the Pocket Vault holder, the identity of the Pocket Vault 102, and possibly identity of the operator of a commercial interface station, based on communications with the Pocket Vault 102 (e.g., via a commercial interface station 104c or via a wireless network such as Bluetooth).

When, at the step 1920, it is determined that a request to authorize a transaction has been made, routine 1900 proceeds to a step 1922, wherein the request to authorize the transaction is processed. An example of a routine that may be employed to implement the step 1922 is discussed in more detail below in connection with Fig. 24.

When, at the step 1920, it is determined no request to authorize a transaction has been made, the routine 1900 returns to the step 1902 (discussed above). With regard to the routine 1900 of Fig. 19, it should be appreciated that all of the requests to accomplish the various tasks may be placed in a queue so that they are serviced on a first-come, first-served or any other basis, rather than servicing them in the particular order shown in Fig. 19.

Fig. 20 is a flow-diagram illustrating an example of a routine that may be employed to implement the step 1904 of the routine 1900 (Fig. 1).

As shown, the routine 1904 begins at a step 2002, wherein a request received from the interface station computer 304 to register a new Pocket Vault holder is acknowledged, and the network server 114 requests the interface station computer 304 to transfer the relevant information regarding the proposed new holder to the network server 114.

After the step 2002, the routine 1904 proceeds to a step 2004, wherein the routine 1904 waits for all of the requisite holder registration information to be received from the interface station computer 304.

When, at the step 2004, it is determined that all of the requisite holder registration information has been received from the interface station computer 304, the routine 1904 proceeds to a step 2006, wherein it is determined whether the proposed Pocket Vault use is

authorized. An example of a routine that may be employed to implement the step 2006 is discussed below in connection with Fig. 25. In determining whether a particular Pocket Vault use is authorized, there are numerous parameters which may be checked. For example, the port to which the interface station computer is connected (e.g., the telephone number or IP address of the computer) may be checked to ensure that it is authorized. Additionally, information from the interface station computer 304 (e.g., a "cookie") may be checked to ensure that the computer itself has been registered with the system. Further, it can be checked whether the current operator of the interface station computer 304 is registered as being associated with the interface station computer 304 being used, and that the proposed new Pocket Vault holder is authorized to use that particular the Pocket Vault 102. In sum, the identity of (1) each piece of equipment, (2) each operator of each piece of equipment, and (3) each location of each piece of equipment may be checked to ensure that the particular use of the Pocket Vault is authorized. It should be appreciated fewer than all of these parameters, different parameters, and/or additional parameters can be checked in alternative embodiments of the invention, and that the invention is not limited to embodiments wherein all of the aforementioned parameters are checked to verify that a particular Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1904 terminates. In such a situation, it is also possible to generate some sort of security alert message to put someone or some entity on notice that an unauthorized use of a Pocket Vault has occurred.

When, the routine 2006 has determined that the proposed Pocket Vault use is authorized, the routine 1904 proceeds to a step 2008, wherein all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114 (Fig. 4). As shown in Fig. 20, this information may include, for example, the interface station operator ID, the interface unit ID, the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder.

After the step 2008, the routine 1904 proceeds to a step 2010, wherein the network server 114 transmits encrypted validation information to the interface station computer 304, which then may be passed on to the pocket vault interface unit 302, and then to the Pocket Vault 102, so as to enable the new holder's fingerprint to be stored in the memory of the Pocket Vault 102.

After the step 2010, the routine 1904 terminates.

Fig. 21 is a flow diagram illustrating example of a routine that may be employed to implement the step 1910 of the primary routine 1900 (Fig. 19).

As shown, the routine 1910 begins at a step 2102, wherein it is determined whether all of the requested updates have been received from the media issuer or advertiser.

When, at the step 2102, it has been determined that all of the requested updates have been received, the routine 1910 proceeds to a step 2104, wherein it is determined whether the media issuer or advertiser is authorized access to the network server 114. This authorization process may require some sort of authentication of the identity of the computer used by the media issuer or advertiser requesting the update, the operator of the computer, and/or the location of the computer, in a manner similar to that in which the interface stations 104 and their operators are authorized.

When, at the step 2104, it is determined that the media issuer or advertiser is not authorized access to the network server 114, the routine 1900 proceeds to a step 2106, wherein a message is transmitted to the media issuer or advertiser informing the media issuer or advertiser that access to the network server 114 has been denied.

After the step 2106, the routine 1910 terminates.

When, at the step 2104, it is determined that the media issuer or advertiser is authorized access to the network server 114, the routine 1910 proceeds to a step 2108, wherein the updates received from the media issuer or advertiser are logged onto the network server 114.

After the step 2108, the routine 1910 terminates.

Fig. 22 is a flow diagram illustrating an example a routine that may be employed to implement the step 1914 of the primary routine 1900 (Fig. 19).

As shown, the routine 1914 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1914 terminates.

When, at the step 2006, it is determined that the Pocket Vault use is authorized, the routine 1914 proceeds to a step 2202, wherein encrypted updates are transmitted to the interface station computer 304 for loading onto the Pocket Vault 102.

After the step 2202, the routine 1914 proceeds to steps 2204 and 2206, wherein the time and date of the updates are logged (step 2204), and the media issuers or advertisers are informed that the updates have been made (step 2206).

Fig. 23 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1918 of the primary routine 1900 (Fig. 9).

As shown, the routine 1918 begins at a step 2302, wherein it is determined whether the file to be loaded onto the network server 114 relates to a secure media issuer.

When, at the step 2302, it is determined that the file does not relate to a secure media issuer, the routine 1918 proceeds to a step 2304, wherein the network server 114 is updated with the non-secure file.

After the step 2304, the routine 1918 terminates.

When, at the step 2302, it is determined that the to-be-loaded file does relate to a secure media issuer, the routine 1918 proceeds to a step 2306, wherein it is determined whether the secure media issuer is a Pocket Vault participant (i.e., a media issuer having access to the network server 114).

When, at the step 2306, it is determined that the secure media issuer is not a Pocket Vault participant, the routine 1918 proceeds to a step 2308, wherein an advisory is sent to the holder indicating an inability to load the file, and inquiring as to whether the holder desires to load the file in a non-secure format. The holder may, for example, opt to load the file to the network server 114 in such a way that the content of the file is not encodable to the Chameleon Card, but can be displayed and shown to a POS operator and manually keyed in at POS by the POS operator.

After the step 2308, the routine 1918 proceeds to a step 2316, wherein it is determine whether the holder has elected to load the file in a non-secure format.

When, at the step 2316, it is determined that the holder has elected not to load the file in a non-secure format, the routine 1918 terminates.

When, at the step 2316, it is determined that the holder has elected to load the file in a non-secure format, the routine 1918 proceeds to a step 2318, wherein the file is loaded onto the network server 114 in a non-secure format.

After the step 2318, the routine 1918 terminates.

When, at the step 2306, it is determined that the secure media issuer is a Pocket Vault participant, the routine 1918 proceeds to a step 2310, wherein the media issuer is queried as to the account status of the holder.

After the step 2310, the routine 1918 proceeds to a step 2312, wherein it is determined whether authorization has been received from the media issuer to load the file.

When, at the step 2312, it is determined that authorization has not been received from the media issuer, the routine 1918 proceeds to the step 2308 (discussed above).

When, at the step 2312, it is determined that authorization has been received from the media issuer, the routine 1918 proceeds to a step 2314, wherein the network server 114 is updated with the secure file.

After the step 2314, the routine 1918 terminates.

Fig. 24 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1922 of the primary routine 1900 (Fig. 19).

As shown, the routine 1922 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted use of the Pocket Vault 102 is authorized.

When, at the step 2006, it is determined that the attempted Pocket Vault use is not authorized, the routine 1922 terminates.

When, at the step 2006, it is determined that the attempted Pocket Vault used is authorized, the routine 1922 proceeds to a step 2402, wherein it is determined whether the requested transaction is within acceptable account parameters (e.g., as set by the media issuer).

When, at the step 2402, it is determined that the requested transaction is not within acceptable account parameters, the routine 1922 proceeds to a step 2404, wherein a message is transmitted to the entity that requested the transaction (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107) indicating that the transaction is outside of acceptable account parameters.

After the step 2404, the routine 1922 terminates.

When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (Fig. 4). As shown, the logged information may

include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction.

After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).

After the step 2408, the routine 1922 terminates.

Fig. 25 is a flow diagram illustrating an example of a routine that may employed to implement the step 2006 of the routines 1904 (Fig. 20), 1914 (Fig. 22), and 1922 (Fig. 24).

As shown, the routine 2006 begins at a step 2502, wherein it is determined whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source (e.g., an authorized telephone line or an authorized internet protocol (IP) address).

When, at the step 2502, it is determined that the entity proposing the transaction is not connected to a valid source, the routine 2006 proceeds to a step 2510, wherein the transaction is refused, and a security alert is generated so that appropriate action(s) may be taken.

When, at the step 2502, it is determined that the entity proposing the transaction is connected to a valid source, the routine 2006 proceeds to a step 2504, wherein it is determined whether the ID of the interface station, card reader or barcode reader is valid, and is properly linked to the source to which is connected.

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is not valid, the routine proceeds to the step 2510 (discussed above).

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107 or an RF signal receiver is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation.

When, at the step 2506, it is determined that the Pocket Vault ID (when available and required) is not valid, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the

Pocket Vault ID (if available) is linked to the ID of the entity proposing the transaction, e.g., a commercial interface station 104c, a card reader 106, or a barcode reader 107.

When, at the step 2508, it is determined that the ID of the Pocket Vault 102 (when available) is not linked to the ID of the entity proposing the transaction, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2508, it is determined that the Pocket Vault ID is linked to the ID of the entity proposing the transaction, or that the ID of the Pocket Vault is not required, the routine 2006 proceeds to a step 2512, wherein the Pocket Vault use is authorized.

With regard to the information checked in connection with the routine 2006 to determine whether a particular Pocket Vault use is authorized, it should be appreciated that, in some embodiments, fewer than all of the verification steps discussed above may be performed when lesser degrees of security are desired or required. For example, in some embodiments, there may be no restrictions as to who can operate an interface station, the source to which the station is connected, and/or the ID of the station.

Figure 27 illustrates a network system similar to that described hereinabove. The system of Fig. 27, however, includes several additional components which serve to increase the network's functionality and utility. Accordingly, it should be appreciated that, in addition to the components illustrated in Fig. 27, the system may also include all or some of the components and features of the system described above in connection with Figs. 1-26, and may also incorporate all or some of that system's functionality.

As shown in Fig. 27, the Pocket Vault 102 may be coupled to an interface station 104 (including an interface unit 302 coupled to an the interface station computer 304). The interface unit 302 may include a communication port 2706, which is adapted to perform basic communications functions for interaction between the interface unit 302 and each of the Pocket Vault 102 and the interface station computer 304. This communication can take place over physical wires using a USB protocol or HotWire, or any other suitable protocol. Alternatively, the communication can be wireless, using a standard wireless protocol, such as Bluetooth, or any other suitable protocol. The communication port 2706 may, of course, be adapted to perform communications functions depending on the requirements on the particular protocol used. In an example embodiment, a USB protocol is used, and the interface unit 302 is connected to the interface station computer 304 through a USB port.

Several suitable methods/techniques for interfacing the Pocket Vault 102 with the interface unit 302 are described above.

In addition to the communication port 2706, as in the embodiment described above, the interface unit 302 contains a stripe reader 315. The purpose and operation of the stripe reader 315 is described below in connection with Figure 34.

The interface station computer 304 may be any suitable computer that employs one or more processors to execute instructions stored in memory. The interface station computer 304 may even comprise several inter-networked computers.

In the illustrative embodiment shown, the interface station computer 304 may use the communication software 2710 to communicate with the network server 114 via the network 2724. The communication software 2710 may be any of a number of communication programs known in the art, and the invention is not limited to any particular type of software. The software 2710 may, for example, comprise a web browser, a terminal emulation program, a proprietary program, or any other software module capable of communicating with other computers using the network 2724. The network 2724 may be any communication network known in the art. For example, the network 2724 may comprise the World Wide Web, a Local Area Network, or any other networking arrangement adapted for communication between digital computers.

In the embodiment shown, the communication software 2710 uses internet settings 2722 when accessing the network 2724. The internet settings 2710 may include any user preferences or software settings relevant to communication functions and usability of the communication software 2710. The internet settings 2722 may comprise, for example, the network name and the identification of the interface station computer 304, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The communication software 2710 may access the network 2724 through communication protocol layer 2714. Depending on how the interface station computer 304 is physically connected to the network 2724. The communication protocol layer 2714 may be dial-up software, a TCP/IP layer, or any other suitable networking layer. The communication protocol layer 2714 may, for example, execute low-level communication functions, thereby

providing useful abstractions to the communication software 2710. In an example embodiment, the interface station computer 304 is connected to the network 2724 using a modem, and the communication protocol layer 2714 is a dialup software module.

As shown, the interface station computer 304 may also contain one or more communication drivers 2712. Although multiple drivers may, in fact, be employed, for simplicity of discussion, the description hereinafter may refer to all such drivers as a single "driver." The communication driver 2712 acts both as a device driver for the interface unit 302, and also as a communications driver capable of accessing internet settings 2722 and facilitating communications between the Pocket Vault 102 and the server 114 by using the communication protocol layer 2714 to establish a connection to the network server 114 through the network 2724.

The network server 114 may comprise any suitable processor-based device or its equivalent. It may be either a single or multi-processor machine, or even a collection of servers inter-networked together. In one embodiment, the network server 114 stores both data and applications that are accessible to users. The network server 114 may, for example, store and serve a website, i.e., a collection of web pages and data that are available to users via a browser.

The network server 114 may include one or more controllers 402 and a database 406, as described above in connection with Figure 4. In addition, the network server 114 may include a communication protocol layer 2716, which provides low-level communication functions to server communications software. The communication protocol layer 2716 may be, but need not be, the same as the communication protocol layer 2714 of the interface station computer 304.

As shown in Fig. 27, the network server 114 may communicate through the network 2724 with an issuer authority 2718. The issuer authority 2718 may correspond, for example, to any of the advertiser(s) 108, non-financial media issuer(s) 110, or financial media issuer(s) 112 described above in connection with Fig. 1, or may be any entity designated to represent any of the same.

Overall, the networking arrangement illustrated in Fig. 27 allows the Pocket Vault 102 to access the network server 114. It also allows the interface station computer 304 to access restricted portions of the network server 114, such as, for example, user data stored in the database 406, when access is authenticated through communication from the Pocket Vault

102 to the network server 114. Authentication and access to restricted areas of the network server 114 will be further described below.

In order for the Pocket Vault 102 to perform communications functions, as well as other functions described elsewhere herein, the Pocket Vault 102 may be driven by control software 2708. Fig. 28 is a block diagram illustrating example components of the control software 2708 that may be disposed on the Pocket Vault 102.

As shown, the control software 2708 may include components such as a communications software module 2802, a card loading module 2804, an internet settings management module 2806, a synchronization module 2808, a statistics module 2810, and a security module 2812. It should be appreciated, of course, that the control software 2708 is not limited to the illustrative modules shown, and that the control software 2708 may comprise fewer modules or additional modules to perform other functions, such as the functionality described above in connection with Figs. 7-12.

The communications software module 2802 may, for example, be responsible for communications with the network server 114 and with the interface station computer 304, in the manner discussed below.

The card loading module 2804 may, for example, be responsible for loading data for new cards or tokens and storing such data in memory, as well as for transferring this data to the network server 114, when appropriate. Examples of how card/token data may be loaded onto the Pocket Vault 102 are discussed below in connection with Fig. 34.

Internet settings management module 2806 may, for example, be responsible for managing the storage and use of internet settings by the Pocket Vault 102. Such internet settings may, for example, correspond to any of the internet settings 2722 that may be stored on the interface station computer 304. The internet settings management module 2806 may allow a user to store, manage, and transfer internet settings, e.g., cookies and preference settings, from one computer to another. Operation of the internet settings management module 2708 will be further described below in connection with the steps 3310 and 3320 of the routine 3024 (Fig. 33).

The synchronization module 2808 may, for example, be responsible for synchronizing data and settings stored on the Pocket Vault 102 with data and settings stored on the network server 114. Operation of the synchronization module 2808 is described below in connection with Fig. 35.

The statistics module 2810 may, for example, collect statistics concerning use of the Pocket Vault 102. Such statistics may, for example, include information such as the number of accesses to various cards stored in the memory of the Pocket Vault 102, the number of financial transactions engaged in, the date of the last update of the Pocket Vault 102, the total amount and kind of data transferred between the Pocket Vault 102 and each interface station 104 and/or the network server 114. In addition, the statistics module 2810 may be adapted to be customized by the user.

The security module 2812 may, for example, ensure security of authentication and communications. All communications to and from the network server 114 and the interface station 104 may be encrypted by the security module 2812, so that any attacker who intercepts those communications will receive no useful information.

Any of numerous types of encryption may be used to satisfactorily protect communications between the Pocket Vault 102 and the other devices in the network. For example, one of the asymmetric-key encryption types, such as public key encryption or private key encryption, may be used. These public/private encryption techniques are well known in the art and therefore will not be described here in detail. Alternatively, one-time pad encryption or other encryption techniques may be used to achieve a similar objective.

As discussed above, the Pocket Vault 102 may be adapted to not release any personal or secure information, even encrypted, until the holder presents satisfactory verification of his or her identity, such as, for example, presenting the holder's fingerprint to the fingerprint scanner 220 or entering a password. In addition, fingerprint and password protection may be used together for authentication purposes, such that personal or secure information can be transferred or released only if the holder has been successfully authenticated using both techniques.

In alternative embodiments, security may be implemented using different measures, or may be omitted altogether in situations where the interface station computer 304 is a trusted host. In addition, security module 2812 may be called on to perform security functions in situations other than communicating with the network server 114 and the interface station computer 304.

The manner of communication among the Pocket Vault 102, the network server 114, and an interface station computer 304 will now be described in connection with Figure 29. Figure 29 is a data flow diagram illustrating how data may be transferred between the Pocket

Vault 102 and a user interface 2902 of the interface station computer 304. The user interface 2902 may, for example, comprise a web browser included in the communications software 2710 running on the interface station computer 304. Alternatively, it may be a stand-alone application that allows a user to interact with the communications software 2710 and, through it, interact with a website located on the network server 114.

In the illustrative embodiment shown, the data transfer takes place via the communication driver 2712, the network server 114, and the communications software 2710, data can flow in both directions at all connection points, and all communications between the Pocket Vault 102 and the user interface 2902 of the interface station computer 304 pass through the network server 114.

Using the arrangement shown, the user may, for example, update settings on the Pocket Vault 102 by using the user interface 2902 and the communication software 2710 to update settings on the network server 114, and then instructing the network server 114 to update settings on the Pocket Vault 102 via the communication driver 2712.

In one embodiment, the network server 114 implements a website, where user information may be selectively stored and accessed by a person using the communication software 2710 (e.g., a web browser) running on the interface station computer 304, and any user may access the website on the network server 114. However, the website may have a so-called "restricted area" which can be accessed only after the user has authenticated his or her identity. As used herein, the term "restricted area" or "restricted information" means any data that is not available to general public without some sort of authentication. For example, each user may have preferences stored in the database 406 that would indicate how the main site should be presented to that user. Those preferences will not be available to other users. In addition to such relatively low-security settings, such as website preferences, database 406 may also contain private user information, such as information about a user's credit cards and identity information. Access to this restricted information may be limited, for example, to only "authenticated" users.

Authentication of a Pocket Vault holder may be achieved, for example, by the holder applying a fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, interfacing the Pocket Vault 102 with the interface unit 302 (which acts essentially as a pass-through device), and establishing a connection between the Pocket Vault 102 and the network server 114 via the communication driver 2712. Based on communications with the Pocket Vault

102 via this "connection," the website may determine: (1) whether the Pocket Vault 102 has been "validated," i.e., whether a fingerprint has been stored in the fingerprint memory of the Pocket Vault 102 and whether validation information (e.g., a PKI certificate) is present on the Pocket Vault 102, and (2) whether the Pocket Vault 102 has been authenticated, i.e., whether the fingerprint recently scanned by the Pocket Vault 102 matched the fingerprint stored in the fingerprint memory of the Pocket Vault 102. If the website determines that the Pocket Vault 102 has not yet been validated, the user may be given an option to validate the Pocket Vault 102 using the website software. If the website determines that the Pocket Vault 102 has been validated and authenticated, then the network server 114 may enable the authenticated holder to access or perform functions relating to some or all of the restricted area of the database 406 containing that holder's information.

Communication driver 2712 may be a light-weight application that can access and modify the internet settings 2722, and can also access communications protocol layer 2714, but cannot transfer information to any other software programs. For example, the communication driver 2712 may access the internet settings 2722 in order to determine that the interface station computer 304 is connected to the network 2724 through a dial-up connection; following that, it may initiate the dial-up connection or use an established connection through the communications protocol layer 2714 in order to tunnel packets from the Pocket Vault 102 to the network 2724.

Fig. 30 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO ACCESS WEBSITE routine 1422 shown in Fig. 14, which may be executed by the controller 308 of the interface station computer 304. As discussed above in connection with Fig. 14, it should be appreciated that this routine need not be accessed as a result of a user selecting it from the menu displayed in the step 1402. Rather, a user may simply use a browser to directly log onto the website on the network server 114.

As shown, the routine 1422 begins at a step 3002, wherein the interface station computer 304 is caused to access the website on the network server 114, e.g., by using a browser to access the website.

After the step 3002, the routine 1422 proceeds to a step 3004, wherein it is determined whether the requisite communication drivers 2712 have been installed.

When, at the step 3004, it is determined that the requisite communication drivers 2712 have not been installed, the routine 1422 proceeds to an INSTALL DRIVER(S) routine 3006

(discussed below in connection with Fig. 31), which is responsible for installing the communication drivers 2712.

After the routine 3006 has completed, the routine 1422 proceeds to a step 3008, wherein the communication drivers 2712 are caused to become operational.

When, at the step 3004, it is determined that the requisite drivers 2712 have already been installed, the routine 1422 proceeds directly to the step 3008 (discussed above).

After the step 3008, the routine 1422 proceeds to steps 3010-3016, wherein attempts are made to establish a connection between the Pocket Vault 102 and the website on the network server 114 within a time out period determined by the step 3014. Each time it is determined that the connection has not yet been established, the user is prompted to interface the Pocket Vault 102 with the interface unit 302 and to connect the interface unit 302 to the interface station computer 304 (e.g., using a USB cable).

When, during the steps 3010-3016, it is determined that a connection has not been established between the Pocket Vault 102 and the website in a timely manner, the routine 1422 proceeds to a step 3026, wherein a message is displayed to the user regarding the unsuccessful communication attempt between the Pocket Vault 102 and the website on the network server 114.

After the step 3026, the routine 1422 terminates.

When, during the steps 3010-3016, it is determined that a connection has been successfully established between the Pocket Vault 102 and the website on the network server 114, the routine 1422 proceeds to a step 3018, wherein it is determined whether the Pocket Vault 102 has been validated, e.g., whether a holder's fingerprints and a PKI certificate are stored therein. The website may, for example, make this determination based upon the messages exchanged during the handshaking protocol engaged in between the Pocket Vault 102 and the network server 114.

When, at the step 3018, it is determined that the Pocket Vault 102 has not yet been validated, the routine 1422 proceeds to a NEW POCKET VAULT HOLDER routine 3020, which is discussed below in connection with Fig. 32.

When, at the step 3018, it is determined that the Pocket Vault 102 has already been validated, the routine 1422 proceeds to an EXISTING POCKET VAULT HOLDER routine 3024, which is discussed below in connection with Fig. 33.

After completion of the EXISTING POCKET VAULT HOLDER routine 3024, the routine 1422 terminates.

After completion of the NEW POCKET VAULT HOLDER routine 3020, the routine 1422 proceeds to a step 3022, wherein it is determined whether a new holder was successfully validated.

When, at the step 3022, it is determined that a new holder was successfully validated, the routine 1422 proceeds to the EXISTING POCKET VAULT HOLDER routine 3024 (discussed above).

When, at the step 3022, it is determined that a new holder was not successfully validated, the routine 1422 terminates.

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine 3006 shown in Fig. 30.

As shown, the routine 3006 begins at a step 3102, wherein the necessary communication drivers 2712 are downloaded from another computer, e.g., a website on the World Wide Web.

After the step 3102, the routine 3006 proceeds to steps 3104-3108, wherein the necessary communication drivers 2712 are installed on the interface station computer 304 and registered with network server 114, and the preferences for the communication drivers 2712 are set either automatically or in response to user input. During the step 3106, the communication driver 2712 may communicate with the network server 114 in order to register itself and its attributes. Among these attributes can be such things as a unique identifier for the interface station computer 304 on which that driver is installed, the identity of the user registering it, and other such items. The preferences that may be set by the user during the step 3108 may, for example, include information such as how and where to access the internet settings 2722, how many attempts at connection should be performed, etc.

After the step 3108, the routine 3006 terminates.

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine 3020 shown in Fig. 30.

As shown, the routine 3020 begins at a step 3202, wherein it is determined whether the new holder has indicated that he or she has already established an account with the website on the network server 114.

When, at the step 3202, it is determined that the new holder has not indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3204, wherein a new account is established on the website on the network server 114 in response to user input to a browser running on the interface station computer 304.

After the step 3204, the routine 3020 proceeds to a step 3206, wherein the new holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 while the Pocket Vault 102 is interfaced with the interface unit 302. The user is further prompted to follow the directions on the Pocket Vault 102. As discussed above in connection with Figs. 7 and 8, when a fingerprint is applied to a fingerprint scanner 220 of an un-validated device, the user is instructed by the Pocket Vault to apply six finger prints (three from one finger on the left hand and three from one finger on the right hand) sequentially to the fingerprint scanner 220, waiting for a beep each time. As discussed in connection with Fig. 8, after the new holder has completed this task, an encrypted message including the Pocket Vault ID may be released from the Pocket Vault to the interface unit 302. Because of the established connection between the Pocket Vault 102 and the website on the network server 114, this encrypted message should reach the website. And, in response to receiving this encrypted message, the website should release encrypted validation information (e.g., a PKI certificate) back to the Pocket Vault 102 via the established connection.

After the step 3206, the routine 3020 proceeds to steps 3208-3210, wherein it is determined whether the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before a timeout period has elapsed.

When, at the step 3210, it is determined that the timeout period elapsed before the encrypted message including the Pocket Vault ID was released to the website, the routine 3020 proceeds to a step 3220, wherein a message is displayed to the user concerning the unsuccessful attempt to validate the Pocket Vault holder.

After the step 3220, the routine 3020 terminates.

When, at the steps 3208-3210, it is determined the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before the timeout period elapsed, the routine 3020 proceeds to a step 3212, wherein it is determined whether the website has released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102.

When, at the step 3210, it is determined that the timeout period elapsed before the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102, the routine 3020 proceeds to the step 3220 (discussed above).

When, at the step 3210, it is determined that the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102 before the timeout period elapsed, the routine 3020 proceeds to a step 3216, wherein a message is displayed to the user concerning the successful validation of the new Pocket Vault holder.

After the step 3216, the routine 3020 terminates.

When, at the step 3202, it is determined that the new holder has indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3218, wherein a check is made to verify the holder's identity. The holder may, for example, be required to enter personal information, such as name, contact information, and security information to verify his or her identity.

When, at the step 3218, it is determined that the holder has successfully verified his or her identity, the routine 3020 proceeds to the step 3206 (discussed above), with the holder's previously-stored account information being used for the new Pocket Vault 102.

When, at the step 3218, it is determined that the holder has not successfully verified his or her identity, the routine 3020 proceeds to the step 3220 (discussed above).

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine 3024 shown in Fig. 30.

As shown, the routine 3024 begins at a step 3302, wherein it is determined whether the Pocket Vault 102 has been authenticated, e.g., whether the Pocket Vault 102 has determined that a fingerprint applied to the fingerprint scanner 220 matches one of the fingerprints stored in the fingerprint memory of the Pocket Vault 102. This authentication procedure may operate as described above in connection with the step 712 (Fig. 7), or an additional or different routine may be employed (e.g., as part of the security module 2812 described above in connection with Fig. 28) to determine whether the holder has successfully authenticated his or her identity, thereby enabling the network server 114 to establish a "trust" relationship with the Pocket Vault 102.

When, at the step 3302, it is determined that the Pocket Vault 102 has not been properly authenticated, the routine 3024 proceeds to a step 3304, wherein the holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault

102 while the Pocket Vault 102 is interfaced with the interface unit 302, i.e., while keeping the connection established between the Pocket Vault 102 and the website on the network server 114.

As shown, the step 3306 determines whether the Pocket Vault 102 has been properly authenticated prior to the expiration of a timeout period.

When, at the step 3306, it is determined that the timeout period elapsed before the Pocket Vault 102 was authenticated, the routine 3024 proceeds to a step 3308, wherein a message is displayed indicating that the authentication attempt was unsuccessful.

After the step 3308, the routine 3024 terminates.

When, at the step 3302, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 3024 proceeds to a step 3310, wherein the communication driver 2712 causes the internet settings 2722 of the interface station computer 304 to be adjusted to reflect certain internet settings stored in the Pocket Vault 102, e.g., by the internet settings management module 2806. In this manner, the internet settings of the Pocket Vault 102 may be "ported" to the interface station computer 304 so that the browser operating on the interface station computer 304 may take advantage of those settings while the Pocket Vault 102 is connected to the website on the network server 114 via the communication driver 2712. The internet settings of the Pocket Vault 102 that may be ported to the interface station computer 304 in this manner may comprise, for example, the network name and identification of the Pocket Vault 102, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The internet settings on the Pocket Vault 102, and porting of the same to the interface station computer 304, may be managed, for example, by one or more modules of the control software, e.g., the internet settings management module 2806. In one embodiment, the user may elect which internet settings are to be ported to the interface station computer 304 during the step 3310. This functionality may be accomplished, for example, during a SET PREFERENCES routine 3324 (described below in connection with Fig. 39).

After the step 3310, the routine 3024 proceeds to a step 3312, wherein it is determined whether one of several "functions" has been selected. In the illustrative embodiment shown,

the seven available functions are: (1) CARD LOADING (see CARD LOADING routine 3314 -- discussed below in connection with Fig. 34), (2) SYNCHRONIZATION (see SYNCHRONIZATION routine 3316 -- discussed below in connection with Fig. 35), (3) RECOVERY (see RECOVERY routine 3318 -- discussed below in connection with Fig. 36), (4) IDENTITY PORTING OPTIONS (see IDENTITY PORTING OPTIONS routine 3320 -- discussed below in connection with Fig. 337), (5) BACKUP (see BACKUP routine 3322 -- discussed below in connection with Fig. 38), (6) SET PREFERENCES (see SET PREFERENCES routine 3324 -- discussed below in connection with Fig. 39), AND (7) TERMINATE SESSION (see step 3326). It should be appreciated that the invention is not limited to the specific functions shown, and that additional, different or fewer functions may be employed.

It should further be appreciated that some or all of the illustrated functions, or operations relating to such functions, may be initiated automatically or may require user initiation, depending on the setting of preferences. For example, the SYNCHRONIZATION routine 3316 may be initiated automatically after completion of the step 3310, if preferences so indicate. Alternatively, certain steps required to accomplish synchronization of the Pocket Vault 102 and the website on the network server 114 may be taken, without actually completing the synchronization. For example, the synchronization module 2808 of the control software 2708 may automatically initiate a comparison of the contents of the Pocket Vault 102 and the website to determine what data should be transferred if synchronization is initiated. Software on the network server 114 may also or alternatively perform a similar comparison function automatically, if so desired.

Moreover, it should be understood that, in some embodiments, some of the above-noted functions may be performed without first requiring a Pocket Vault 102 to be authenticated. For example, some functions may involve the transfer of public or non-sensitive data, and may not require protection via the authentication verification step 3302.

As shown in Fig. 33, when any of the above-listed seven functions is selected, either automatically or in response to user input, the selected function is performed. For each of functions 3314, 3316, 3318, 3320, 3322, and 3324, after performing the routine associated with the function, the routine 3024 proceeds to a step 3332, wherein it is determined whether the connection between the Pocket Vault 102 and the website on the network server 114 is still established.

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is still established, the routine 3024 returns to the step 3312 (discussed above).

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is no longer established, the routine 3024 proceeds to a step 3327, wherein some or all of the internet settings 2722 are ported from the interface station computer 304 to the Pocket Vault 102. The communication driver 3712 may cause the settings to be ported directly to the Pocket Vault 102 from the interface station computer 304 (via the interface unit 302), or the settings may be transferred first to the network server 114 and then to the Pocket Vault 102 (via the connection between the network server 114 and the Pocket Vault 102). In some embodiments, only certain types or classes of settings, e.g., certain type of cookies, PKI certificates, etc., are ported from the interface station computer 304 to the Pocket Vault 102 in this manner. The classes or types of settings that are ported during the step 3327 may, for example, be determined by the user in some embodiments. For example, the user may set certain preferences, e.g., during the SET PREFERENCES routine 3324 or by manipulating the Pocket Vault 102 directly, that control the nature and type of internet settings that are ported to the Pocket Vault 102 from the interface station computer 304 during the step 3327.

After the step 3327, the routine 3024 proceeds to a step 3328, wherein the communication driver 2712 causes the internet settings 2722 on the interface station computer 304 to return to their original state, i.e., the configuration the internet settings 2712 were in before they were altered in the step 3310.

After the step 3328, the routine 3024 proceeds to a step 3330, wherein any cached web pages or other information temporarily stored in the interface station computer 304 during the communication session between the Pocket Vault 102 and the website on the network server 114 are deleted from cache and other memory in the interface station computer 304. Thus, after completion of the step 3330, the interface station computer 304 is in essentially the same state it was in prior to the beginning of the routine 1422. The communication driver 2712 may remain on the interface station computer 304 or may be deleted in connection with the step 3330. If the communication driver 2712 is kept on the interface station computer 304, any cache or other memory associated with it that might store personal or sensitive information may also be erased. In some embodiments, the

communication driver 2712 caches or stores very little, if any, information that is passed between the Pocket Vault 102 and the website on the network server 114. In any event, the communication driver 2712 may be constructed such that no useful data, i.e., data that reflects any personal or sensitive information, remains on it after completion of the step 3330.

When, at the step 3312, the holder chooses the TERMINATE SESSION function, the connection between the Pocket Vault 102 and the website on the network server 114 is de-established, and the routine 3024 proceeds immediately to the steps 3327, 3328 and 3330 (discussed above).

After the step 3330, the routine 3024 terminates.

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine 3314 shown in Fig. 33.

As shown, the routine 3314 begins at a step 3402, wherein a determination is made as to whether the card desired to be loaded is "swipeable." The user may, for example, be prompted to indicate whether the card has an operational magnetic stripe disposed thereon.

When, at the step 3402, the user indicates that the card does not have an operational magnetic stripe, the routine 3314 proceeds to a step 3406, wherein the user is prompted (e.g., via the browser on the interface station computer 304) to input information to be used in creating a card account.

When, at the step 3402, the user indicates that the card does have an operational magnetic stripe, the routine 3314 proceeds to the step 3410, wherein the user is prompted to swipe the card through the stripe reader 315 of the interface unit 302.

After the step 3406, the routine 3314 proceeds to steps 3408 and 3409, wherein it is determined whether the interface station computer 304 has received the information from a card swiped through the stripe reader 315 of the interface unit 302 prior to the expiration of a timeout period.

When, at the step 3409, it is determined that the timeout period elapsed before information from a swiped card was received, the routine 3314 proceeds to a step 3411, wherein a message is displayed to the user concerning the failure to properly read the magnetic stripe.

After the step 3411, the routine 3314 returns to the step 3402 (discussed above). Thus, when a user is unsuccessful in swiping a card one or more times, the user may determine that the magnetic stripe is non-operational, and may indicate at the step 3402 that

the card is not swipeable. The user may thereafter create an account for the card manually at the step 3410 (discussed above).

After the step 3410, the routine proceeds to a step 3412, wherein the website on the network server 114 determines whether the account for the card is valid. This determination may be made, for example, by confirming that the card is owned by the person attempting to add it to his or her Pocket Vault 102, that the card has not expired, etc.

When, at the step 3408, it is determined that information from the swiped card has been received prior to the expiration of the timeout period, the routine 3314 proceeds to the step 3412 (discussed above), wherein a determination is made as the validity of the account based upon the information read by the stripe reader 315.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is not valid, the routine 3314 proceeds to a step 3414 wherein appropriate security precautions are taken.

After the step 3414, the routine 3314 terminates.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is valid, the routine 3314 proceeds to a step 3416, wherein the information for the card is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3416, the routine 3314 proceeds to a step 3418, wherein a message is displayed that indicates the card has been successfully loaded onto the Pocket Vault 102 for use in future transactions.

After the step 3418, the routine 3314 terminates.

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine 3316 shown in Fig. 33.

As shown, the routine 3316 begins at a step 3502, wherein certain parameters required to synchronize the Pocket Vault 102 to the website on the network server 114 are determined based upon user preferences and the ID of the Pocket Vault 102. For example, if a holder has two or more Pocket Vaults 102, the holder may wish to elect one of them to be a master for synchronization purposes, or the holder may even elect to have the website act as the master. When a holder has more than one Pocket Vault 102, the holder also may desire to be prompted to select either the current date or the date of the last synchronization as the basis for the synchronization operation.

After the step 3502, the routine 3316 proceeds to a step 3504, wherein the website on the network server 114 generates sets of current data to transfer to the Pocket Vault 102. The website may, for example, compare its current data to the data stored on the Pocket Vault 102 so as to identify any data it needs to receive from the Pocket Vault 102 to properly synchronize therewith.

After the step 3504, the routine 3316 proceeds to steps 3506 and 3508, wherein it is determined whether the Pocket Vault 102 has indicated that it is ready to synchronize prior the expiration of a timeout period (measured by the step 3508). The Pocket Vault 102 may, for example, also be performing a similar comparison (e.g., using the synchronization module 2808) between its data and the data stored on the website of the network server to determine what data it needs to receive from the website to properly synchronize therewith.

When at the step 3508, it is determined that the timeout period has elapsed before the Pocket Vault 102 had indicated its readiness to synchronize, the routine 3316 proceeds to a step 3510, wherein a message is generated indicating the attempt to synchronize the Pocket Vault 102 with the website on the network server 114 has failed.

After the step 3510, the routine 3316 terminates.

When at the step 3506, it is determined that the Pocket Vault 102 has indicated its readiness to synchronize with the website prior to the expiration of the timeout period, the routine 3316 proceeds to a step 3512, wherein accumulated synchronization data is transferred from the website to the Pocket Vault 102, and vice versa, via the communication driver 2712.

After the step 3512, the routine 3316 proceeds to a step 3516, wherein the date of the successful synchronization is stored in both the Pocket Vault 102 and the network server 114.

After the step 3516, the routine 3316 proceeds to a step 3518, wherein a message is generated indicating that the Pocket Vault 102 has been successfully synchronized with the website on the network server 114.

After the step 3518, the routine 3316 terminates.

Figure 36 is a flow diagram illustrating an example implementation of the RECOVERY routine 3318 shown in Fig. 33.

As shown, the routine 3318 begins at a step 3602, wherein the website on the network server 114 compiles all data necessary to recover the Pocket Vault 102 to its state as of the last time its contents were synchronized with the website of the network server 114 (e.g.,

using the routine 3316 – described above) or backed up on the website of the network server 114 (e.g., using routine 3322 – described below).

After the step 3602, the routine 3318 proceeds to step 3604, wherein the data compile in the step 3602 is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712, and a determination is made as to where that downloading has completed prior to the expiration of a timeout period measured at the step 3606.

When, at the step 3606, it is determined that the timeout period elapsed prior to the downloading being completed, the routine 3318 proceeds to a step 3608, wherein a message is generated indicating that the attempted recovery was unsuccessful.

After the step 3606, the routine 3318 terminates.

When, at the step 3606, it is determined that the downloading was completed in a timely manner, the routine 3318 proceeds to a step 3610, wherein a message is generated indicating that the attempted recovery of data to the Pocket Vault 102 was successful.

After the step 3610, the routine 3318 terminates.

Figure 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine 3320 shown in Fig. 33.

As shown, the routine 3320 begins at a step 3702, wherein the internet settings 2722 from the interface station computer 304 are downloaded from the interface station computer 304 to the website on the network server 114.

After the step 3702, the routine 3320 proceeds to a step 3704, wherein the website on the network server 114 compiles and displays the downloaded internet settings to the user via the browser on the interface station computer 304. The settings may be displayed to the user in any of a number of ways. Preferably, the settings are displayed in a manner that enables the user to readily distinguish between various classes of settings, and that permits the user to readily identify the purpose of each type of setting. In some embodiments, only a subset of the all of the internet settings 2722 (e.g., only settings such as cookies and PKI certificates) are transferred to the website for possible modification by the user.

After the step 3704, the routine 3320 proceeds to steps 3706 and 3708, wherein the user is given an opportunity to modify the displayed internet settings. The user may, for example, elect to keep certain cookies that were retained among the internet settings 2722, while choosing to discard others.

When at the step 3708, the user has indicated that he or she has completed any modifications of the retrieved internet settings 2722, the routine 3320 proceeds to a step 3710, wherein the modified internet settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3710, the routine 3320 terminates.

When at the step 3706, it is determined that the user did not elect to modify any settings, the routine 3320 terminates.

Figure 38 is a flow diagram illustrating an example implementation of the BACKUP routine 3322 shown in Fig. 33.

As shown, the routine 3322 begins at a step 3802, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, asking the Pocket Vault 102 to send the website backup data. This backup data may, for example, constitute all data necessary to place the Pocket Vault 102 back into its present state if any portion of data on the Pocket Vault 102 was lost, or to place a new Pocket Vault 102 into the same state as the backed up Pocket Vault 102 (e.g., using the RECOVERY routine 3318 – discussed above).

After the step 3802, the routine 3322 proceeds to steps 3804 -3806, wherein it is determined whether the requested backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 before the expiration of a timeout period (measured by the step 3806).

When, at the step 3806, it is determined that the timeout period elapsed prior to the backup data being successfully transferred, the routine 3322 proceeds to a step 3808, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that a communication error has occurred and that the backup operation was unsuccessful.

After the step 3808, the routine 3322 terminates.

When, at the step 3804, the routine 3322 determined that, before the timeout period, the backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712, the routine 3322 proceeds to a step 3810, wherein the received backup data is stored by the network server 114, e.g., for use in connection with the RECOVERY routine 3318.

After the step 3310, the routine 3322 proceeds to a step 3812, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the backup operation was successfully completed.

After the step 3312, the routine 3322 terminates.

Figure 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine 3324 shown in Fig. 33. The SET PREFERENCES routine 3324 permits the holder to set or alter preferences on his or her Pocket Vault 102 using a browser on the interface station computer 104.

As shown, the routine 3324 begins at a step 3902, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, requesting the Pocket Vault 102 to transmit all "preferences" information stored on the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712. This information may, for example, comprise definitions of home pages, connection of secure and non-secure media, order of media presentment, sort orders, user interface options, synchronization defaults, etc.

After the step 3902, the routine 3324 proceeds to steps 3904 and 3906, wherein it is determined whether the preferences information has been received from the Pocket Vault 102 prior to the expiration of a timeout period (measured by the step 3906).

When, at the step 3906, it is determined that the timeout period elapsed before the preferences information was transferred from the Pocket Vault 102 to the website, the routine 3324 proceeds to a step 3908, wherein a message is displayed (e.g., on the browser) indicating that a communication error has occurred.

After the step 3908, the routine 3324 terminates.

When, at the step 3904, it is determined that the preferences information has been successfully transferred from the Pocket Vault 102 to the website on the network server 114, the routine 3324 proceeds to a step 3910, wherein the website compiles and displays the current preference settings for the Pocket Vault 102 (e.g., on the browser) in a user friendly manner.

After the step 3910, the routine 3324 proceeds to steps 3912 and 3914, wherein the user is given an opportunity to modify the displayed preference settings.

When, at the step 3912, the user opts not to modify any of the displayed settings, the routine 3324 terminates.

When, at the steps 3912 and 3914, the user opts to modify the displayed settings and indicates that he or she has completed modification thereof, the routine 3324 proceeds to a step 3916, wherein the modified preference settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3918, a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the preference settings for the Pocket Vault 102 were successfully modified.

After the step 3918, the routine 3324 terminates.

One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time-sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who make room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room.

After the time period of the guest's room reservation has expired, the Pocket Vault 102 may automatically delete the room key icon. This deletion may occur for the convenience of the Pocket Vault holder, not necessarily for hotel security reasons, since the room's lock will reject any previously-used key card (Chameleon or traditional key card) after the key card's specified time period has expired.

Having thus described at least one illustrative embodiment of the invention, various alterations, modifications and improvements will readily occur to those skilled in the art. Such alterations, modifications and improvements are intended to be within the spirit and scope of the invention. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention is limited only as defined in the following claims and the equivalents thereto.

What is claimed is:

CLAIMS

1. A method for enabling a software module on a computer operated by a user to access restricted information on a server, comprising steps of:

(A) with an electronic device distinct from the computer, authenticating an identity of the user to determine that the user is permitted to access the restricted information on the server; and

(B) in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

2. The method of claim 1, wherein the step (A) comprises comparing, with the electronic device, a measured bio-metric parameter of the user with a stored bio-metric parameter of the user.

3. The method of claim 1, further comprising a step of:

(C) accessing, with the software module on the computer, the restricted information on the server.

4. The method of claim 3, further comprising a step of:

(D) establishing a connection between the electronic device and the server.

5. The method of claim 4, wherein the step (D) includes establishing the connection via a driver in the computer.

6. The method of claim 4, further comprising steps of:

(D) in response to input to the computer by the user, altering settings stored on the server; and

(E) transmitting a signal from the server to the electronic device via the connection, the signal causing the settings on the electronic device to be changed to correspond to the altered settings stored on the server.

7. The method of claim 1, further comprising a step of:

(C) transmitting a signal from the computer to the server, which signal indicates that the electronic device has authenticated the identity of the user of the computer and determined that the user is permitted to access the restricted information on the server.

8. A method for altering settings on a computer to correspond to settings on an electronic device distinct from the computer, comprising steps of:

(A) with the electronic device, authenticating an identity of a user to determine that the user is authorized to use the electronic device; and

(B) in response to authenticating the identity of the user to determine that the user is authorized to use the electronic device, altering the settings on the computer to correspond to settings on the electronic device.

9. The method of claim 8, further comprising a step of:

(C) with the computer, accessing a server based upon the settings on the computer.

10. The method of claim 9, further comprising a step of:

(D) establishing a connection between the electronic device and the server.

11. The method of claim 10, wherein the step (D) includes establishing the connection via a driver in the computer.

12. The method of claim 11, wherein the step (B) includes, using the driver to update the settings on the computer.

13. The method of claim 10, further comprising steps of:

(E) altering the settings on the computer in response to user input to the computer; and

(F) transferring at least some of the altered settings on the computer to the electronic device when the connection is de-established.

14. The method of claim 10, further comprising a step of:

(E) restoring the settings on the computer to their original state when the connection is de-established.

15. The method of claim 8, wherein the step (A) comprises comparing, with the electronic device, a measured bio-metric parameter of the user with a stored bio-metric parameter of the user.

16. The method of claim 8, wherein the settings comprise at least one of a bookmark list, a web site cookie, an encoding of a user password, and personal user data.

17. A system for enabling a software module on a computer operated by a user to access restricted information on a server, comprising:

an electronic device distinct from the computer, the electronic device including a user-authenticator to authenticate an identity of the user to determine that the user is permitted to access the restricted information on the server; and

means for, in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

18. The system of claim 17, wherein the user authenticator includes a bio-metric authenticator.

19. The system of claim 17, further comprising:

means for accessing, with the software module on the computer, the restricted information on the server.

20. The system of claim 19, further comprising:

means for establishing a connection between the electronic device and the server.

21. The system of claim 19, further comprising:

means for, in response to input to the computer by the user, altering settings stored on the server; and

means for transmitting a signal from the server to the electronic device via the connection, the signal causing the settings on the electronic device to be changed to correspond to the altered settings stored on the server.

22. The method of claim 17, further comprising:

means for transmitting a signal from the computer to the server, which signal indicates that the electronic device has authenticated the identity of the user of the computer and determined that the user is permitted to access the restricted information on the server.

23. A system for altering settings on a computer to correspond to settings on an electronic device distinct from the computer, comprising:

a user authenticator included in the electronic device to authenticate an identity of a user to determine that the user is authorized to use the electronic device; and

means for, in response to authenticating the identity of the user to determine that the user is authorized to use the electronic device, altering the settings on the computer to correspond to settings on the electronic device.

24. The system of claim 23, further comprising:

means for accessing a server with the computer based upon the settings on the computer.

25. The system of claim 24, further comprising:

means for establishing a connection between the electronic device and the server.

26. The system of claim 25, further comprising:

means for altering the settings on the computer in response to user input to the computer; and

means for transferring at least some of the altered settings on the computer to the electronic device when the connection is de-established.

27. The system of claim 25, further comprising:

means for restoring the settings on the computer to their original state when the connection is de-established.

28. The system of claim 23, wherein the user authenticator includes a bio-metric authenticator.

29. The system of claim 23, wherein the settings comprise at least one of a bookmark list, a web site cookie, an encoding of a user password, and personal user data.

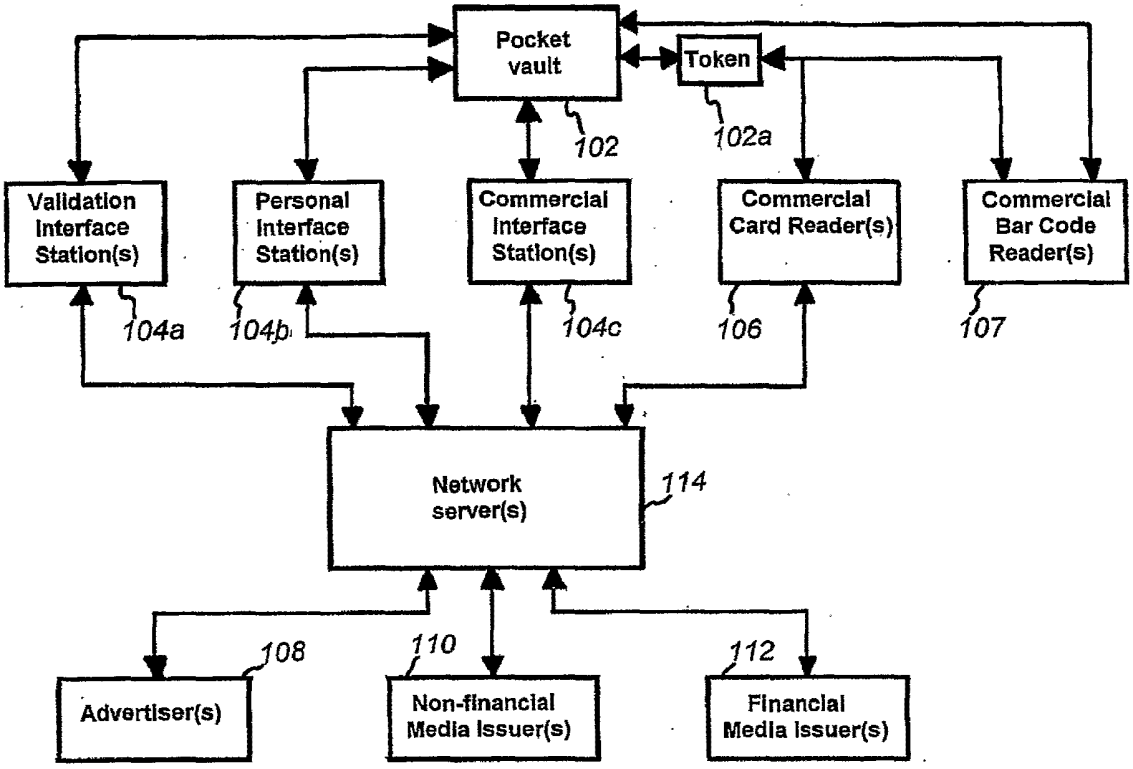

Pocket vault
Token
102
102a
Validation Interface Station(s)
Personal Interface Station(s)
Commercial Interface Station(s)
Commercial Card Reader(s)
Commercial Bar Code Reader(s)
104a
104b
104c
106
107
Network server(s)
114
Advertiser(s)
Non-financial Media Issuer(s)
Financial Media Issuer(s)
108
110
112

Fig. 1

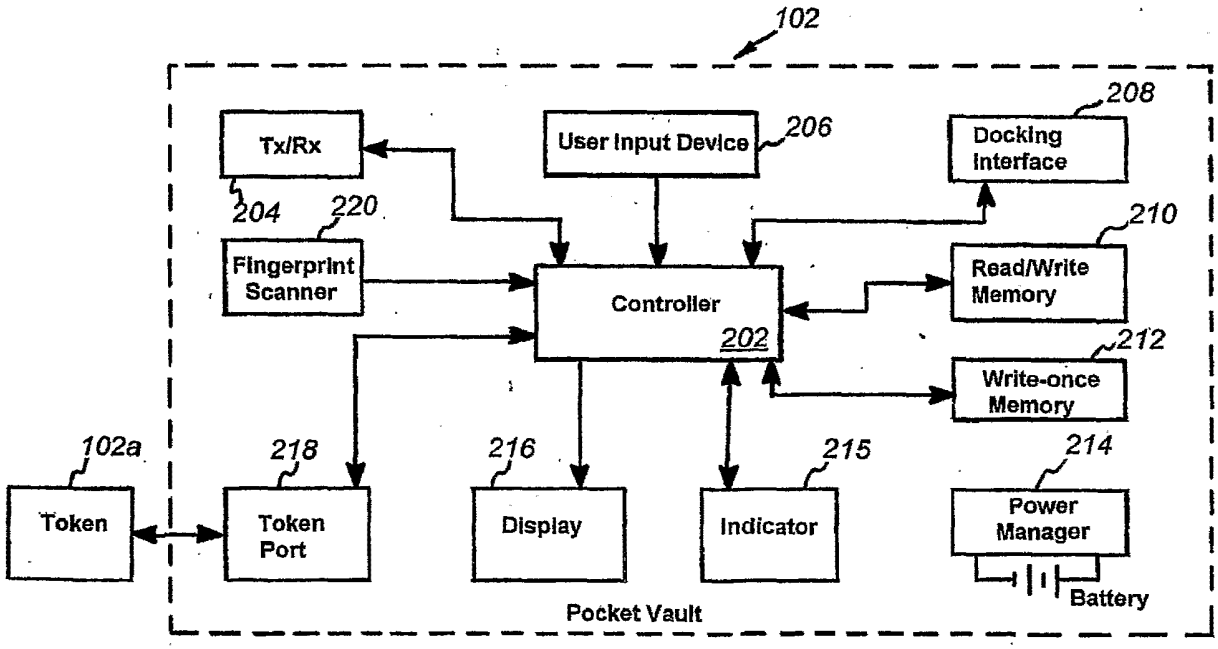

102
Tx/Rx
204
User Input Device
206
Docking Interface
208
220
Fingerprint Scanner
Controller
202
Read/Write Memory
210
Write-once Memory
212
102a
Token
218
Token Port
216
Display
215
Indicator
214
Power Manager
Battery
Pocket Vault

Fig. 2

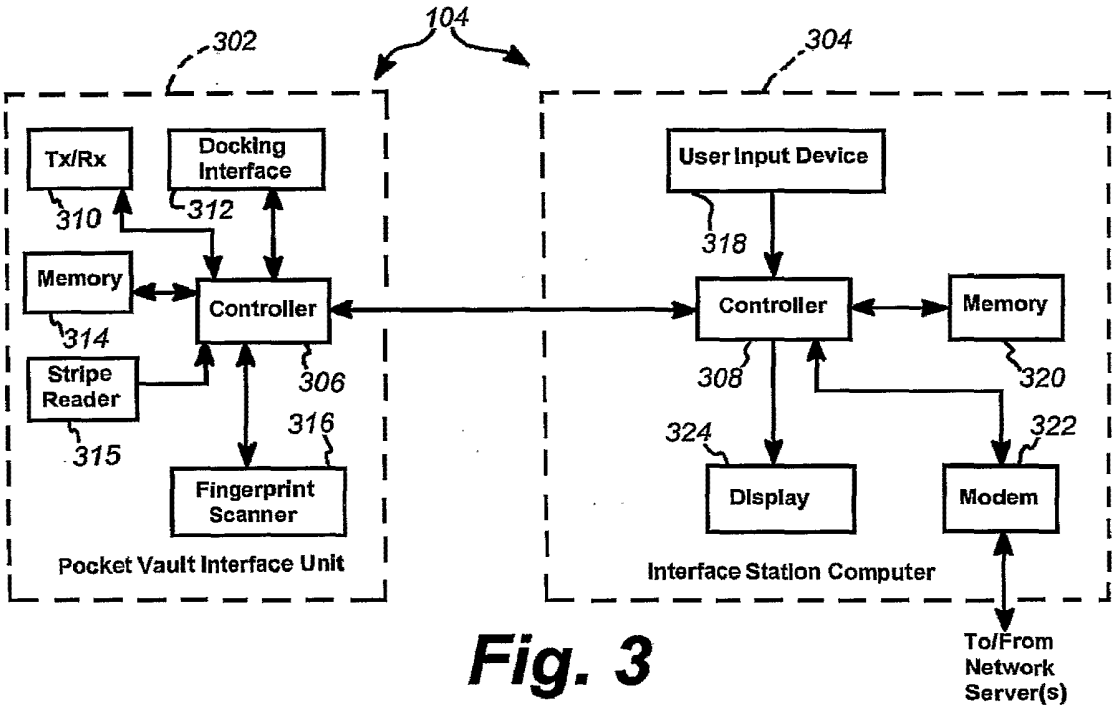

104
302
304
Tx/Rx
Docking Interface
310
312
Memory
Controller
314
306
Stripe Reader
315
316
Fingerprint Scanner
Pocket Vault Interface Unit
User Input Device
318
Controller
Memory
308
320
324
322
Display
Modem
Interface Station Computer
To/From Network Server(s)

Fig. 3

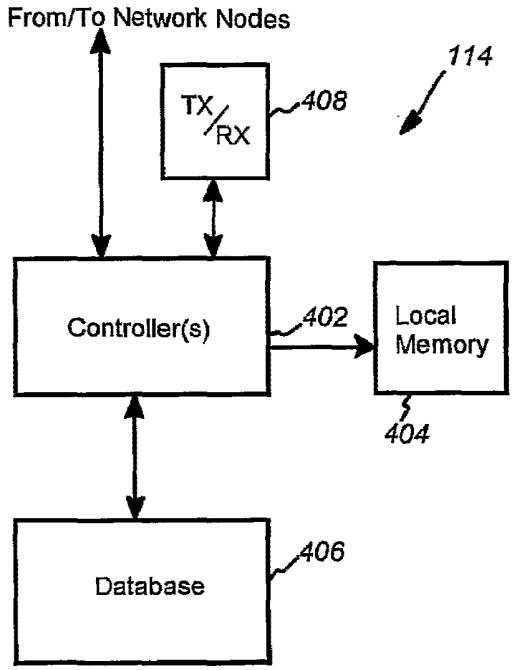

From/To Network Nodes
114
TX/RX
408
Controller(s)
402
Local Memory
404
Database
406

Fig. 4

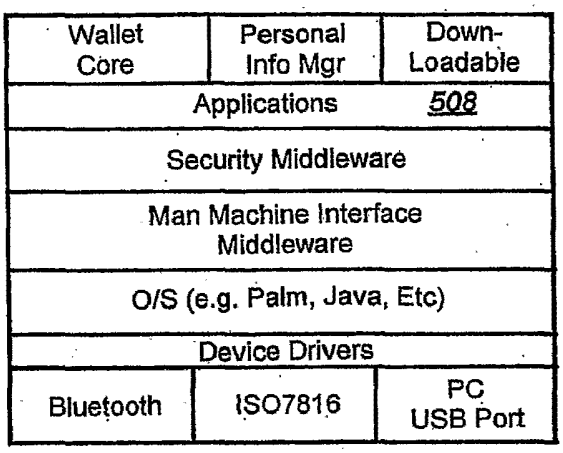

Wallet Core
Personal Info Mgr
Down-Loadable
Applications 508
Security Middleware
Man Machine Interface Middleware
O/S (e.g. Palm, Java, Etc)
Device Drivers
Bluetooth
ISO7816
PC USB Port

Fig. 5

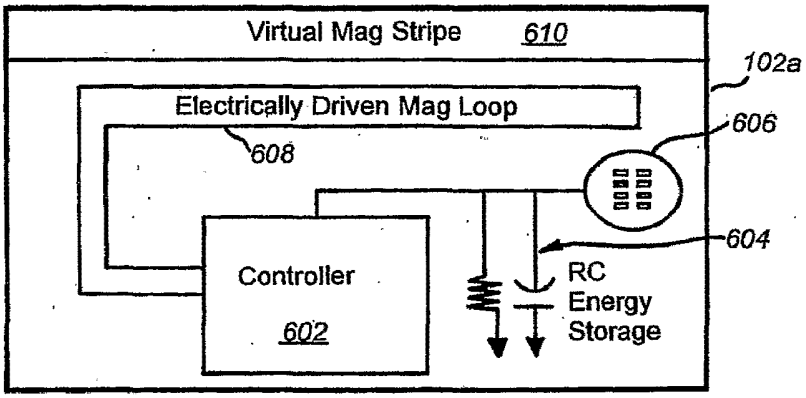

Virtual Mag Stripe 610
102a
Electrically Driven Mag Loop
606
608
604
Controller
602
RC
Energy
Storage

Fig. 6

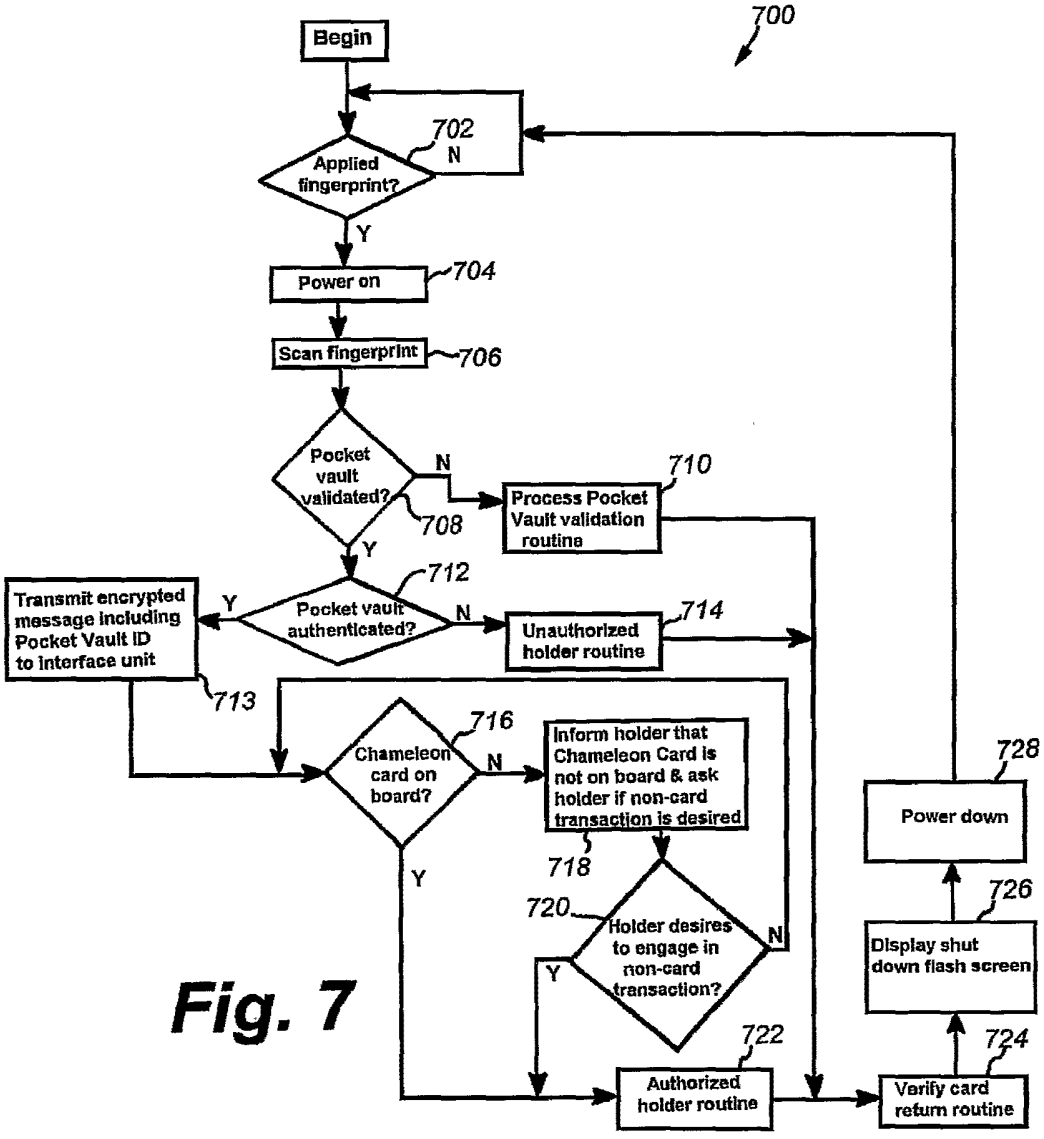

700
Begin
Applied fingerprint?
702
N
Y
Power on
704
Scan fingerprint
706
Pocket vault validated?
N
708
710
Process Pocket Vault validation routine
Y
Transmit encrypted message including Pocket Vault ID to interface unit
Y
Pocket vault authenticated?
712
N
Unauthorized holder routine
714
713
Chameleon card on board?
716
N
Inform holder that Chameleon Card is not on board & ask holder if non-card transaction is desired
718
Y
720
Holder desires to engage in non-card transaction?
N
Y
Authorized holder routine
722
Verify card return routine
724
Display shut down flash screen
726
Power down
728

Fig. 7

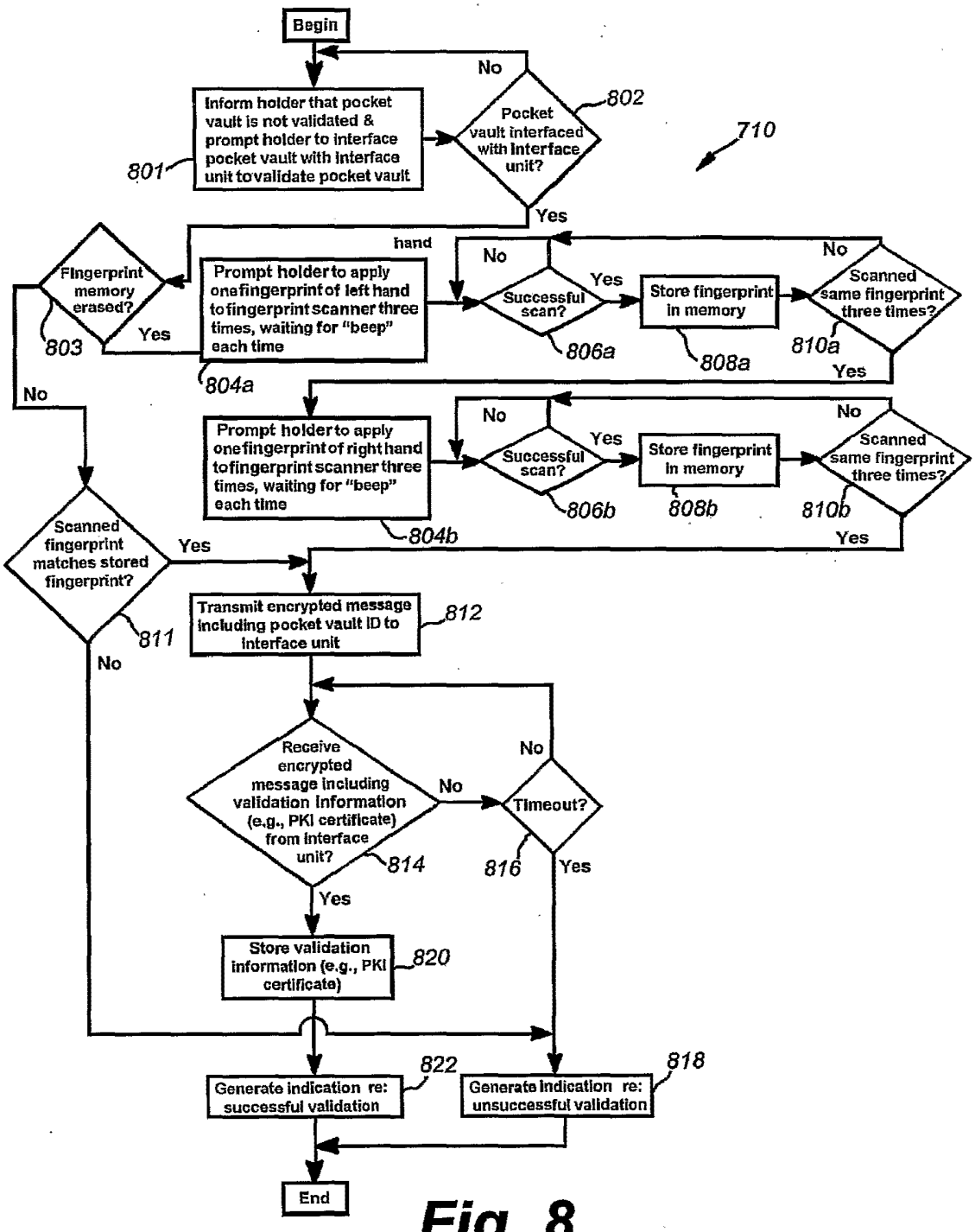

Begin
Inform holder that pocket vault is not validated & prompt holder to interface pocket vault with interface unit to validate pocket vault
801
Pocket vault interfaced with interface unit?
802
No
Yes
710
Fingerprint memory erased?
803
Yes
Prompt holder to apply one fingerprint of left hand to fingerprint scanner three times, waiting for "beep" each time
804a
Successful scan?
806a
No
Yes
Store fingerprint in memory
808a
Scanned same fingerprint three times?
810a
No
Yes
No
Prompt holder to apply one fingerprint of right hand to fingerprint scanner three times, waiting for "beep" each time
804b
Successful scan?
806b
No
Yes
Store fingerprint in memory
808b
Scanned same fingerprint three times?
810b
No
Yes
Scanned fingerprint matches stored fingerprint?
811
Yes
No
Transmit encrypted message including pocket vault ID to interface unit
812
Receive encrypted message including validation information (e.g., PKI certificate) from interface unit?
814
No
Yes
Timeout?
816
No
Yes
Store validation information (e.g., PKI certificate)
820
Generate indication re: successful validation
822
Generate indication re: unsuccessful validation
818
End

Fig. 8

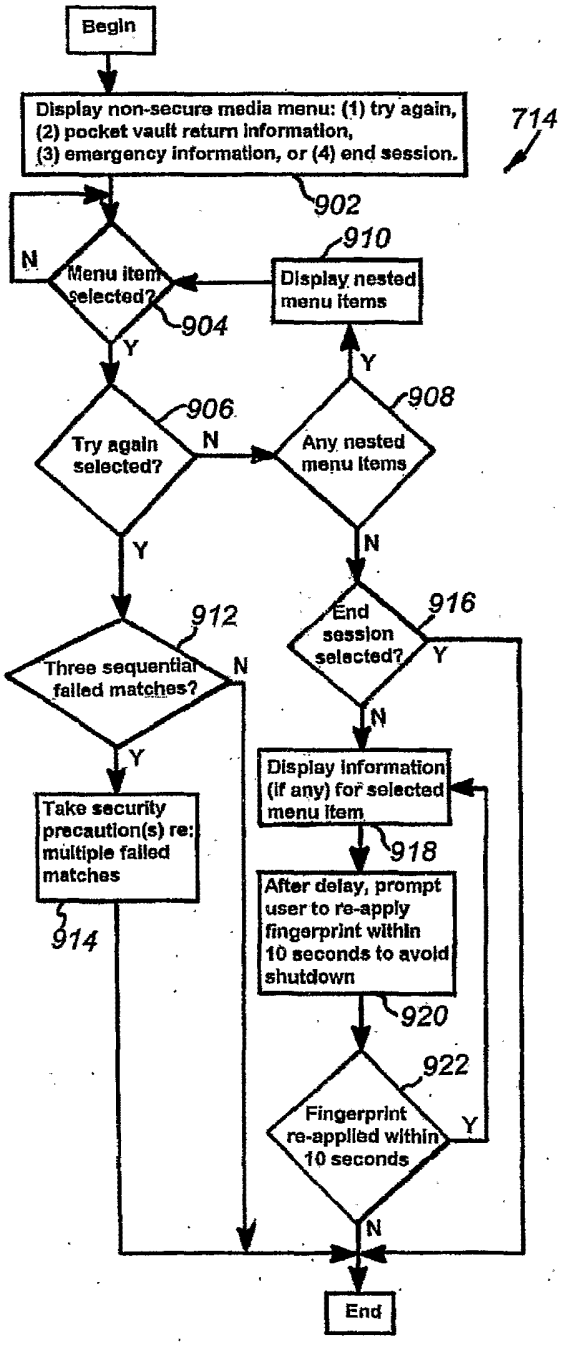

Begin
Display non-secure media menu: (1) try again, (2) pocket vault return information, (3) emergency information, or (4) end session.
714
902
910
Menu item selected?
904
Display nested menu items
N
Y
906
Try again selected?
908
Any nested menu items
912
Three sequential failed matches?
916
End session selected?
Take security precaution(s) re: multiple failed matches
914
Display information (if any) for selected menu item
918
After delay, prompt user to re-apply fingerprint within 10 seconds to avoid shutdown
920
922
Fingerprint re-applied within 10 seconds
End

Fig. 9

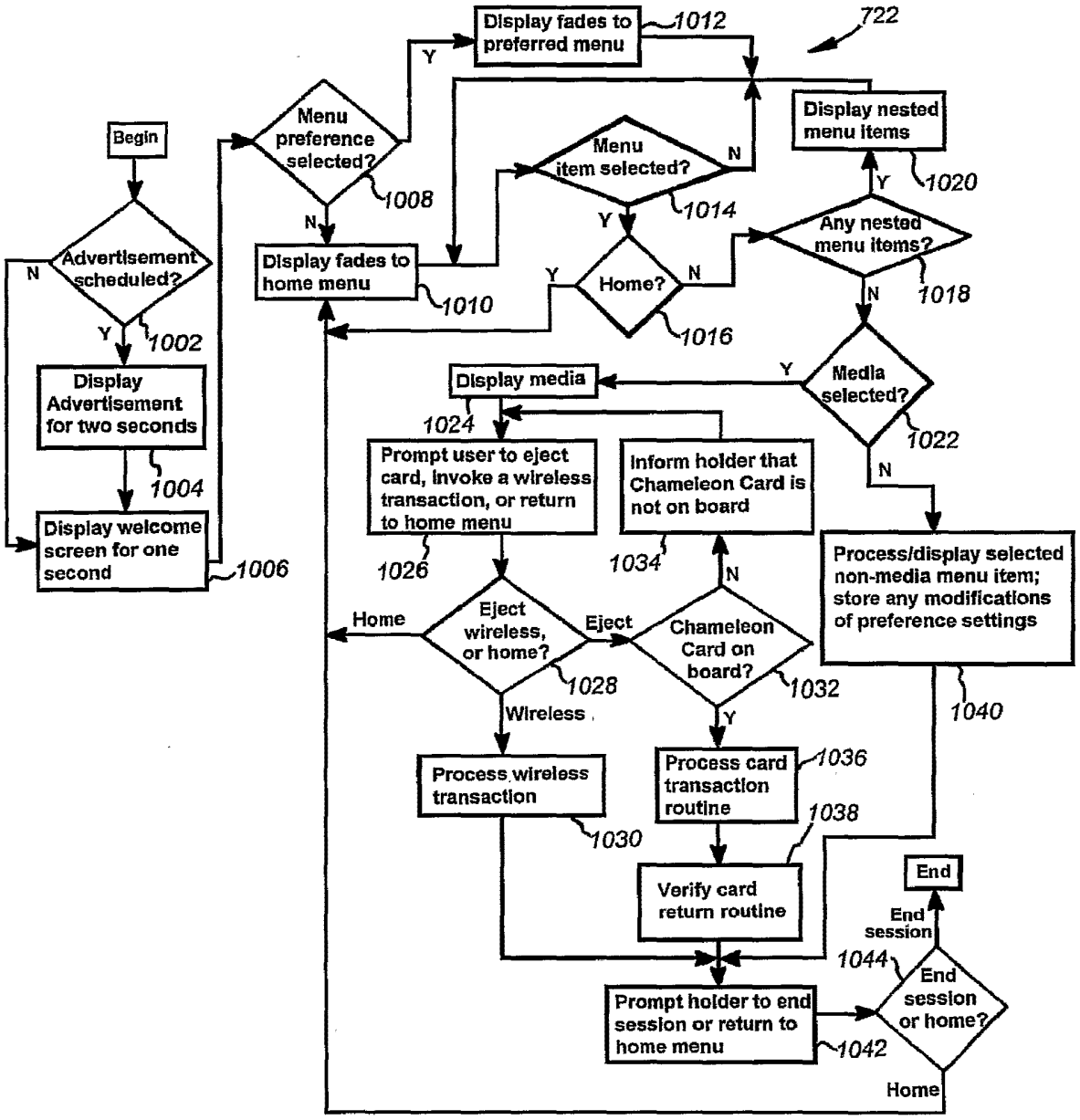

Begin
Advertisement scheduled?
1002
Display Advertisement for two seconds
1004
Display welcome screen for one second
1006
Menu preference selected?
1008
Display fades to home menu
1010
Display fades to preferred menu
1012
Menu item selected?
1014
Home?
1016
Any nested menu items?
1018
Display nested menu items
1020
Media selected?
1022
Display media
1024
Prompt user to eject card, invoke a wireless transaction, or return to home menu
1026
Eject wireless, or home?
1028
Process wireless transaction
1030
Chameleon Card on board?
1032
Inform holder that Chameleon Card is not on board
1034
Process card transaction routine
1036
Verify card return routine
1038
Process/display selected non-media menu item; store any modifications of preference settings
1040
Prompt holder to end session or return to home menu
1042
End session or home?
1044
End session
End
Home
Eject
Wireless
Y
N
722

Fig. 10

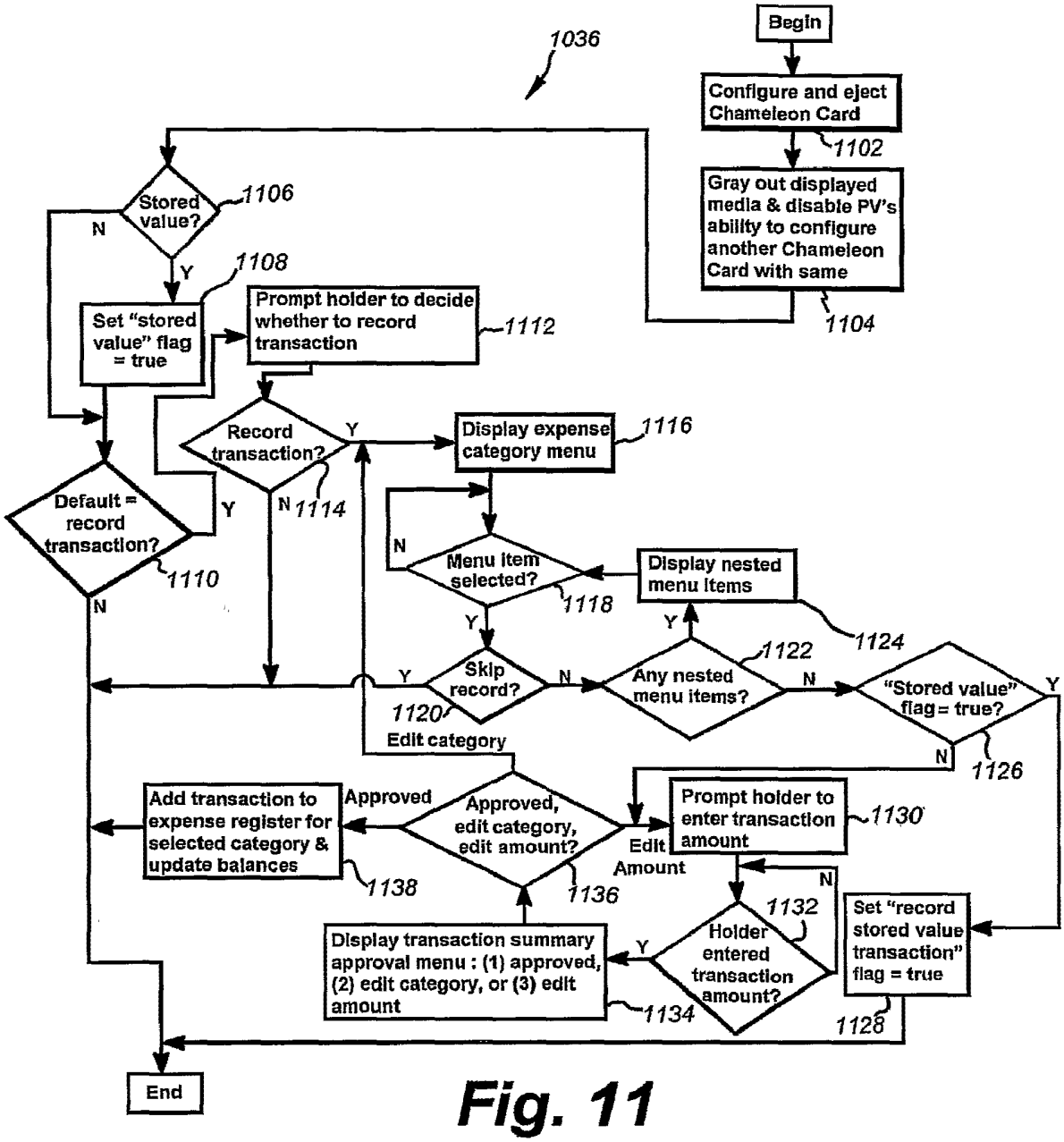

1036
Begin
Configure and eject Chameleon Card
1102
Gray out displayed media & disable PV's ability to configure another Chameleon Card with same
1104
Stored value?
1106
N
Y
1108
Set "stored value" flag = true
Prompt holder to decide whether to record transaction
1112
Record transaction?
Y
N
1114
Display expense category menu
1116
Default = record transaction?
Y
N
1110
N
Menu item selected?
1118
Display nested menu items
1124
Y
Y
Skip record?
Y
N
1120
Edit category
Any nested menu items?
1122
N
"Stored value" flag = true?
Y
N
1126
Add transaction to expense register for selected category & update balances
1138
Approved
Approved, edit category, edit amount?
1136
Edit Amount
Prompt holder to enter transaction amount
1130
N
1132
Holder entered transaction amount?
Y
Display transaction summary approval menu : (1) approved, (2) edit category, or (3) edit amount
1134
Set "record stored value transaction" flag = true
1128
End

Fig. 11

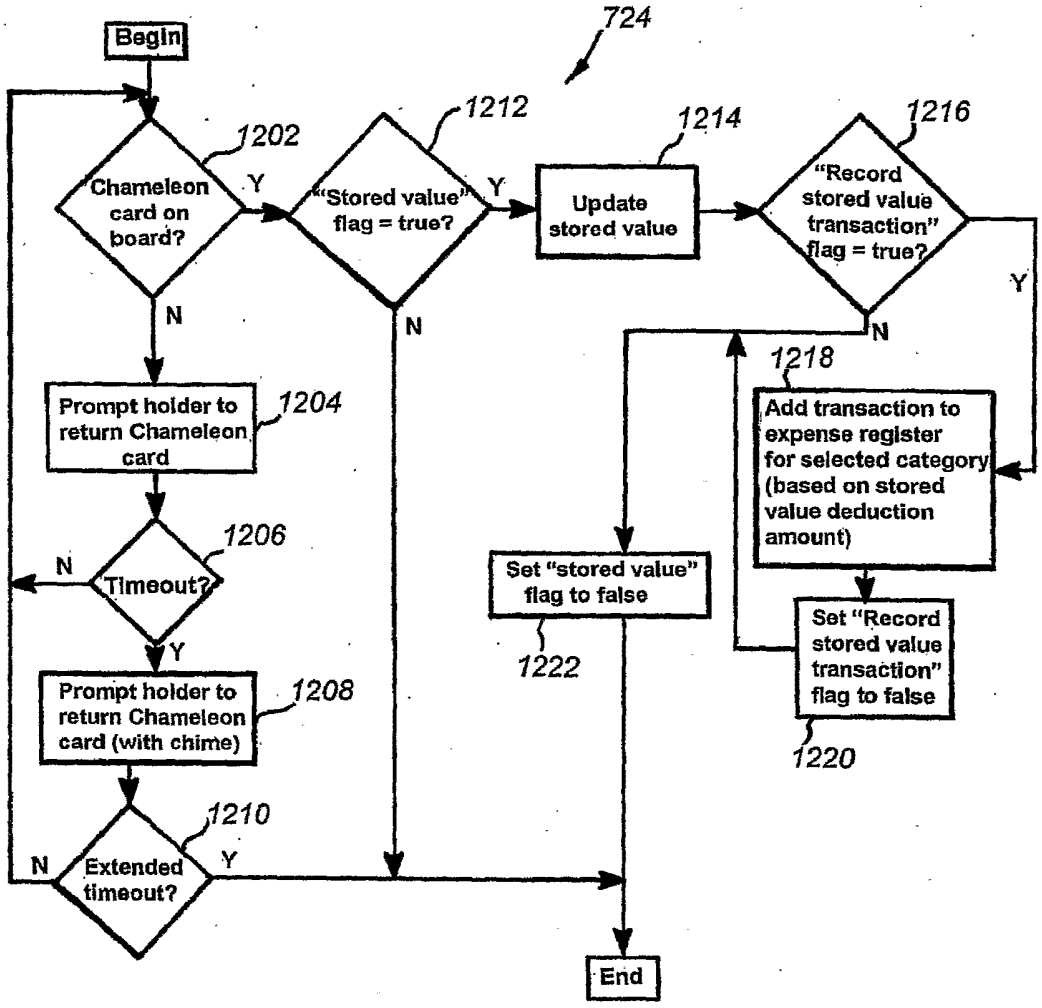

724
Begin
1202
Chameleon card on board?
Y
N
1212
"Stored value" flag = true?
Y
N
1214
Update stored value
1216
"Record stored value transaction" flag = true?
Y
N
1218
Add transaction to expense register for selected category (based on stored value deduction amount)
Set "Record stored value transaction" flag to false
1220
Set "stored value" flag to false
1222
Prompt holder to return Chameleon card
1204
1206
Timeout?
N
Y
Prompt holder to return Chameleon card (with chime)
1208
1210
Extended timeout?
N
Y
End

Fig. 12

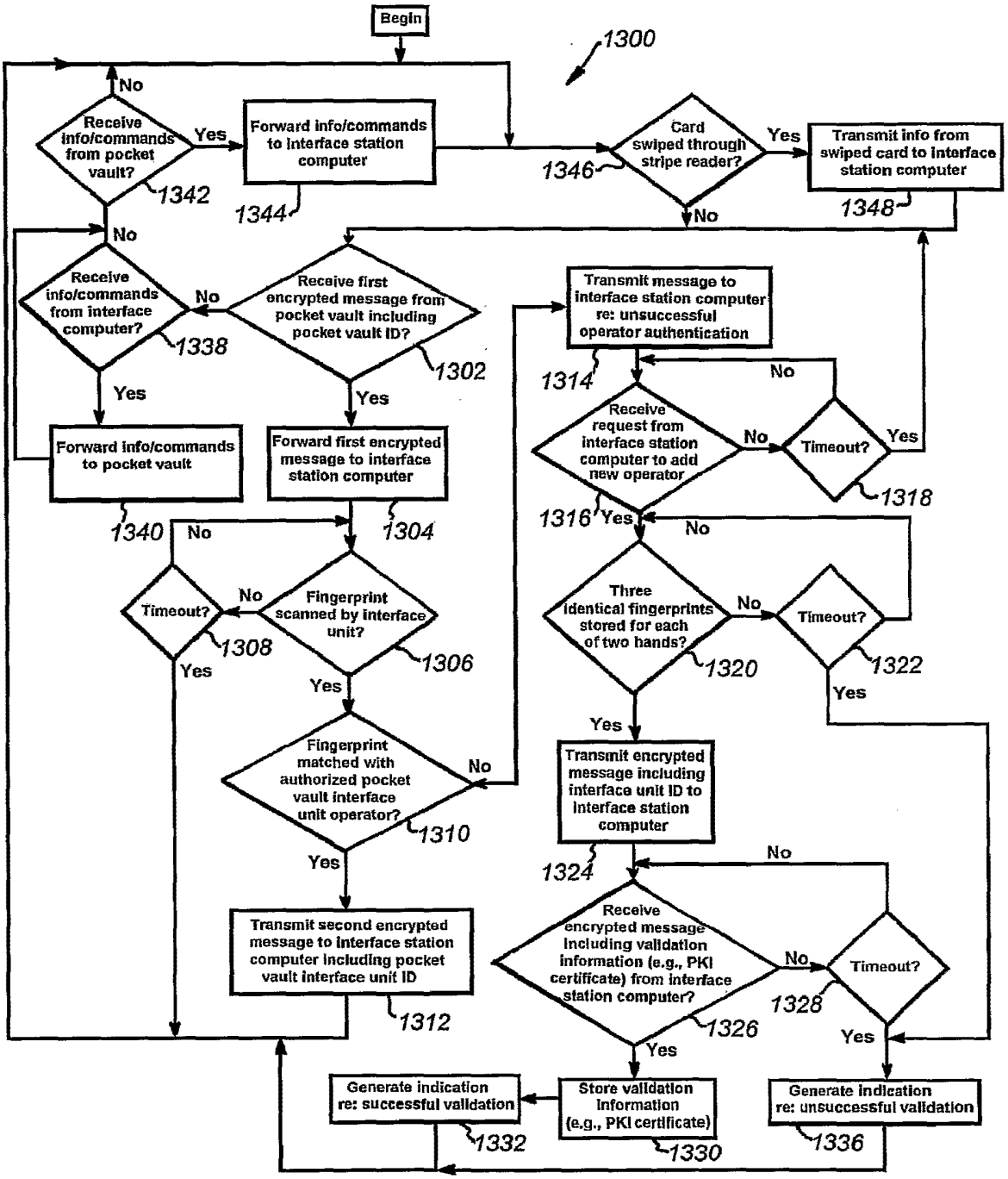

Begin
1300
Receive info/commands from pocket vault?
1342
Yes
No
Forward info/commands to interface station computer
1344
Card swiped through stripe reader?
1346
Yes
No
Transmit info from swiped card to interface station computer
1348
Receive info/commands from interface computer?
1338
No
Yes
Receive first encrypted message from pocket vault including pocket vault ID?
1302
Yes
No
Forward info/commands to pocket vault
1340
Forward first encrypted message to interface station computer
1304
Timeout?
1308
No
Yes
Fingerprint scanned by interface unit?
1306
No
Yes
Fingerprint matched with authorized pocket vault interface unit operator?
1310
No
Yes
Transmit second encrypted message to interface station computer including pocket vault interface unit ID
1312
Transmit message to interface station computer re: unsuccessful operator authentication
1314
Receive request from interface station computer to add new operator
1316
No
Yes
Timeout?
1318
No
Yes
Three identical fingerprints stored for each of two hands?
1320
No
Yes
Timeout?
1322
No
Yes
Transmit encrypted message including interface unit ID to interface station computer
1324
Receive encrypted message including validation information (e.g., PKI certificate) from interface station computer?
1326
No
Yes
Timeout?
1328
No
Yes
Store validation information (e.g., PKI certificate)
1330
Generate indication re: successful validation
1332
Generate indication re: unsuccessful validation
1336

Fig. 13

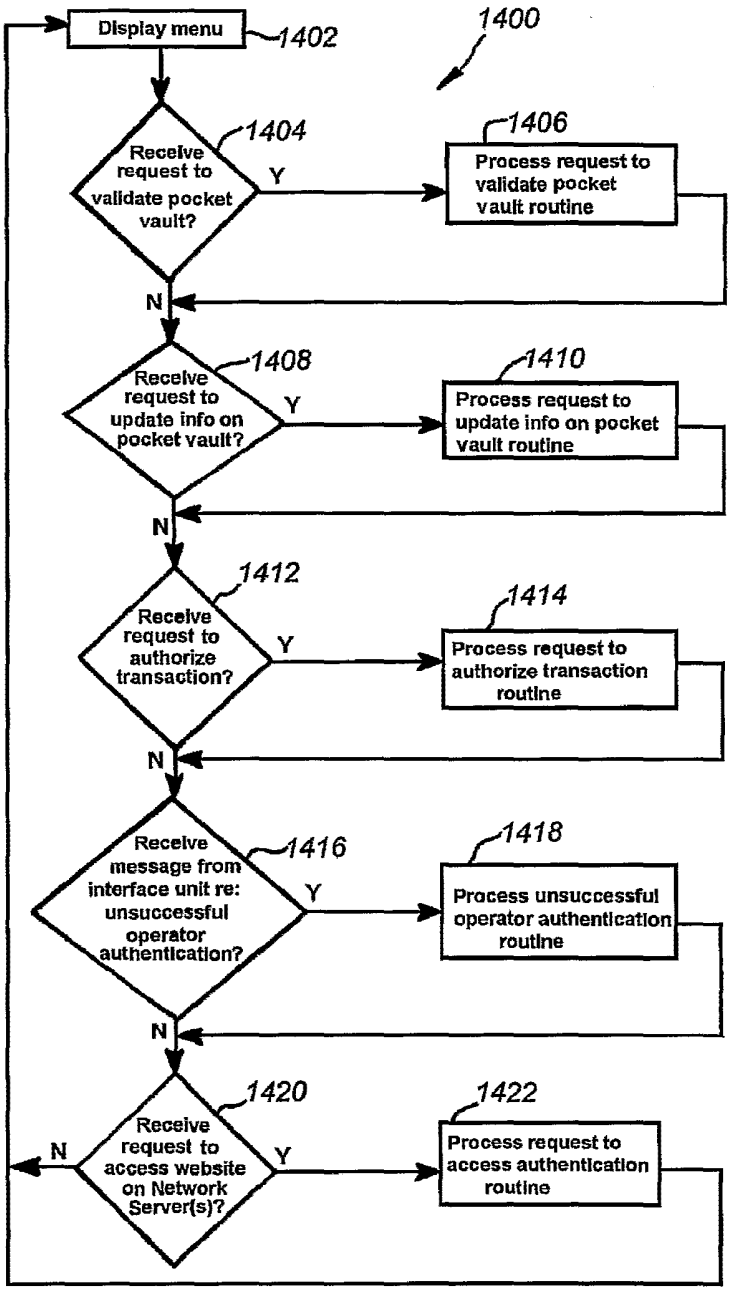

Display menu
1402
1400
Receive request to validate pocket vault?
1404
Y
1406
Process request to validate pocket vault routine
N
Receive request to update info on pocket vault?
1408
Y
1410
Process request to update info on pocket vault routine
N
Receive request to authorize transaction?
1412
Y
1414
Process request to authorize transaction routine
N
Receive message from interface unit re: unsuccessful operator authentication?
1416
Y
1418
Process unsuccessful operator authentication routine
N
Receive request to access website on Network Server(s)?
1420
N
Y
1422
Process request to access authentication routine

Fig. 14

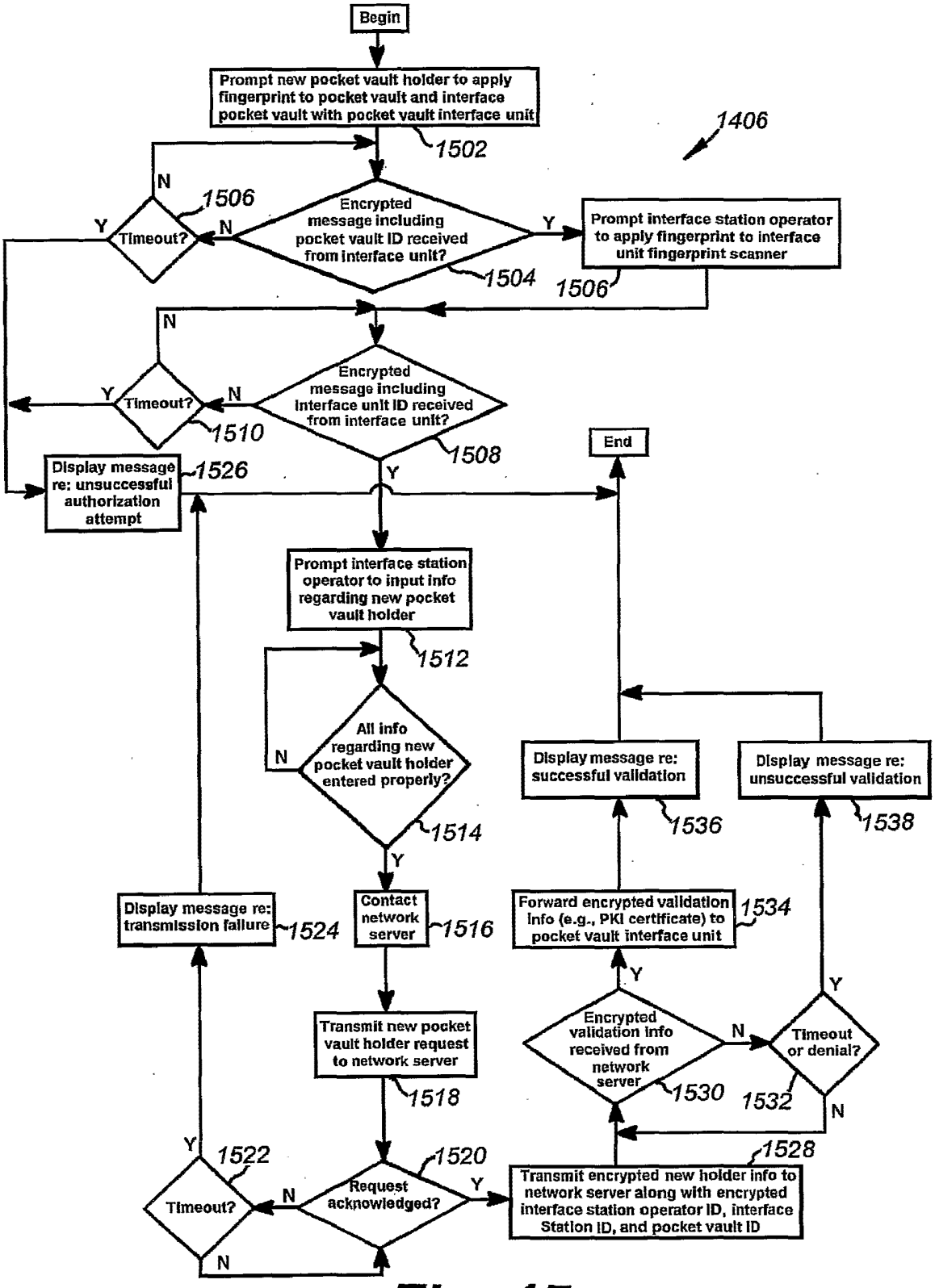

Begin
Prompt new pocket vault holder to apply fingerprint to pocket vault and interface pocket vault with pocket vault interface unit
1502
1406
Encrypted message including pocket vault ID received from interface unit?
1504
Timeout?
1506
Prompt interface station operator to apply fingerprint to interface unit fingerprint scanner
1506
Encrypted message including interface unit ID received from interface unit?
1508
Timeout?
1510
End
Display message re: unsuccessful authorization attempt
1526
Prompt interface station operator to input info regarding new pocket vault holder
1512
All info regarding new pocket vault holder entered properly?
1514
Display message re: successful validation
1536
Display message re: unsuccessful validation
1538
Display message re: transmission failure
1524
Contact network server
1516
Forward encrypted validation info (e.g., PKI certificate) to pocket vault interface unit
1534
Transmit new pocket vault holder request to network server
1518
Encrypted validation info received from network server
1530
Timeout or denial?
1532
Request acknowledged?
1520
Timeout?
1522
Transmit encrypted new holder info to network server along with encrypted interface station operator ID, interface Station ID, and pocket vault ID
1528
Y
N

Fig. 15

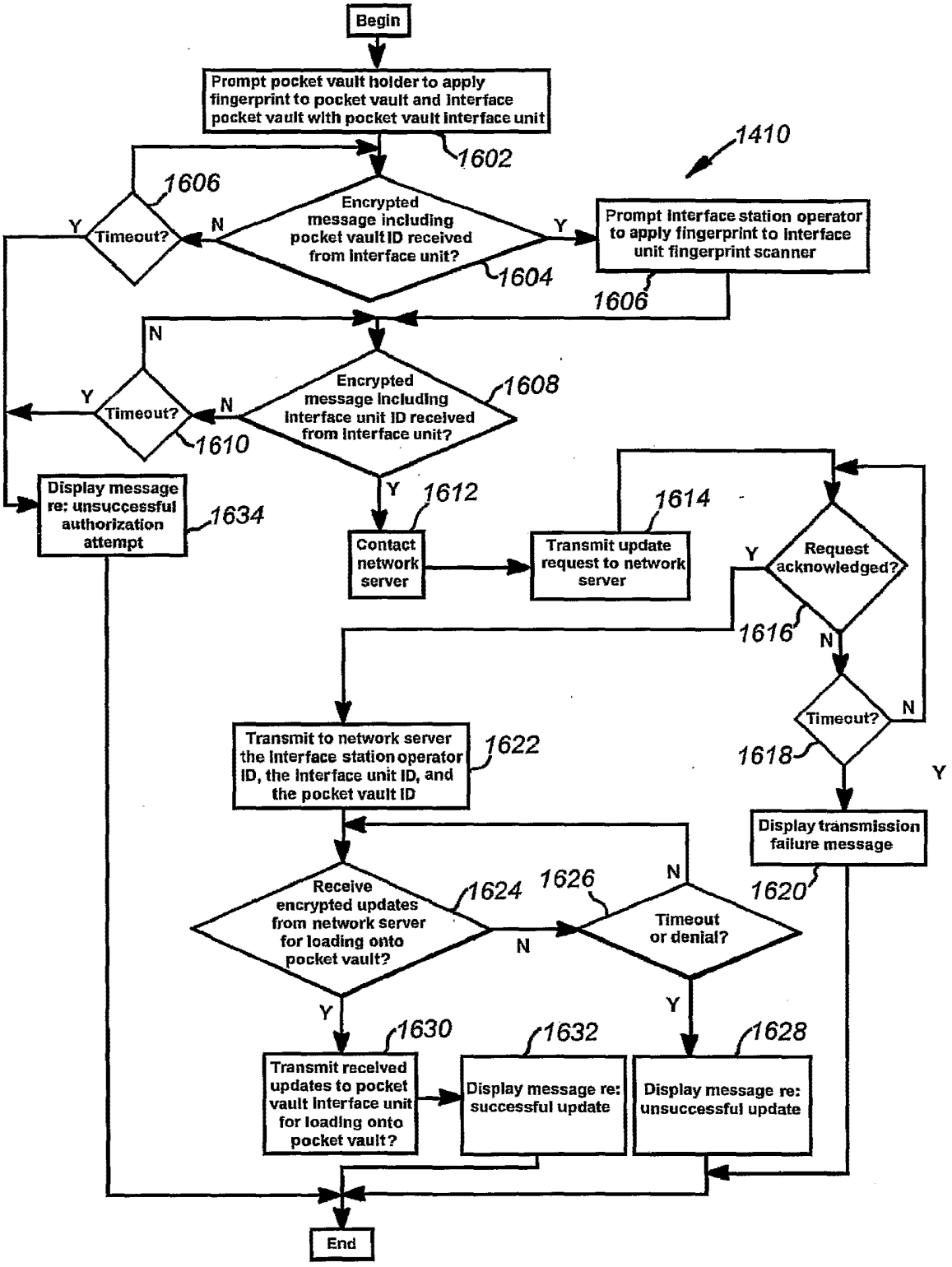

Begin
Prompt pocket vault holder to apply fingerprint to pocket vault and interface pocket vault with pocket vault interface unit
1602
1410
1606
Encrypted message including pocket vault ID received from interface unit?
1604
Y
N
Timeout?
Prompt interface station operator to apply fingerprint to interface unit fingerprint scanner
1606
N
Encrypted message including interface unit ID received from interface unit?
1608
Timeout?
1610
Y
N
Display message re: unsuccessful authorization attempt
1634
Y
1612
Contact network server
Transmit update request to network server
1614
Request acknowledged?
Y
1616
N
Timeout?
1618
N
Y
Transmit to network server the interface station operator ID, the interface unit ID, and the pocket vault ID
1622
Display transmission failure message
1620
Receive encrypted updates from network server for loading onto pocket vault?
1624
1626
Timeout or denial?
N
N
Y
Y
1630
1632
1628
Transmit received updates to pocket vault interface unit for loading onto pocket vault?
Display message re: successful update
Display message re: unsuccessful update
End

Fig. 16

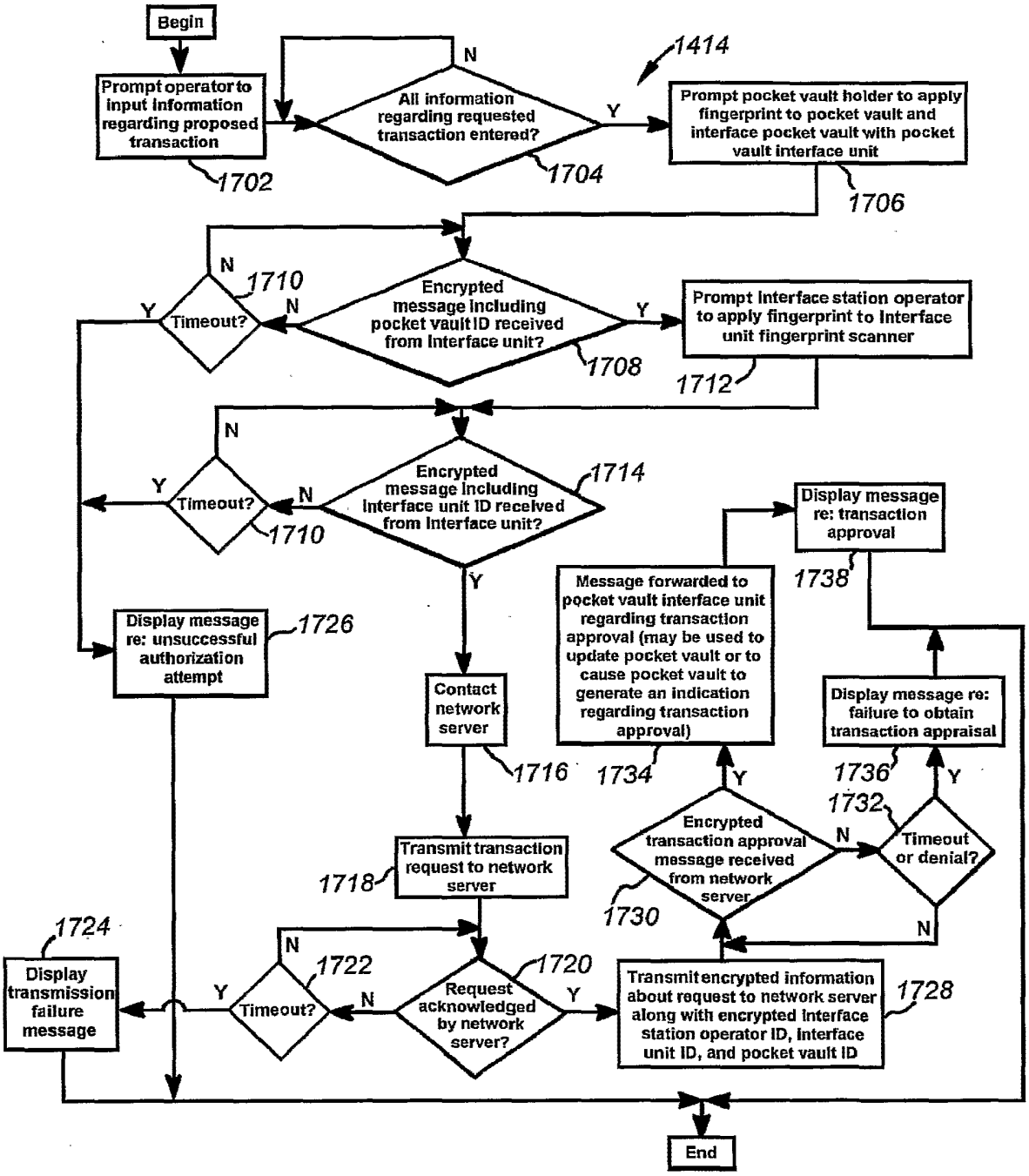

Begin
Prompt operator to input information regarding proposed transaction
1702
All information regarding requested transaction entered?
1704
N
Y
1414
Prompt pocket vault holder to apply fingerprint to pocket vault and interface pocket vault with pocket vault interface unit
1706
Encrypted message including pocket vault ID received from interface unit?
1708
Timeout?
1710
Prompt interface station operator to apply fingerprint to interface unit fingerprint scanner
1712
Encrypted message including interface unit ID received from interface unit?
1714
Timeout?
1710
Display message re: unsuccessful authorization attempt
1726
Contact network server
1716
Transmit transaction request to network server
1718
Request acknowledged by network server?
1720
Timeout?
1722
Display transmission failure message
1724
Transmit encrypted information about request to network server along with encrypted interface station operator ID, interface unit ID, and pocket vault ID
1728
Encrypted transaction approval message received from network server
1730
Timeout or denial?
1732
Message forwarded to pocket vault interface unit regarding transaction approval (may be used to update pocket vault or to cause pocket vault to generate an indication regarding transaction approval)
1734
Display message re: failure to obtain transaction appraisal
1736
Display message re: transaction approval
1738
End

Fig. 17

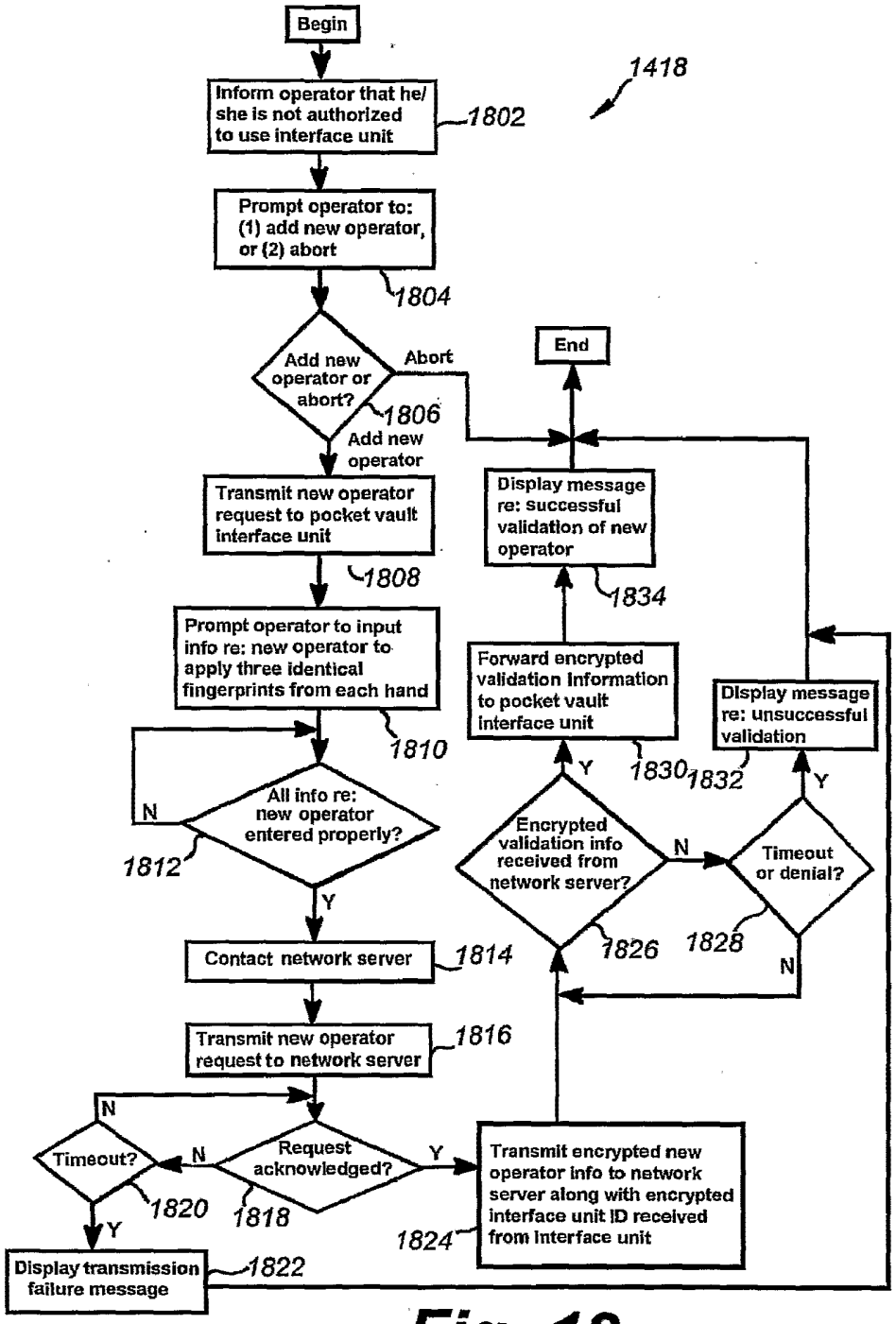

Begin
1418
Inform operator that he/she is not authorized to use interface unit
1802
Prompt operator to: (1) add new operator, or (2) abort
1804
Add new operator or abort?
1806
Abort
End
Add new operator
Transmit new operator request to pocket vault interface unit
1808
Display message re: successful validation of new operator
1834
Prompt operator to input info re: new operator to apply three identical fingerprints from each hand
1810
Forward encrypted validation information to pocket vault interface unit
1830
Display message re: unsuccessful validation
1832
N
All info re: new operator entered properly?
1812
Y
Y
Encrypted validation info received from network server?
1826
N
Timeout or denial?
1828
Y
N
Contact network server
1814
Transmit new operator request to network server
1816
N
Timeout?
1820
N
Request acknowledged?
1818
Y
Transmit encrypted new operator info to network server along with encrypted interface unit ID received from interface unit
1824
Y
Display transmission failure message
1822

Fig. 18

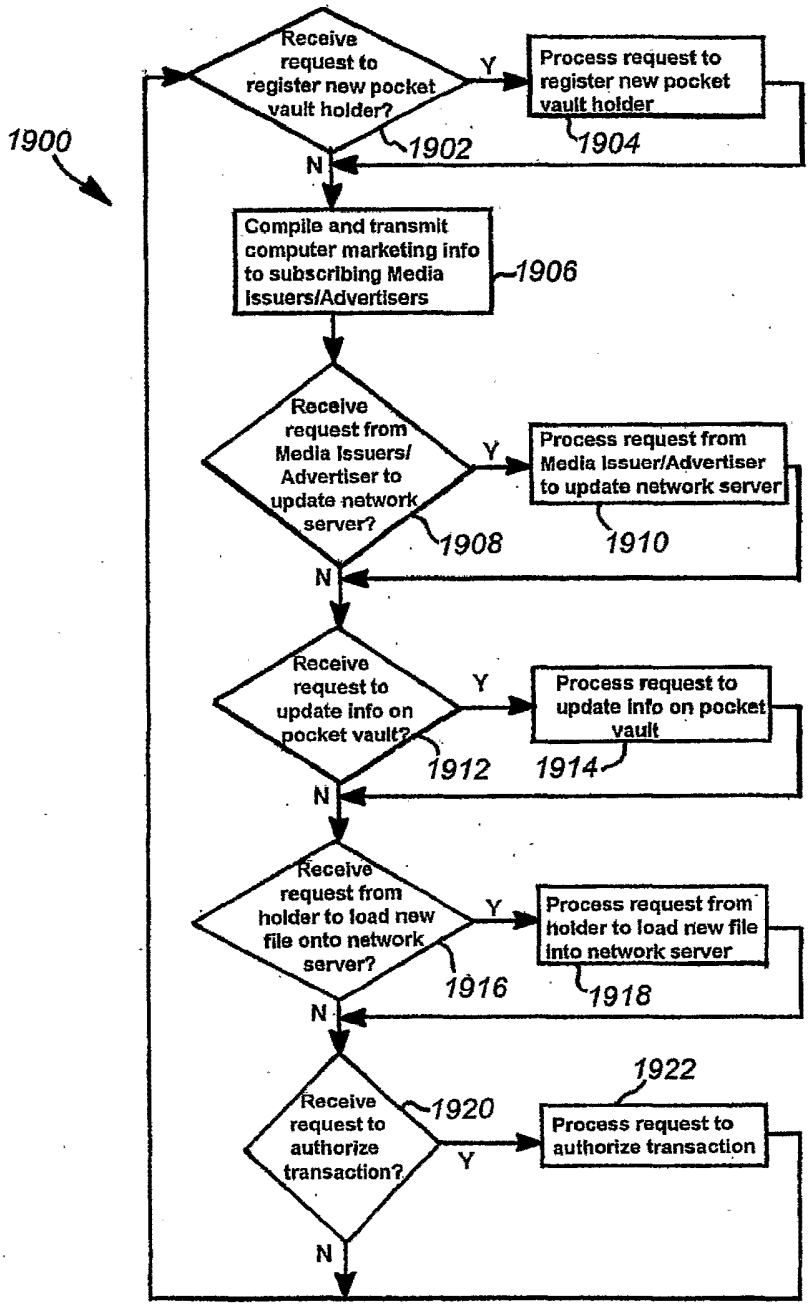

1900
Receive request to register new pocket vault holder?
1902
Y
Process request to register new pocket vault holder
1904
N
Compile and transmit computer marketing info to subscribing Media Issuers/Advertisers
1906
Receive request from Media Issuers/ Advertiser to update network server?
1908
Y
Process request from Media Issuer/Advertiser to update network server
1910
N
Receive request to update info on pocket vault?
1912
Y
Process request to update info on pocket vault
1914
N
Receive request from holder to load new file onto network server?
1916
Y
Process request from holder to load new file into network server
1918
N
Receive request to authorize transaction?
1920
Y
1922
Process request to authorize transaction
N

Fig. 19

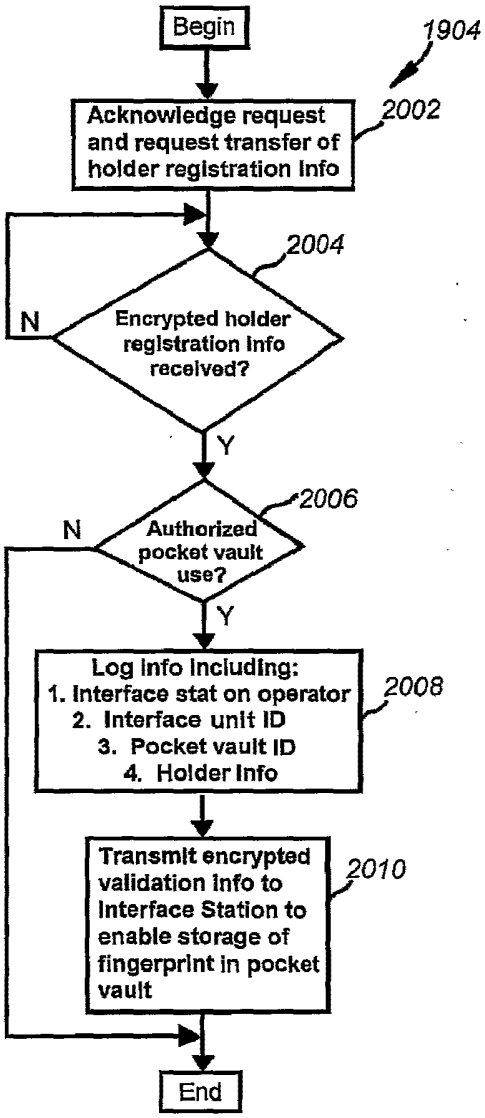

Begin
1904
Acknowledge request and request transfer of holder registration info
2002
2004
N
Encrypted holder registration info received?
Y
2006
N
Authorized pocket vault use?
Y
Log info including:
1. Interface stat on operator
2. Interface unit ID
3. Pocket vault ID
4. Holder info
2008
Transmit encrypted validation info to Interface Station to enable storage of fingerprint in pocket vault
2010
End

Fig. 20

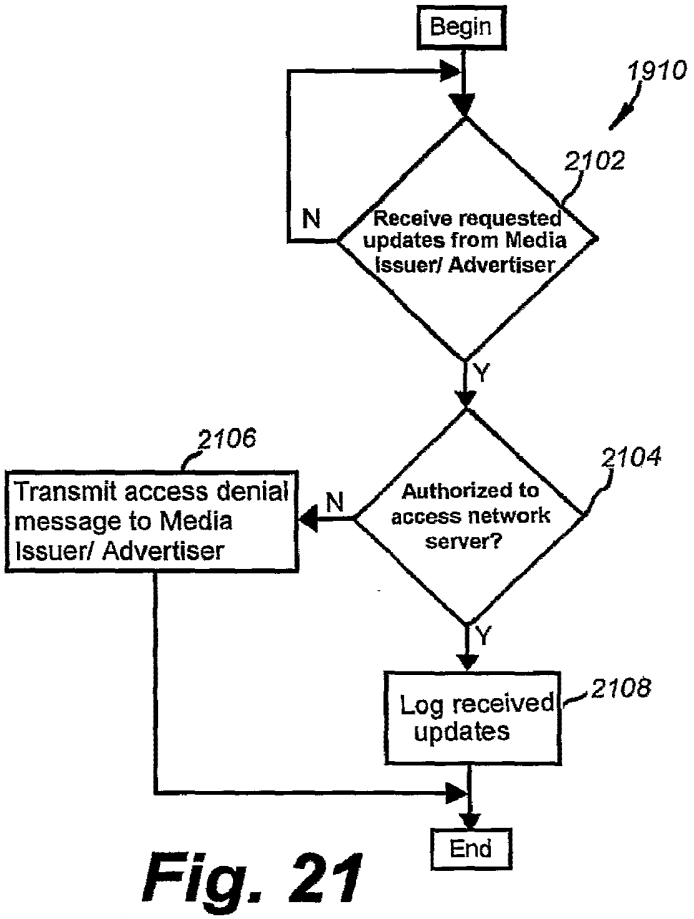

Begin
1910
2102
N
Receive requested updates from Media Issuer/ Advertiser
Y
2106
Transmit access denial message to Media Issuer/ Advertiser
N
2104
Authorized to access network server?
Y
Log received updates
2108
End

Fig. 21

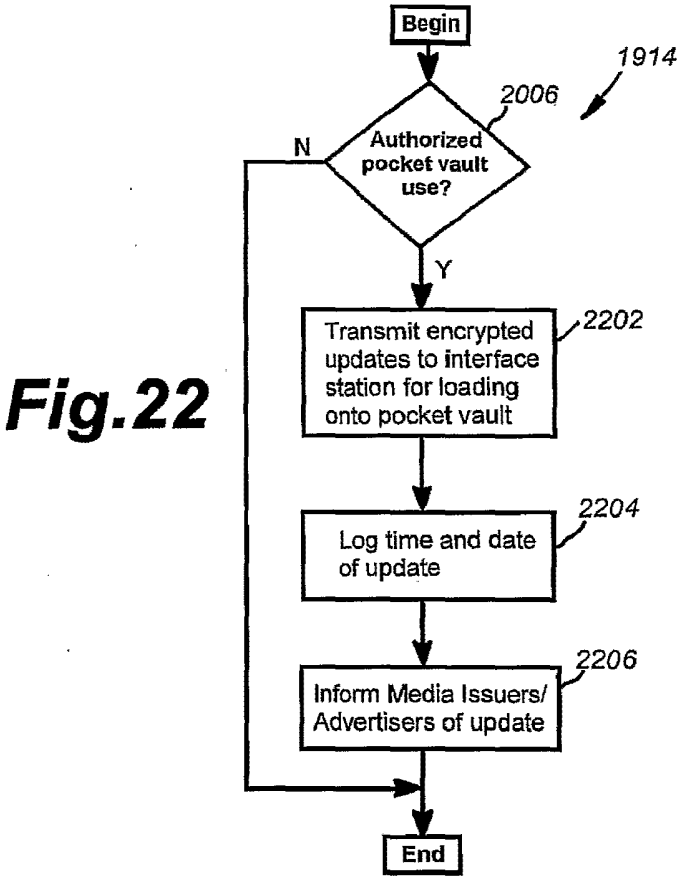

Begin
1914
2006
Authorized pocket vault use?
N
Y
Transmit encrypted updates to interface station for loading onto pocket vault
2202
Log time and date of update
2204
Inform Media Issuers/ Advertisers of update
2206
End

Fig.22

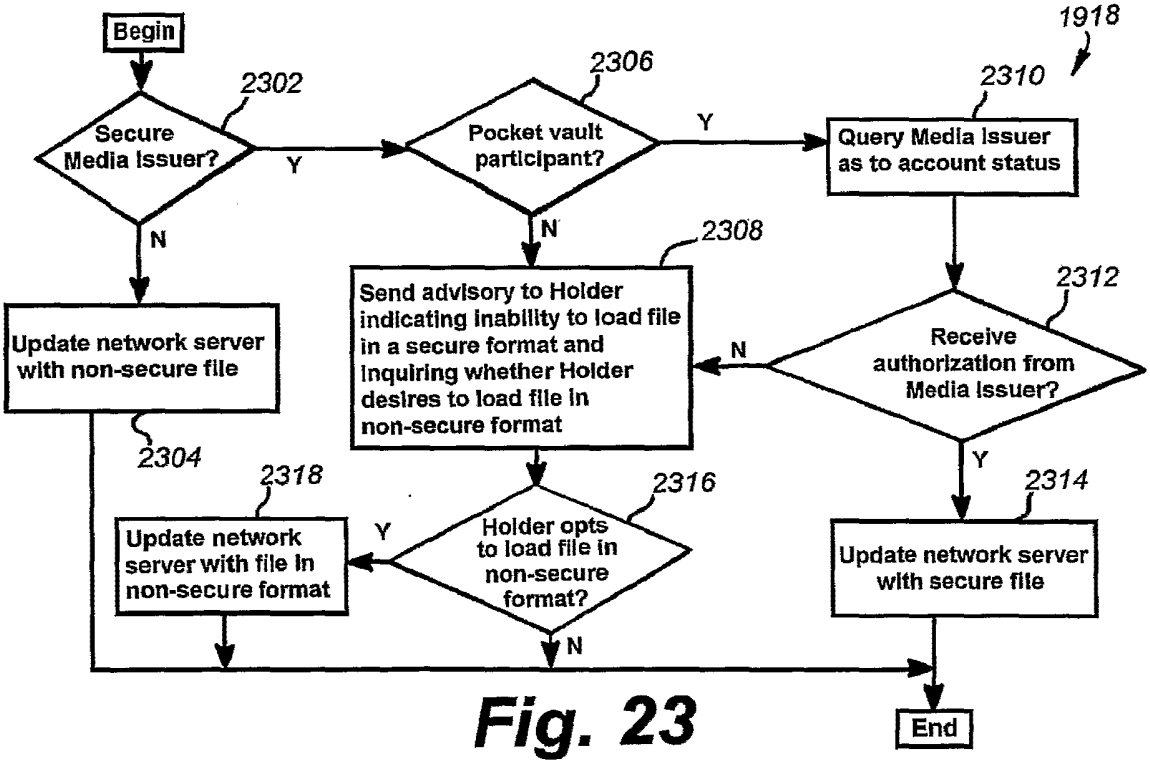

Begin
1918
2302
Secure Media Issuer?
Y
N
2306
Pocket vault participant?
Y
N
2310
Query Media Issuer as to account status
2308
Send advisory to Holder indicating inability to load file in a secure format and inquiring whether Holder desires to load file in non-secure format
2312
Receive authorization from Media Issuer?
N
Y
Update network server with non-secure file
2304
2318
Update network server with file in non-secure format
Y
2316
Holder opts to load file in non-secure format?
N
2314
Update network server with secure file
End

Fig. 23

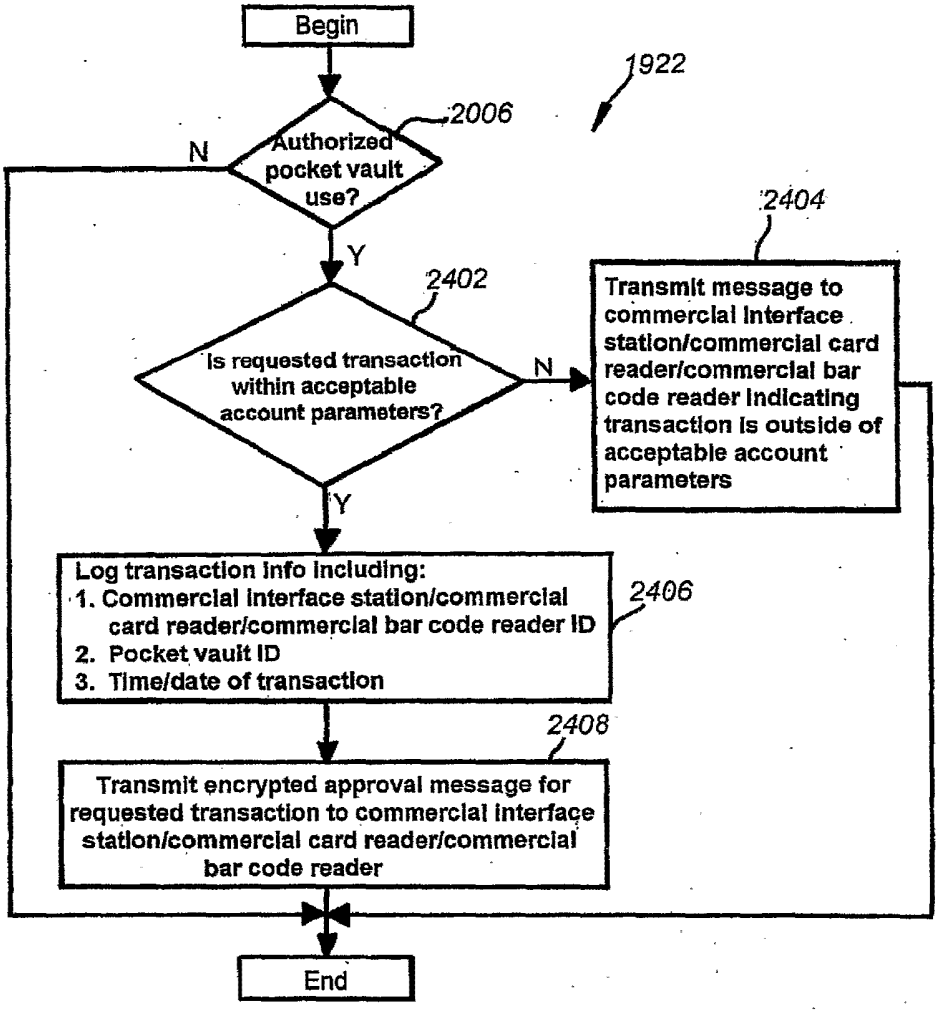

Begin
1922
2006
Authorized pocket vault use?
N
Y
2402
Is requested transaction within acceptable account parameters?
N
2404
Transmit message to commercial interface station/commercial card reader/commercial bar code reader indicating transaction is outside of acceptable account parameters
Y
Log transaction info including:
1. Commercial interface station/commercial card reader/commercial bar code reader ID
2. Pocket vault ID
3. Time/date of transaction
2406
2408
Transmit encrypted approval message for requested transaction to commercial interface station/commercial card reader/commercial bar code reader
End

Fig. 24

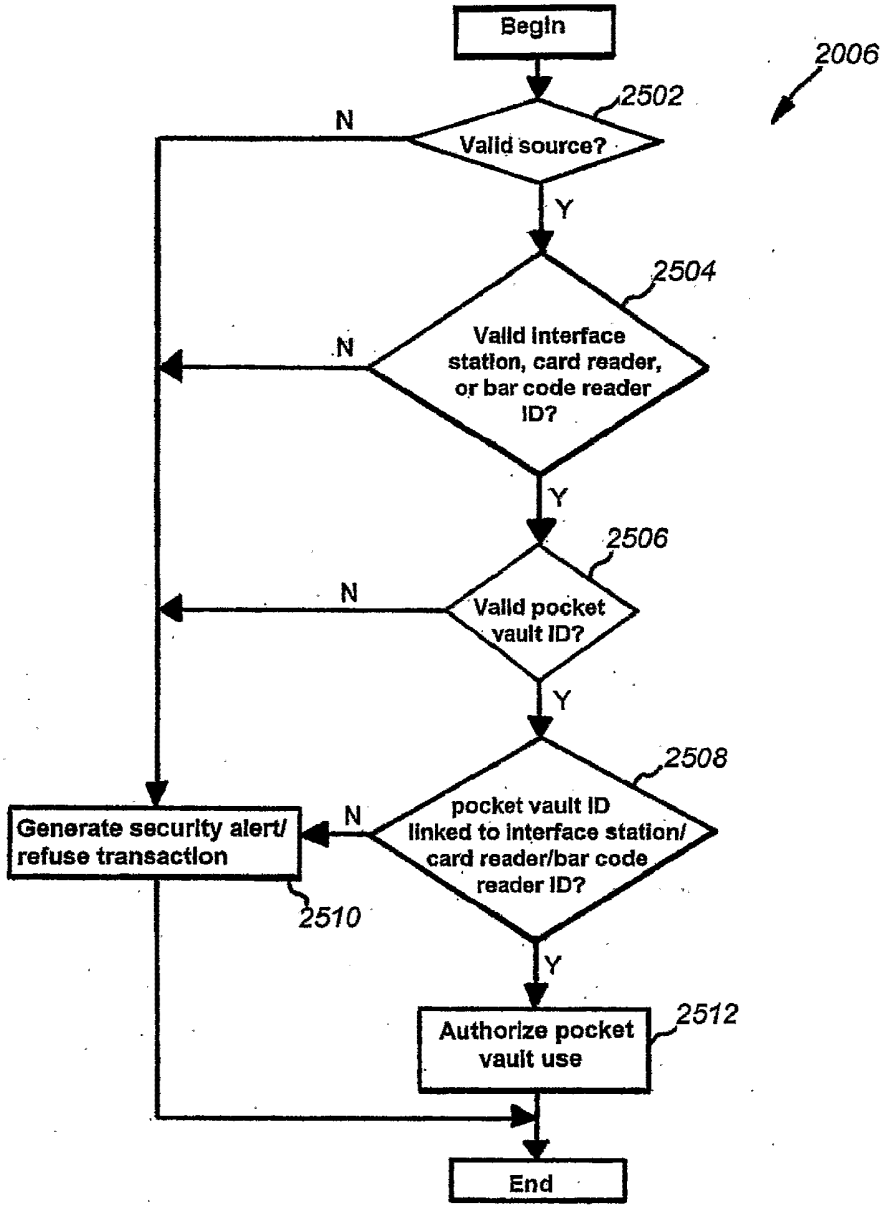

Begin
2006
2502
Valid source?
N
Y
2504
Valid interface station, card reader, or bar code reader ID?
N
Y
2506
Valid pocket vault ID?
N
Y
2508
pocket vault ID linked to interface station/ card reader/bar code reader ID?
N
Y
Generate security alert/ refuse transaction
2510
Authorize pocket vault use
2512
End

Fig. 25

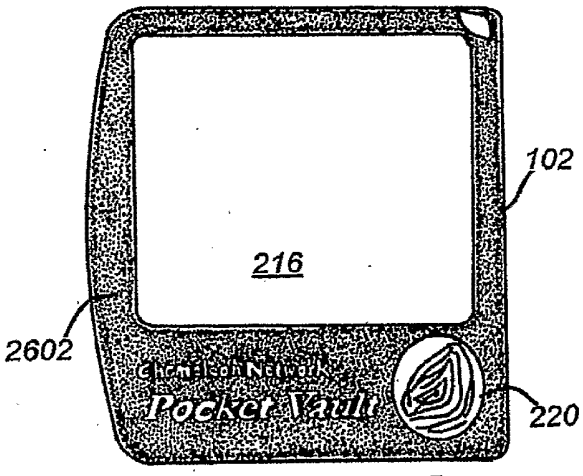


Fig. 26A

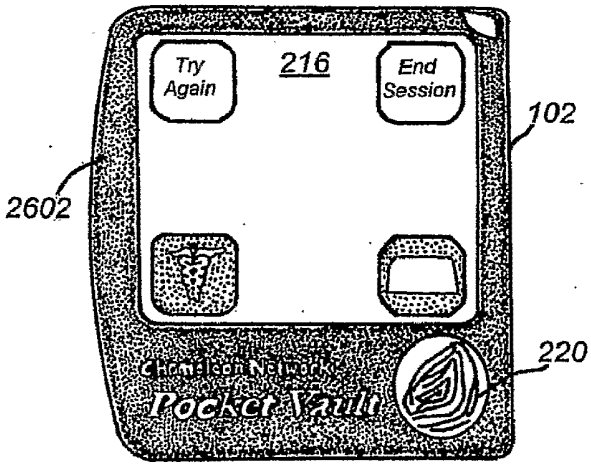


Fig. 26B

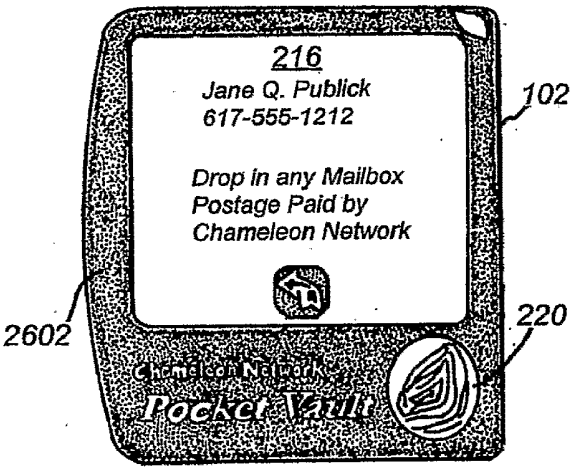


Fig. 26C

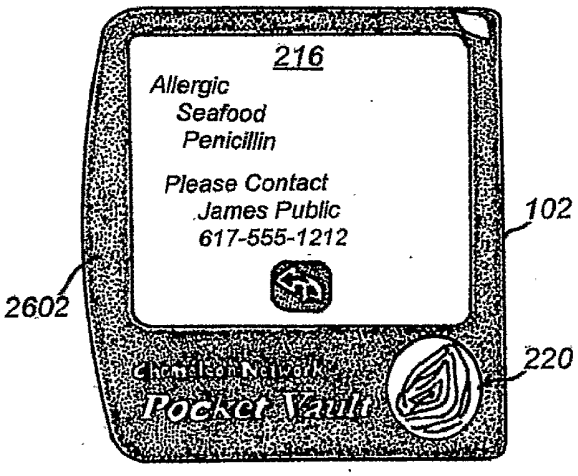


Fig. 26D

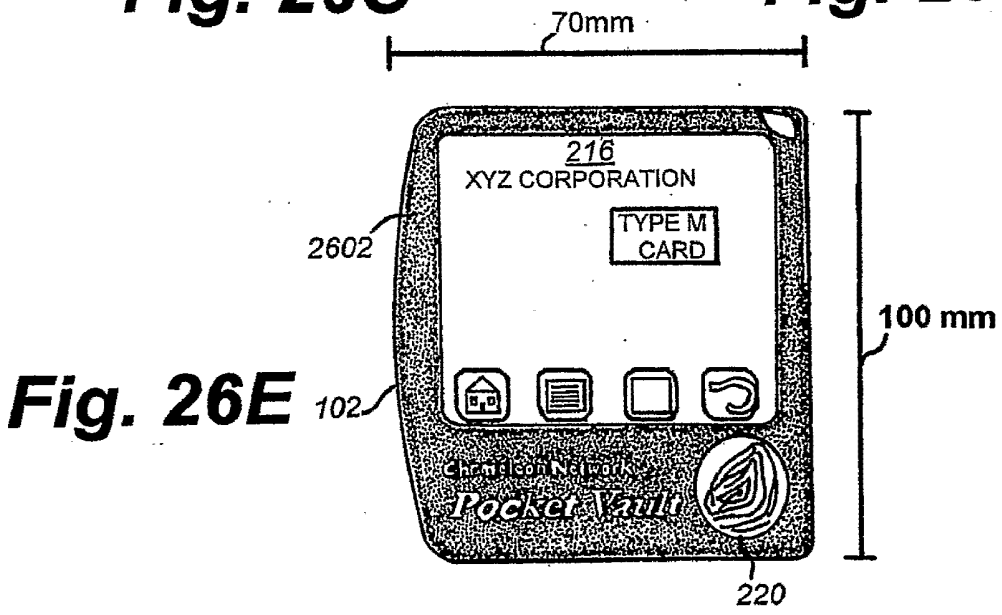


Fig. 26E

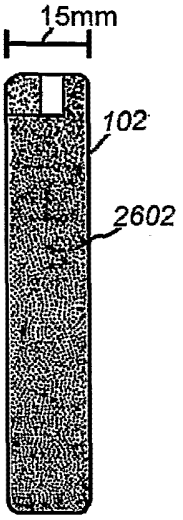


Fig. 26F

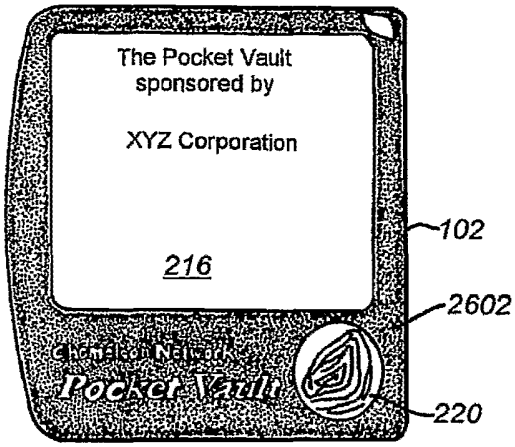


Fig. 26G

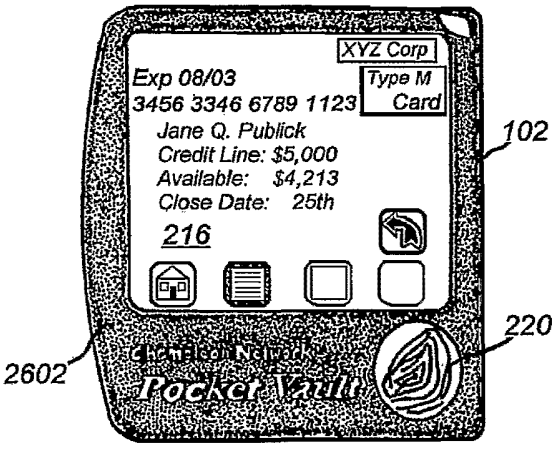


Fig. 26H

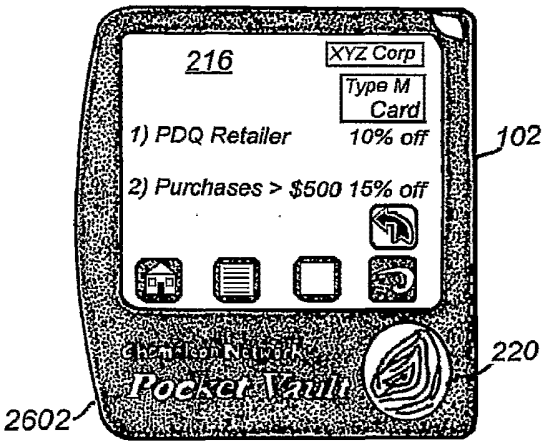


Fig. 26I

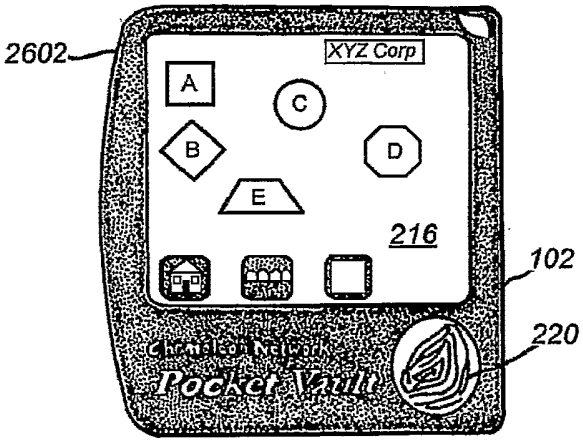


Fig. 26J

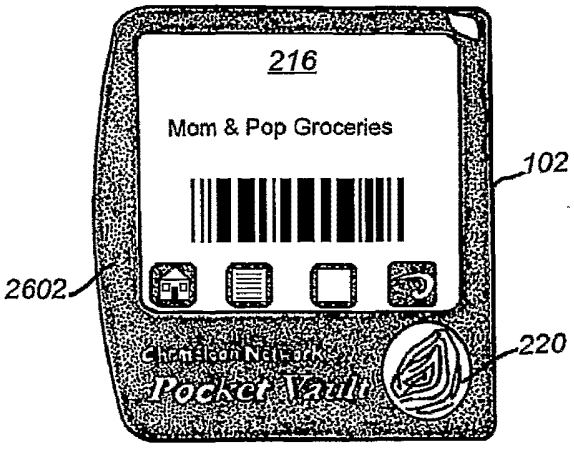


Fig. 26K

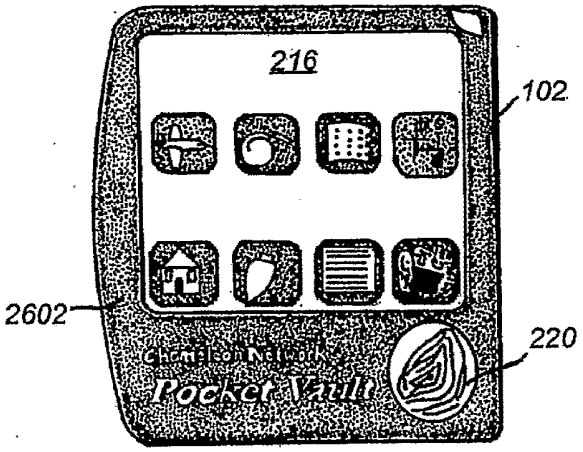


Fig. 26L

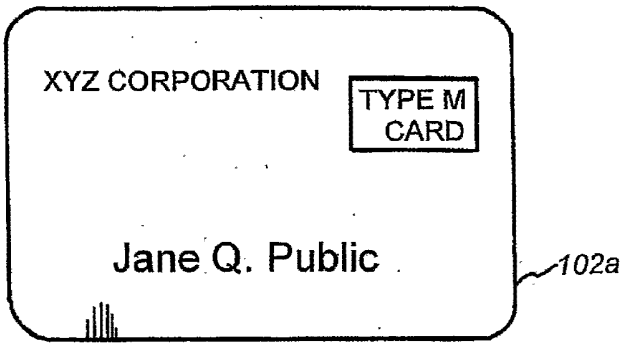


Fig. 26M

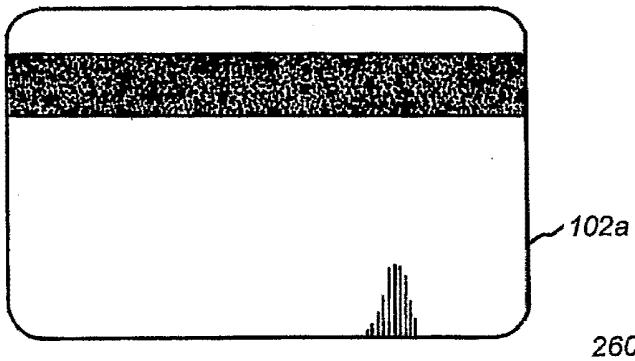


Fig. 26N

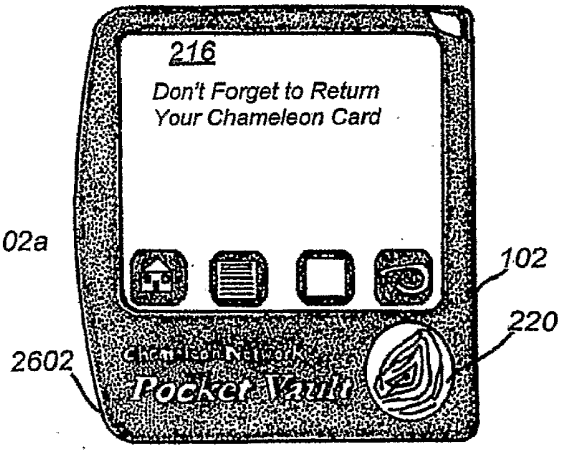


Fig. 26O

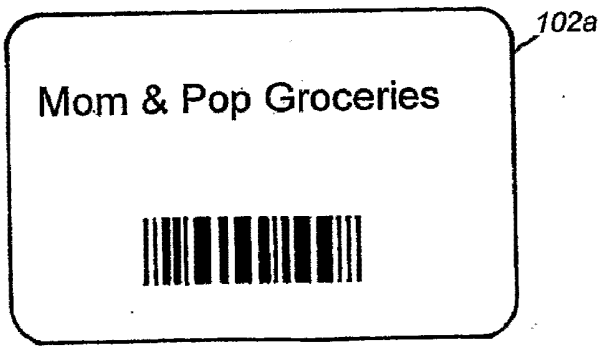


Fig. 26P

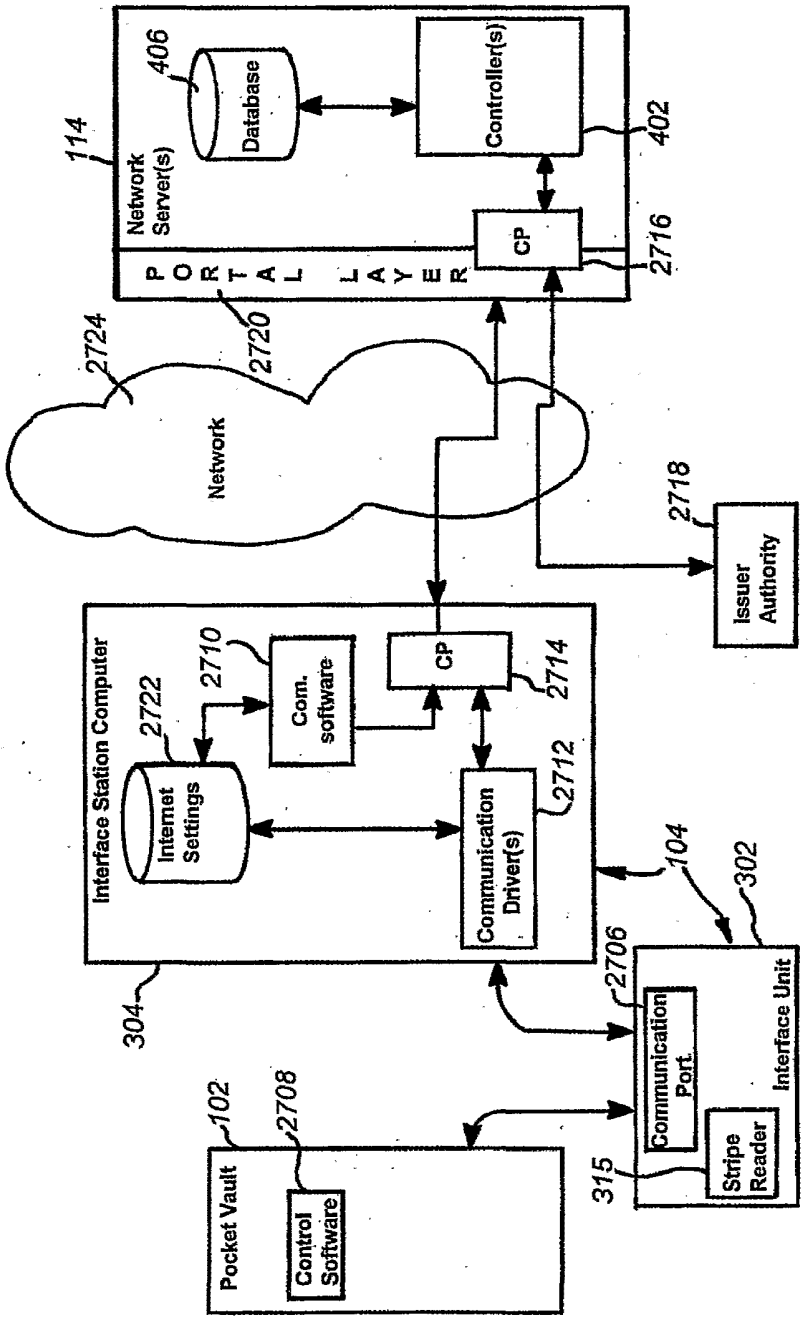

114
Network Server(s)
406
Database
Controller(s)
402
PORTAL LAYER
CP
2716
2720
2724
Network
2718
Issuer Authority
Interface Station Computer
2722
Internet Settings
2710
Com. software
CP
2714
2712
Communication Driver(s)
104
302
304
2706
Communication Port
Stripe Reader
315
Interface Unit
102
2708
Pocket Vault
Control Software

Fig. 27

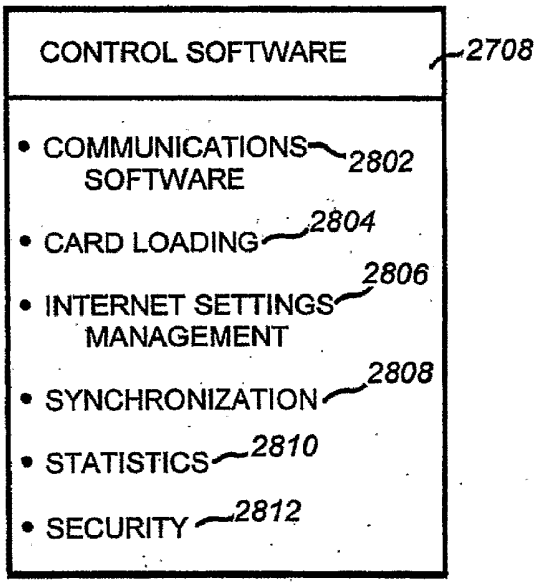

CONTROL SOFTWARE
2708
• COMMUNICATIONS SOFTWARE
2802
• CARD LOADING
2804
• INTERNET SETTINGS MANAGEMENT
2806
• SYNCHRONIZATION
2808
• STATISTICS
2810
• SECURITY
2812

Fig. 28

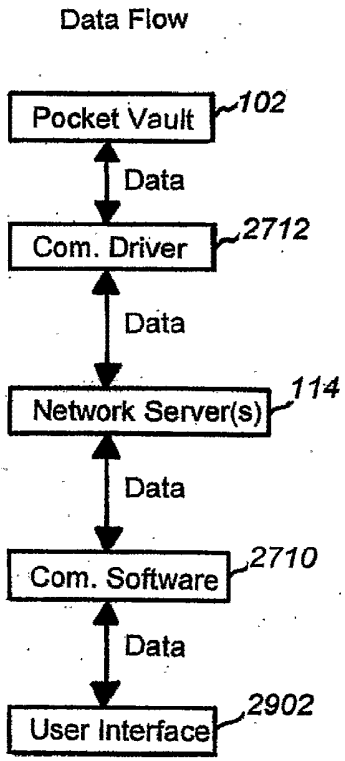

Data Flow
Pocket Vault
102
Data
Com. Driver
2712
Data
Network Server(s)
114
Data
Com. Software
2710
Data
User Interface
2902

Fig. 29

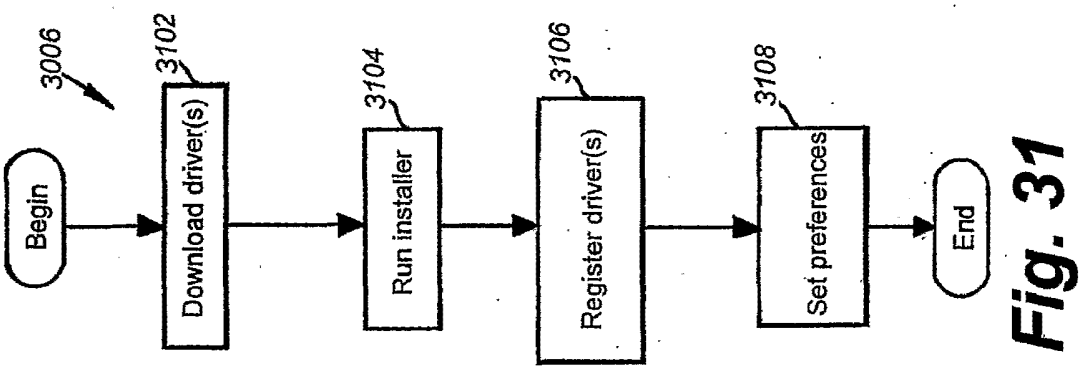

3006
3102
3104
3106
3108
Begin
Download driver(s)
Run installer
Register driver(s)
Set preferences
End

Fig. 31

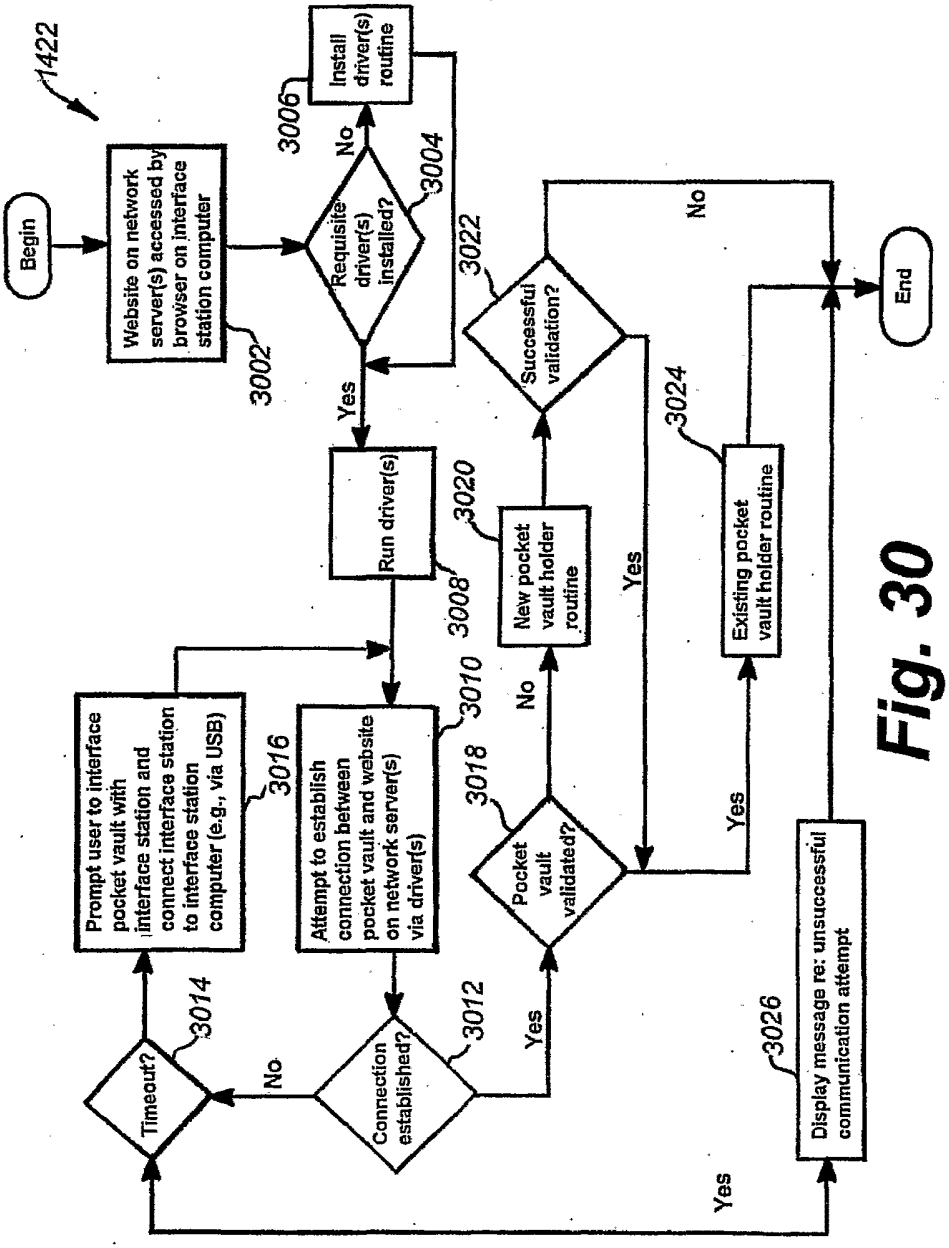

1422
Begin
Website on network server(s) accessed by browser on interface station computer
3002
Requisite driver(s) installed?
3004
No
Install driver(s) routine
3006
Yes
Run driver(s)
3008
Prompt user to interface pocket vault with interface station and connect interface station to interface station computer (e.g., via USB)
3016
Attempt to establish connection between pocket vault and website on network server(s) via driver(s)
3010
Timeout?
3014
No
Connection established?
3012
Yes
Pocket vault validated?
3018
No
New pocket vault holder routine
3020
Yes
Successful validation?
3022
No
Existing pocket vault holder routine
3024
Yes
Display message re: unsuccessful communication attempt
3026
Yes
End

Fig. 30

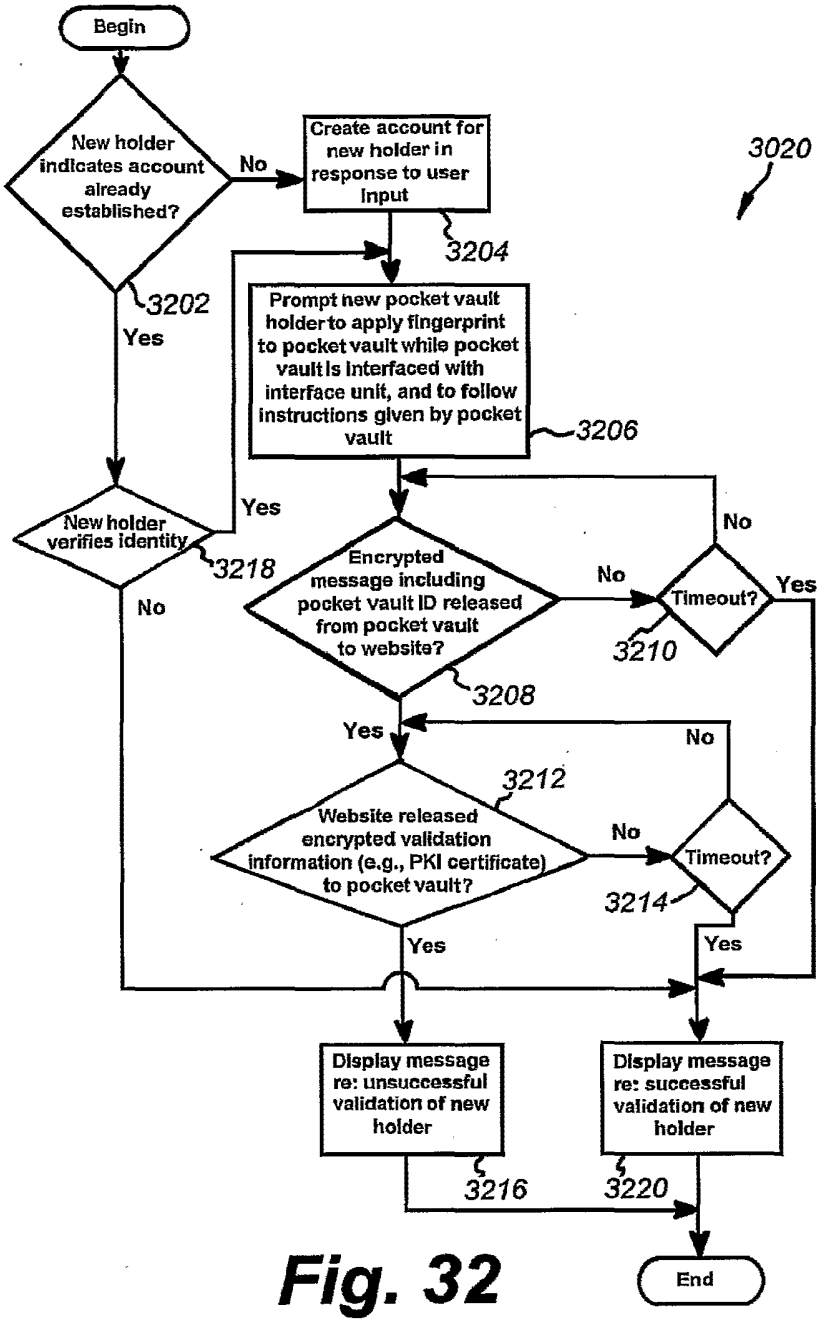

Begin
New holder indicates account already established?
No
Create account for new holder in response to user input
3204
3020
3202
Yes
Prompt new pocket vault holder to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit, and to follow instructions given by pocket vault
3206
New holder verifies identity
Yes
3218
No
Encrypted message including pocket vault ID released from pocket vault to website?
No
Timeout?
Yes
No
3210
3208
Yes
No
3212
Website released encrypted validation information (e.g., PKI certificate) to pocket vault?
No
Timeout?
3214
Yes
Yes
Display message re: unsuccessful validation of new holder
Display message re: successful validation of new holder
3216
3220
End

Fig. 32

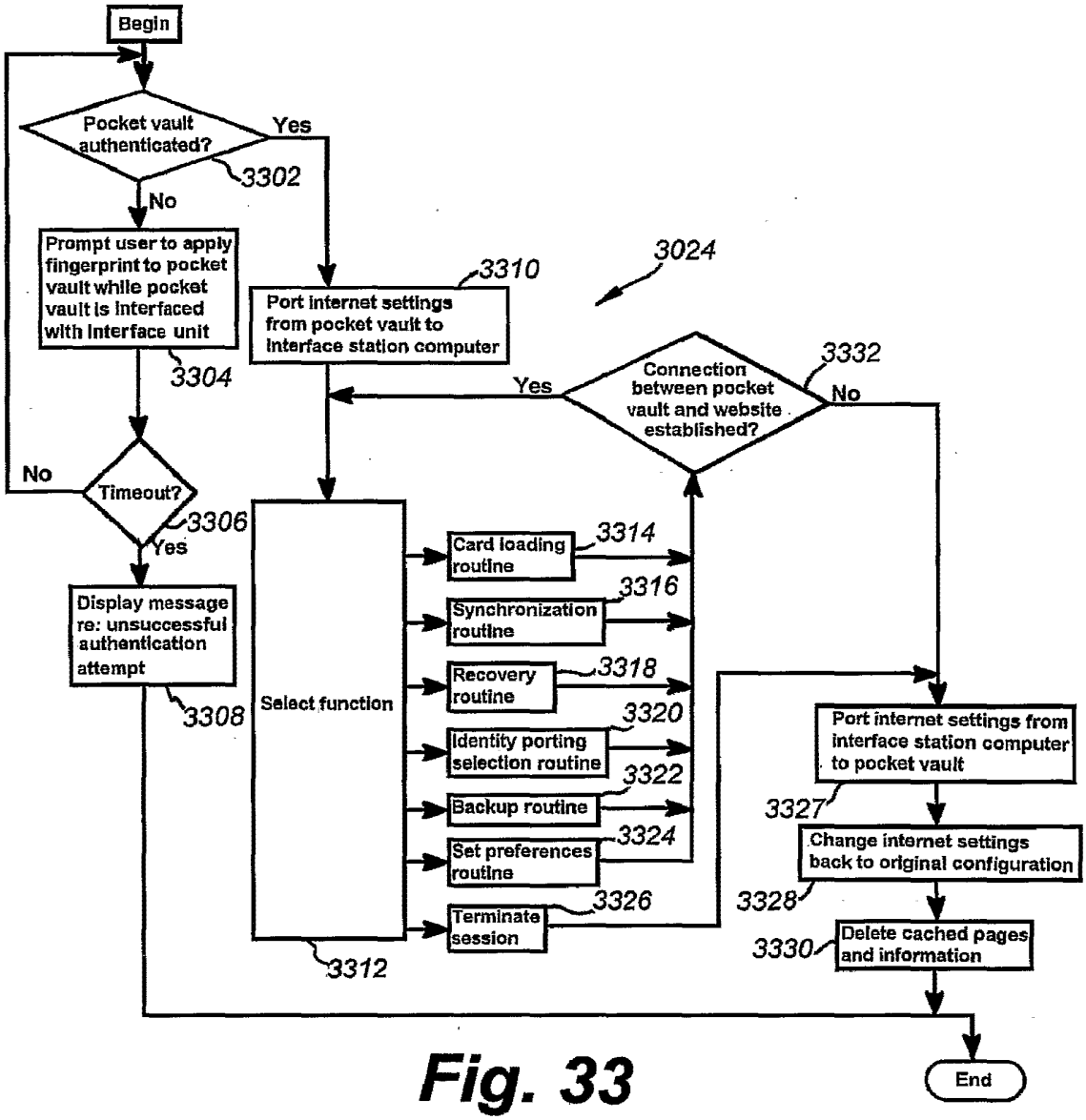

Begin
Pocket vault authenticated?
Yes
3302
No
Prompt user to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit
3304
Timeout?
No
3306
Yes
Display message re: unsuccessful authentication attempt
3308
3310
Port internet settings from pocket vault to interface station computer
3024
Connection between pocket vault and website established?
3332
Yes
No
Select function
Card loading routine
3314
Synchronization routine
3316
Recovery routine
3318
Identity porting selection routine
3320
Backup routine
3322
Set preferences routine
3324
Terminate session
3326
3312
Port internet settings from interface station computer to pocket vault
3327
Change internet settings back to original configuration
3328
Delete cached pages and information
3330
End

Fig. 33

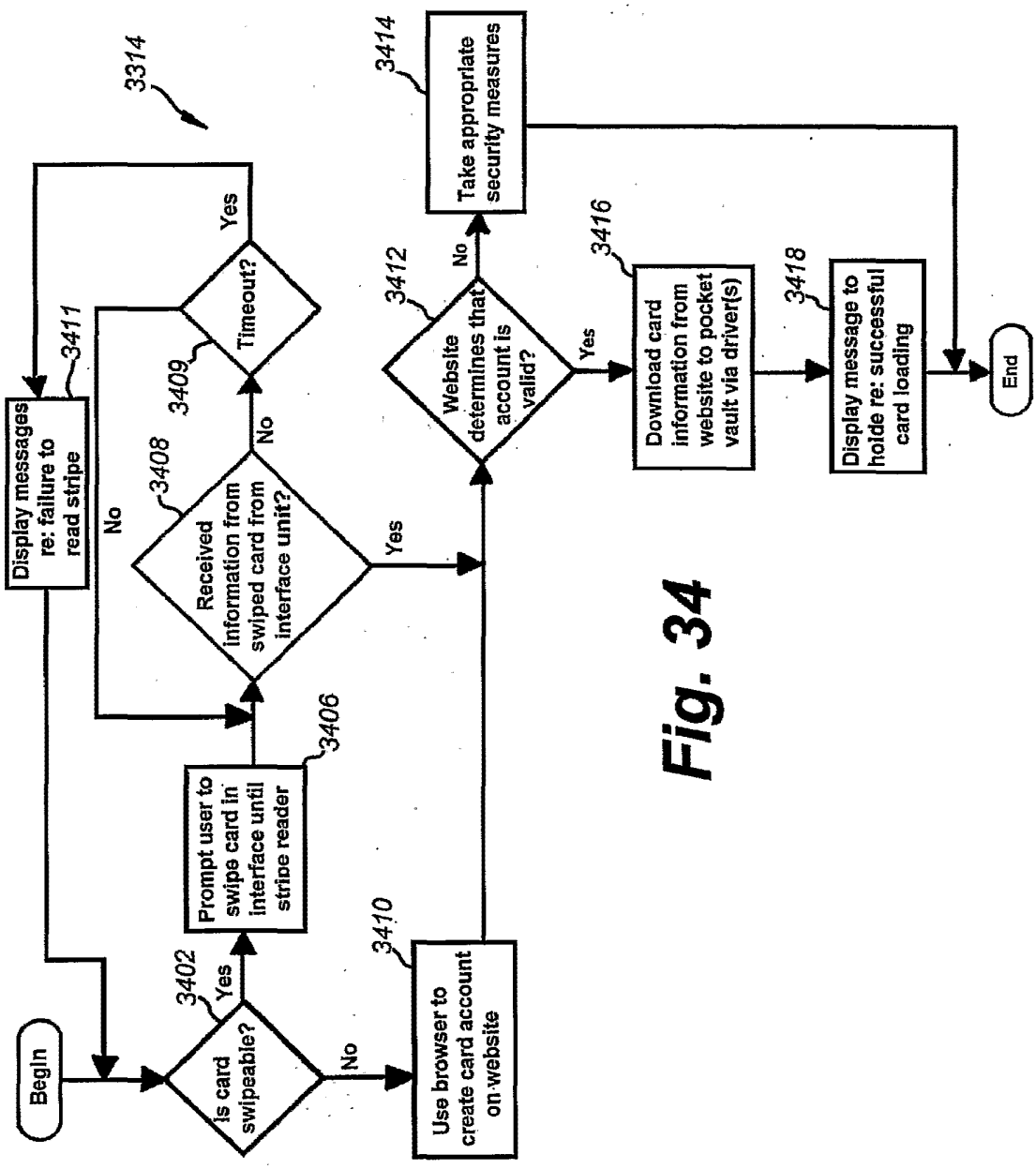

3314
Begin
Is card swipeable?
3402
Yes
No
Prompt user to swipe card in interface until stripe reader
3406
Use browser to create card account on website
3410
Received information from swiped card from interface unit?
3408
No
Yes
Timeout?
3409
Yes
No
Display messages re: failure to read stripe
3411
Website determines that account is valid?
3412
No
Yes
Take appropriate security measures
3414
Download card information from website to pocket vault via driver(s)
3416
Display message to holde re: successful card loading
3418
End

Fig. 34

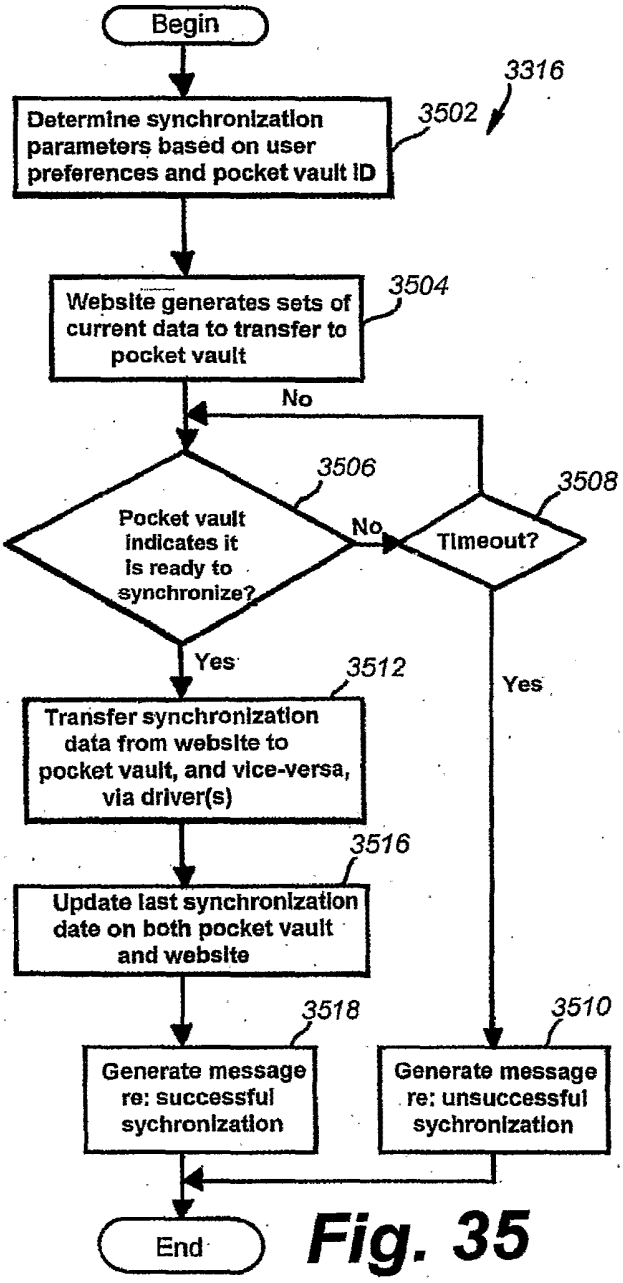

Begin
3316
Determine synchronization parameters based on user preferences and pocket vault ID
3502
Website generates sets of current data to transfer to pocket vault
3504
No
3506
Pocket vault indicates it is ready to synchronize?
No
3508
Timeout?
Yes
Yes
3512
Transfer synchronization data from website to pocket vault, and vice-versa, via driver(s)
3516
Update last synchronization date on both pocket vault and website
3518
Generate message re: successful sychronization
3510
Generate message re: unsuccessful sychronization
End

Fig. 35

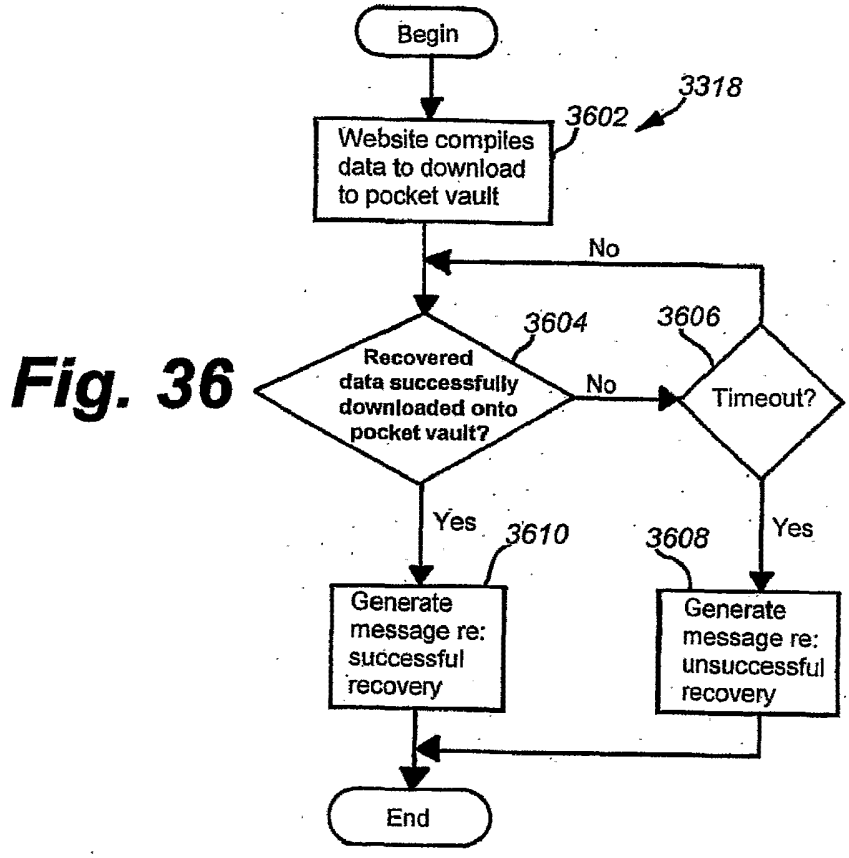

Begin
3318
3602
Website compiles data to download to pocket vault
No
3604
3606
Recovered data successfully downloaded onto pocket vault?
No
Timeout?
Yes
3610
3608
Yes
Generate message re: successful recovery
Generate message re: unsuccessful recovery
End

Fig. 36

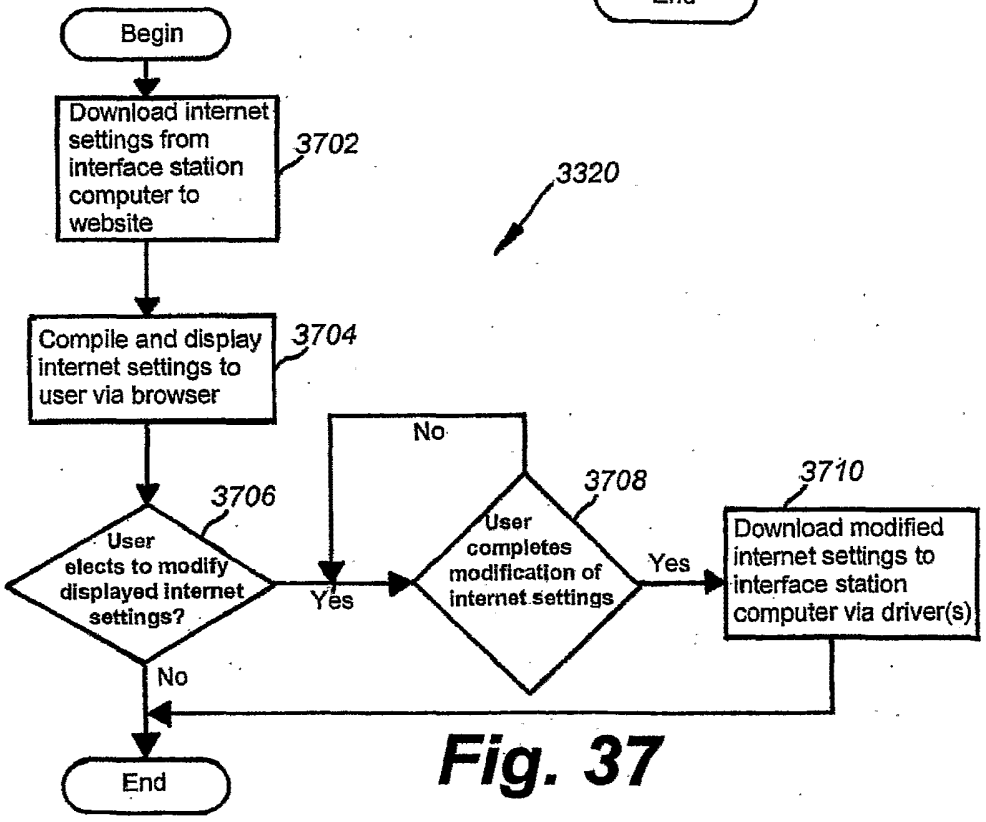

Begin
Download internet settings from interface station computer to website
3702
3320
Compile and display internet settings to user via browser
3704
No
3706
3708
3710
User elects to modify displayed internet settings?
Yes
User completes modification of internet settings
Yes
Download modified internet settings to interface station computer via driver(s)
No
End

Fig. 37

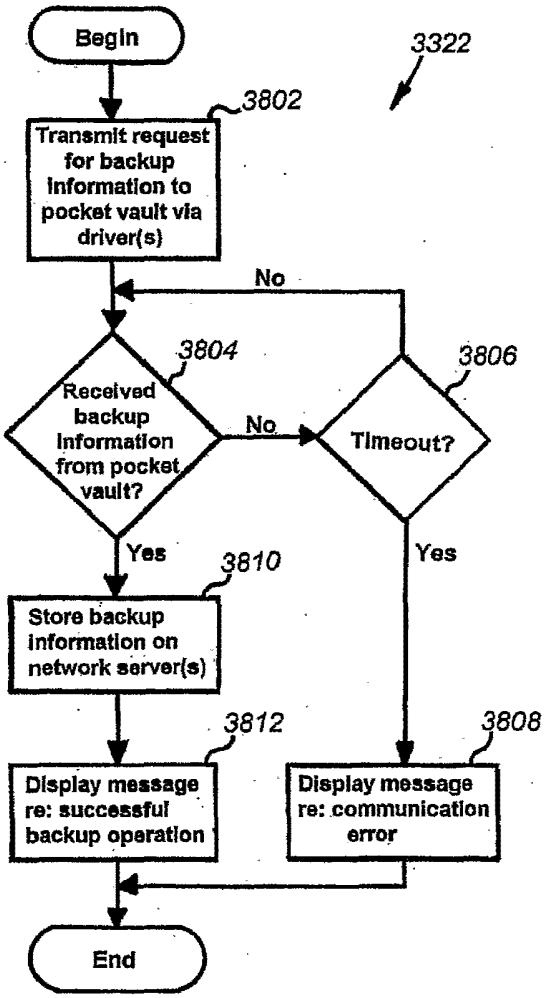

Begin
3322
3802
Transmit request for backup information to pocket vault via driver(s)
No
3804
Received backup information from pocket vault?
No
3806
Timeout?
Yes
Yes
3810
Store backup information on network server(s)
3812
Display message re: successful backup operation
3808
Display message re: communication error
End

Fig. 38

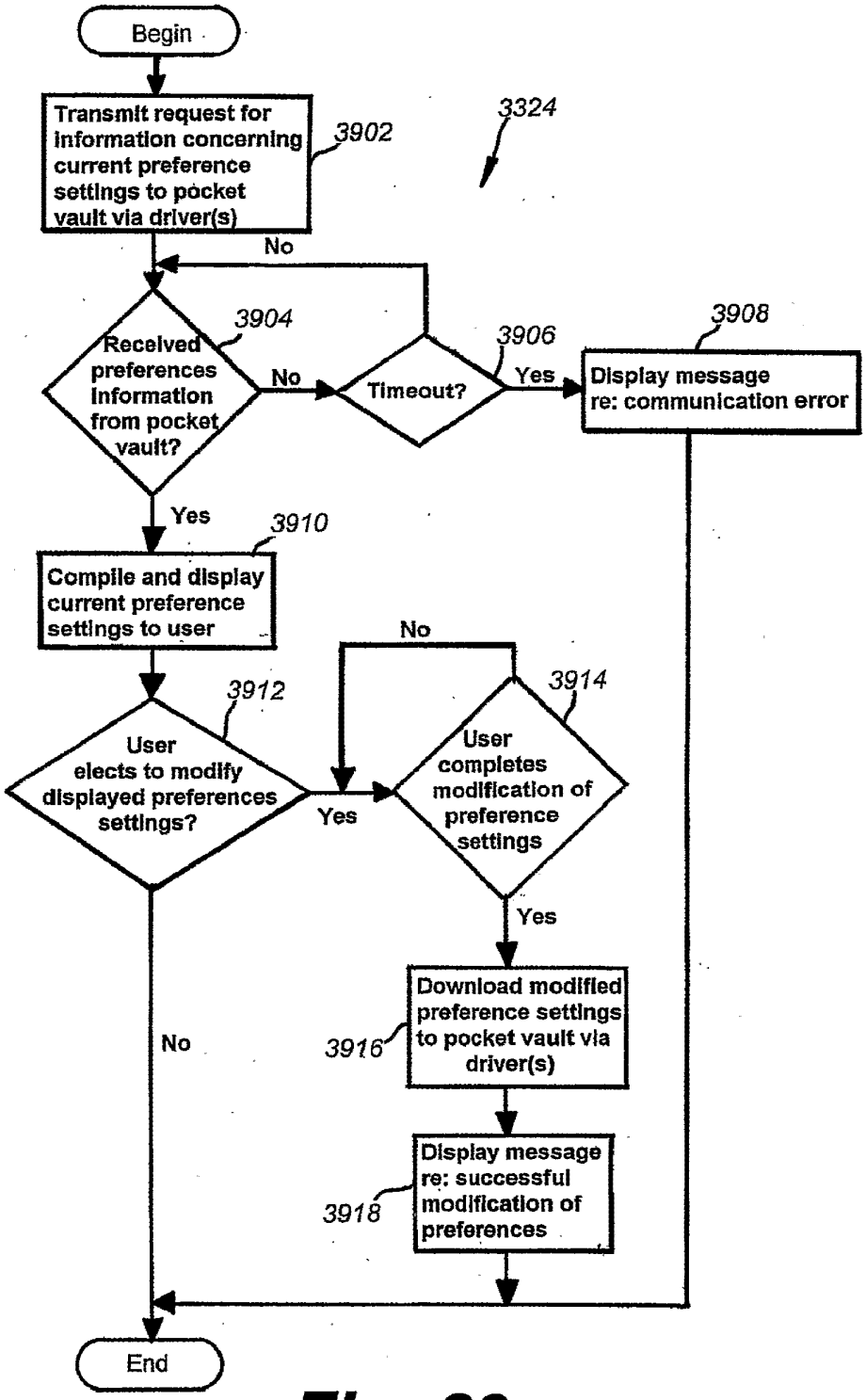

Begin
Transmit request for information concerning current preference settings to pocket vault via driver(s)
3902
3324
No
Received preferences information from pocket vault?
3904
No
Timeout?
3906
Yes
Display message re: communication error
3908
Yes
Compile and display current preference settings to user
3910
No
User elects to modify displayed preferences settings?
3912
Yes
User completes modification of preference settings
3914
Yes
No
Download modified preference settings to pocket vault via driver(s)
3916
Display message re: successful modification of preferences
3918
End

Fig. 39

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2003 (18.09.2003)

PCT

(10) International Publication Number
WO 03/077473 A1

(51) International Patent Classification[7]: H04L 12/28, G07F 19/00

(21) International Application Number: PCT/DK03/00163

(22) International Filing Date: 13 March 2003 (13.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PA 2002 00387 13 March 2002 (13.03.2002) DK

(71) Applicant *(for all designated States except US)*: **BEAMTRUST A/S** [DK/DK]; Borupvang 1A, DK-2750 Ballerup (DK).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ANDERSSON, Sten** [SE/SE]; Bryggaregatan 12, S-227 36 Lund (SE). **KAARLE, Peter** [SE/SE]; Lackes gränd 7, S-244 95 Furulund (SE). **KAPNOULA, Anna** [SE/SE]; Västra Stationstorget 14, S-222 37 Lund (SE). **ELGAARD, Robert** [DK/DK]; Stænget 11, DK-2820 Gentofte (DK).

(74) Agent: **ZACCO DENMARK A/S**; Hans Bekkevolds Allé 7, DK-2900 Hellerup (DK).

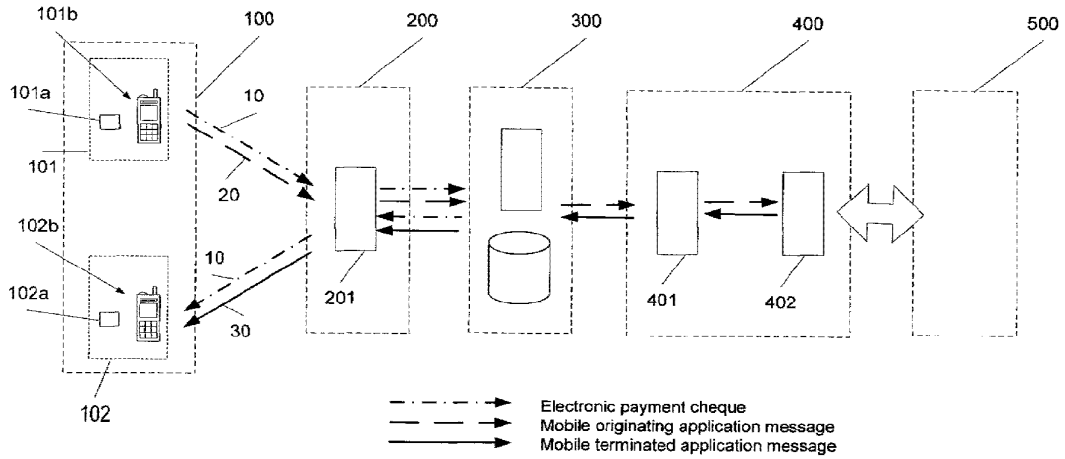
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, 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 (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, 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: A METHOD OF PROCESSING AN ELECTRONIC PAYMENT CHEQUE



(57) Abstract: The invention relates to processing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute to an account of a second user in a second banking institute, which processing includes generating digital signatures by means of asymmetric encryption. The method comprises the following steps: • in a first SIM card, creating an electronic payment cheque and signing the electronic payment cheque with a first signature; • transmitting the signed electronic payment cheque to a second SIM card in a second mobile equipment of the second user; • in the second SIM card, additionally signing the electronic payment cheque with a second signature; • transmitting the thus signed electronic payment cheque to subsequently initiate a deposit of the amount of money in the electronic payment cheque into the account of the second user.

WO 03/077473 A1

A method of processing an electronic payment cheque

This invention relates to a method of processing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute to an account of a second user in a second banking institute, which processing includes generating digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key.

A plurality of payment means are common today, such as bank notes and coins, cheques, money transfers from one bank account to another, credit cards, debit cards, giro transfer forms, etc. Some of these payment means are more suitable for transferring money from one person to another than others. The security of a money transfer is important; some persons do not want to carry big cash amounts, everybody prefers a security that a money transfer via a bank account or a giro account reaches the rightful receiver and when a payment means has an inherent protection against utilization, if unlawfully acquired, this is favoured.

Regarding money transfers, a solution which provides a secure and simple way of transferring money electronically from one person to another is desirable, for instance an electronic substitute of a cheque.

US patent 5,677,955 describes a computer-based electronic instrument that can comprise an electronic substitute of a cheque. It is described, that the electronic instrument can be transferred from one computer to another and can relate to the transferral of funds from an account of a payer to an account of a payee. The electronic instrument can be signed by means of an electronic signature using asymmetric key cryptography, and by receipt of the electronic substitute of a cheque, the payee can deposit the cheque at his bank by means of the internet and/or e-mails.

Even though the electronic substitute of a cheque can be stored on a portable PCMCIA card, the use of the electronic substitute of a cheque is not mobile as such, in that it is limited to use in computers/PC's. Moreover, the electronic substitute of a cheque might be cumbersome to use in that the requirements for the information included are relatively high.

It would be desirable to be able to use an electronic substitute of a cheque in a mobile telephone for a number of reasons, viz. the inherent mobility of mobile telephones, the low power consumption and the fact, that many mobile telephones are substantially always turned on. The use of electronic substitutes of cheques has yet not been carried into effect on mobile telephones because the high security, that is necessary in connection with any transferral of money, including a transferral of a electronic substitute of a cheque, has not yet been obtainable.

Therefore there is a need for a secure method to transfer an electronic substitute of a cheque from a mobile telephone to another mobile telephone and/or to a bank.

The above and other objects are reached when the method mentioned in the opening paragraph is characterised in that the method comprises the steps of in a first SIM card of the first user, creating an electronic payment cheque and signing the electronic payment cheque with a first signature generated by means of a first private key of a first asymmetric key pair, which first private key resides on the first SIM card hosted by the first mobile equipment; via a first mobile equipment hosting the SIM card of the first user, transmitting the signed electronic payment cheque to a second SIM card hosted in a second mobile equipment of the second user; in the second SIM card, signing the electronic payment cheque, which has been signed with a first signature, with an additional second signature generated on the second SIM card, by means of a second private key of a second asymmetric key pair, which second private key resides on the second SIM card hosted by the second mobile equipment; transmitting the electronic payment cheque signed

with the first and the second digital signatures from the second mobile station to a the central hub, which central hub is in communication with the first and the second banking institutes, and in the central hub, initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user by initialising a verification of the second signature at the banking institution of the second user and a verification of the first signature at the banking institution of the first user.

When the creation and signing of the electronic payment cheque is performed on a SIM-card and the signing of a received electronic payment cheque for depositing/withdrawal thereof also is performed on SIM-card, a high level of security is obtained, because the interface between a SIM-card and a mobile equipment hosting it inherently limits the access to data on the SIM-card. Examples of the digital mobile telephone system used can be the Global System for Mobile communication (GSM) or Digital-American Mobile Phone Service (D-AMPS).

Preferably, the first and the second private key are generated on the first and the second SIM card, respectively, in the method according to the invention. When the private keys are generated on a SIM card and never have been exposed outside the SIM card, they are tamperproof.

In a preferred embodiment, the transmittal of the signed electronic payment cheque from the first mobile equipment hosting the SIM card of the first user to the second SIM card hosted in a second mobile equipment of the second user is performed via a digital mobile telephone system. In another preferred embodiment, the signed payment cheque is transmitted as a Short Message by means of IR, Bluetooth or Wi-Fi standards.

According to a preferred embodiment of the method, creating an electronic payment cheque comprises indicating a telephone number associated to the second SIM card, an amount to be transferred and an account index to the account, wherefrom the amount should be withdrawn. Thereby, the user of

the first mobile equipment, i.e. the issuer of an electronic payment cheque, need only know the telephone number of the receiver of the cheque, i.e. the user of the second mobile equipment, the amount he/she wants to transfer to the receiver and from which account he/she wants to withdraw the money. The method supports the possibility that the issuer of the electronic payment cheque has a plurality of accounts to choose to withdraw money from, and preferably a default account is set, from which the money is withdrawn if the user do not change this setting.

When the signed payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system, the method provides a cheap, fast and simple way of money transfer.

Preferably, the method further comprises via the first mobile equipment, prompting the first user to confirm creation of an electronic payment cheque, which prompting is initiated at the first SIM card hosted by the first mobile equipment. Hereby, it is avoided that money transfers are generated unintentionally. Preferably, the conformation of the creation of the electronic payment cheque comprises entering of a PIN-RSA number. The PIN-RSA number is a PIN code of 4 digits, which is used to get access to the key files on the SIM card.

According to the invention, the encrypted electronic payment cheque is transmitted via a message proxy and preferably, the encrypted electronic payment cheque proxy is converted to an SMS Point-to-point data download message, which subsequently is transmitted to the second SIM card hosted by the second mobile equipment. The message proxy is an integrated part of the central hub.

The message proxy in the central hub is suitable for sending application specific messages from a banking institute via a bank application, typically also hosted in the BDC, to SIM cards hosted in mobile equipment. A BDC domain may consist of several Bank domains, i.e. several banks that are

linked to the service of the BDC domain and are using the same BDC for processing of the transactions. The BDC domain can be divided into one BDC and several bank areas. The BDC is responsible for hosting some of the functionality that might be common between banks e.g. the Internet bank(s).

The other claims describe other preferred embodiments of the invention.

The term "mobile telephone" or "mobile phone" is used synonymous with "mobile station" and is used to define a mobile phone, which is divided in the two logical units: "mobile equipment" and "Subscriber Identity Module (SIM)". The mobile equipment has all the functions for radio communication with the digital mobile telephone system. The mobile equipment together with the SIM thus equals the mobile station. Without the SIM, the mobile equipment is only able to perform emergency calls. The SIM card is a smart card that is used for storing of subscription related information.

The invention will be explained more fully below in connection with an example of a preferred embodiment and with reference to the drawing, in which:

fig. 1a and 1b show overviews of the parts performing the method of the invention,

fig. 2 is a diagram of the data flow between some of the parts performing the method of the invention, and

fig. 3a and 3b overviews of the digital signature calculation and the digital signature verification, respectively.

Throughout the figures, the same reference numbers refers to like elements.

Fig. 1a shows an example of an overview of the parts performing the method of the invention. The parts are shown hosted in a user's domain 100, an operator's domain 200, a central hub 300, a Bank Data processing Centre's (BDC domain) 400 and in a banking institute 500, respectively. Shown are to mobile telephones 101 and 102 operating in a digital mobile telephone system 100, whereof the mobile telephone 101 is an issuer of an electronic payment cheque and the mobile telephone102 is the receiver thereof. This digital mobile telephone system 100 could be the Global System for Mobile communication (GSM) or Digital-American Mobile Phone Service (D-AMPS).

Throughout this description, the term "receiver" is meant to denote the mobile telephone 102, to which an electronic payment cheque is sent, and the term "issuer" is meant to denote the mobile telephone 101, from which the electronic payment cheque is sent. However, the terms "receiver" and "issuer" can also denote the user of the mobile telephone 102, to which an electronic payment cheque is sent, and the user of the mobile telephone 101 from which the electronic payment cheque is sent, respectively.

As stated above, the term "mobile telephone" or "mobile phone" is used synonymous with "mobile station" and is used to define a mobile phone 101, 102, which is divided in the two logical units: "mobile equipment" 101b, 102b and "Subscriber Identity Module (SIM)" 101a, 102a. The mobile equipment 101b, 102b has all the functions for radio communication with the digital mobile telephone system. The mobile equipment 101b, 102b together with the SIM 101a, 102a thus equals the mobile station 101, 102 respectively. In this description, the applications for performing the method of the inventions are placed on the SIM card; for facilitate the reading of this description, this is not always stated explicitly.

To use the method of the invention, i.e. activate the applications, a user has to register at the banking institute 500, typically through an Internet Bank, which will be explained below. After registration the user receives a new SIM card 101a, 102a from an operator 200, where the user is a subscriber. This

SIM card 101a, 102a contains an application for supporting issuance and reception of electronic payment cheques according to the method of the invention. The SIM card 101a, 102a is preferably personalised to allow remote updates over the air (OTA). An activation procedure must be successfully executed before it is possible to use the service for performing the method according to the invention, and thereafter, the user can use the mobile equipment together with the customised SIM card 101a, 102a. The application on the SIM card 101a, 102a is responsible for signing electronic payment cheques and for the interaction with the user.

The OTA updates are performed by sending application specific messages from the Bank application 402 to the mobile phone 101, 102 via an SMS Gateway/Proxy 401 in the BDC's domain 400 and the operator's SMS-C 201. The application messages are transferred as user data within Short Messages and are transported between the mobile phone 101, 102 and the SMS-C 201 using mobile originated and mobile terminated short messages

The BDC domain 400 has an interface to the central hub 300 and thereby to the operator's GSM environment. The SMS gateway 401 is responsible for communication with the SMS-C 201 within the operator domain 200 via the central hub 300. The Bank application 402 within the BDC domain 400 communicates with the SMS Gateway/Proxy 401 using an XML interface. With this interface it is possible for the BDC 200 to request OTA updates of application information on the SIM card 101a, 102a. The XML interface includes the receiver's phone number and a string to be sent either as an ordinary text message or an application message destined for the SIM application. The XML documents are sent between the Bank application 402 and the SMS Gateway/Proxy 401 using the HTTP method POST.

The SMS Gateway/Proxy 401 also has a service listening for mobile originated messages. This service handle all messages from mobile phones 101, 102 (independent of whether it's a mobile originating request or a

response of a mobile terminated request) and delivers the messages as a XML document to the domain of the banking institute 500.

For information transmitted from the Bank application 402 to the SMS Gateway/Proxy 401, the Bank application 402 acts as an HTTP client and the SMS Gateway/Proxy 401 acts as an HTTP server. For information transmitted from the SMS Gateway/Proxy 401 to the Bank application 402, the reverse applies, i.e. the SMS Gateway/Proxy 401 acts as an HTTP client whereas the Bank application 402 acts as an HTTP server.

The information exchange, shown by arrows, between the issuer 101 and the receiver 102 of an electronic payment cheque is carried out over Short Message Service (SMS) with assistance from the central hub 300 and an SMS gateway/proxy server 401 in the BDC domain 400 of the issuer's bank and via an SMS centre SMS-C 201 in the operator's domain 200. The SMS gateway/proxy server 401 is supported by a bank application 302, which is in communication with the banking institute 500. The BDC domain 400 can be located within or in close proximity to the banking institute 500, but this is not necessary as long as the BDC domain 400 and the banking institute 500 are able to communicate.

The communication between the SMS Gateway/proxy 401, the central hub 300 and the SMS-C 201 is transparent to the Bank application 402. The SMS Gateway/proxy 401 within the BDC domain 400 is connected to the operator's SMS-C 201 using an SMS-C protocol, such as SMPP. The SMS-C 201 is responsible for sending short messages to the mobile phone upon request from the SMS Gateway/proxy 401 as well as forwarding short messages originated from the mobile phone to the SMS Gateway/proxy 401. The mobile originated short messages are addressed to a specific SME address, a so-called large account. The SMS-C maps the SME address to an address to the SMS Gateway/proxy 401 and forwards the message to the SMS Gateway/proxy 401 within the BDC domain 400. The sender of the message, i.e. the MSISDN of the mobile phone, must be transferred from the

SMS-C 201 to the SMS Gateway/proxy 401 for further delivery to the Bank application 402.

In the above, the abbreviation SME denotes "Short Message Entity", which is an entity capable of receiving and/or sending short messages. The SME can for instance be located in the mobile station or in a fixed network. The abbreviation MSISDN denotes the "Mobile Station International ISDN Number", which is the standard international telephone number used to identify a given subscriber. The number is based on the ITU-T (International Telecommunications Union-Telecommunication Standardization Sector) E.164 standard. Finally, the abbreviation SMPP denotes "short message peer to peer", where "Peer to peer" is a communications model in which each party has the same capabilities and either party can initiate a communication session.

The application messages are thus transferred as user data within short messages and are transported between the mobile phone and the SMS-C 201 using mobile originated and mobile terminated short messages. The SMS Gateway 401 also has a service listening for mobile originated messages. This service handle all messages from a mobile phone 101, 102 (independent of whether it's a mobile originating request or a response of a mobile terminated request) and delivers the messages as a XML document to the banking institute 500. The SMS gateway/proxy functionality has to be able to send a message, coded as an SMS Point-To-Point Data Download message, from one mobile phone to another.

The requirements on the SMS gateway/proxy 401 are explained closer in the following. The SMS gateway/proxy 401 must be able to cheque all messages originating from a mobile station 101, 102. Depending on the message type, the SMS gateway/proxy 401 should either route the message to the banking institute 500 or forward the message to another mobile phone 101, 102. The messages shown in fig. 1 from or to a mobile telephone includes the electronic payment cheque 10, the mobile originating application message 20

and the mobile terminated application message 30. Of course, Short Messages (SM) sent from one mobile telephone 101 to another 102 can in general comprise text messages; however, those are not shown in fig. 1 since they are not in the interest of the invention.

On messages sent from one mobile phone 101 and forwarded to another mobile phone 102. The SMS gateway/proxy 401 should perform the following:

- Take the phone number of the receiver 102 from the mobile originating application message 20 and put it in the SM header as the Destination Address.
- Take the Originating Address from the mobile originating SM header and put it in the application message as a parameter for the sender's (issuer's) phone number.
- Preferably, append the actual date from the gateway/proxy server to the application message as a parameter. Hereby the electronic payment cheque is provided with a cheque issue date providing the option that a cheque is valid for a limited time period set by the bank. A cheques' valid time can then be counted from the time the cheque is sent i.e. the date when it passes the SMS Gateway/proxy server 401 of the issuer's banking institute 500.
- Code the mobile terminated message as SMS Point-To-Point Data Download (SMS PP DD) messages. This enables the Mobile equipment to transparently forward the short messages to the SIM.

Fig. 1b shows the elements from fig. 1a in conjunction with the domain 250 of an operator of the receiver, a domain 350 of a Bank Data processing Centre (BDC domain) of the receiver of the electronic payment cheque and a banking institute 550 of the receiver, respectively. The operator's domain 250 comprises an SMS centre SMS-C 251, and the BDC domain 350 of the

receiver's banking institute comprises an SMS gateway/proxy server 351 and a bank application 352. Hollow arrows in fig. 1a and 1b indicate that some communication can take place, without specifying this communications further.

When a receiver 102 has received an electronic payment cheque, he/she can deposit it in a bank account in his banking institute 550. For this purpose, the receiver sends an SMS from the mobile telephone 102 to his/her banking institute 550 via the SMS-C 251, the hub 300, the SMS gateway/proxy server 451 and the bank application 452 to the banking institute 550. This SMS contains the electronic payment cheque 10 and a cheque deposit request 40. After receipt of the cheque deposit request 40, the banking institute 550 initiates a communication with the banking institute 500 of the issuer to carry a transfer of money indicated in the electronic payment cheque from the issuer's account to an account of the receiver into effect. The details of this communication are described below.

The receiver 102 has received the electronic payment cheque with the telephone number of the receiving mobile telephone 102, the amount to be transferred from the issuer to the receiver and the issuer account, from which the money should be withdrawn together with the digital signature generated by the application on the SIM of the mobile telephone 101; additionally the SMS gateway/proxy 301 automatically appends the MSISDN of the issuing mobile telephone 101. Thereby the issuer of the electronic payment cheque can be presented unambiguously to the receiving mobile telephone 102. The SMS gateway/proxy 301 also adds a date stamp, which provides an issue date to the electronic payment cheque.

The receiver initiates a signing of the electronic payment cheque with a second digital signature, and the electronic payment cheque, thus signed with the first and the second digital signatures is transmitted from the second mobile station 102 to the central hub 300. The hub 300 performs the following processing:

- Sends the part of the cheque, which is signed by the second user 102 to the banking institution 550 of the second user 102. The banking institution 550 of the second user 102 verifies the signature and, on basis of the GSM number and account index of the second user 102, returns the corresponding account number.

- The central hub 300 attaches the real account number received from the banking institute 550 of the second user 102 to the part of the transaction, which is signed by the first user 101. This data is sent to the banking institute 500 of the first user 101. The banking institute 500 of the first user verifies the signature from the first user and determines whether sufficient funds exist in the account indicated by the telephone number (e.g. the GSM number) and account index of the first user 101. If sufficient funds exist in the account of the first user 101, the banking institute 500 of the first user 101 initiates a transfer to the second user's account in the second banking institute 550. The banking institute 500 of the first user 101 sends a reply back to the central hub 300. If the reply is a reject, the central hub 300 sends a short message to both the first and the second user 101, 102 with information, that the transfer has been rejected. If the reply is an acknowledgement, the central hub 300 sends an application type SMS to the second user 102, which application type SMS erases the check from the SIM card of the second user 102.

No matter whether the reply is a reject or an acknowledgement of the transfer of money, the receiver of the electronic payment cheque is notified thereof substantially without delay. Likewise the receiver of an electronic payment cheque is notified of the reception substantially without delay from the receipt.

Even though only two users, BDC's, two banking institutes are shown, it should be understood, that substantially any number of users in the user

domain can perform the method of the invention. Moreover a plurality of BDC's, banking institutes, SMS centres could be used in the implementation of the invention.

The application on the SIM card of a user for implementing the method of the invention supports issuance of cheques from a plurality of accounts in different banking institutes; a user have activated the service for implementing the method in e.g. 5 different banks for use of a total of 10 accounts.

Fig. 2 is a diagram of the data flow between some of the parts performing the method of the invention. Fig. 2 shows that cheque issuer data 50 are sent from a mobile telephone 101 of the issuer a second mobile telephone 102 of the receiver of the electronic payment cheque. The cheque issuer data 50 includes at least the electronic payment cheque, the telephone number of the receiving mobile telephone 102, the amount to be transferred from the issuer to the receiver and the issuer account, from which the money should be withdrawn. The cheque issuer data also contains a digital signature generated by the application on the SIM of the mobile telephone 101. The cheque issuer data 50 have thus been confirmed and signed by the issuer before sending and is sent via SMS. The cheque issuer data 50 are sent via the SMS gateway/proxy 301 (not shown in fig. 2) of the issuer, which SMS gateway/proxy receives the SM, recodes and forwards it to the receiving mobile telephone 102.

When the receiver 102 wants to deposit a received cheque to a bank account, it can also be done via SMS. The receiver 102 enters the appropriate application on the SIM card of the mobile telephone 102 via the appropriate menu entry in the service menu and is presented with a list of all received cheques. In the next interactions the receiver 102 chooses a cheque that should be deposited and, if no default account is set, also chooses the account to which it should deposited, and he/she enters the

personal service PIN code, the PIN-RSA, to allow the transaction to be signed.

Before a cheque deposit request 51 is sent from the receiver 102, a summary of the collected information is displayed to the receiver 102. The information displayed is amount, account nickname, date and a reference number. The reference number shown is a transaction identifier concatenated with the signature identifier. The user confirms and digitally signs the summary and the cheque deposit request 51 is transmitted to the central hub 300. Thus, the cheque deposit request 51 includes both the signature of the receiver of the cheque and the signature of the issuer of the cheque.

The central hub 300 initiates a data communication 52 to the banking institution 550 of the second user 102. The central hub 300 sends the part of the cheque, which is signed by the second user 102 to the banking institution 550 of the second user 102 in the data transmission 52, and the banking institution 550 of the second user 102 verifies the signature and, on basis of the GSM number and account index of the second user 102, returns the corresponding account number to the central hub 300.

The central hub 300 attaches the real account number received from the banking institute 550 of the second user 102 to the part of the transaction, which is signed by the first user 101. This data is sent to the banking institute 500 of the first user 101 in a data transmission 53. The banking institute 500 of the first user verifies the signature from the first user and determines whether sufficient funds exist in the account indicated by the telephone number (e.g. the GSM number) and account index of the first user 101. If sufficient funds exist in the account of the first user 101, the banking institute 500 of the first user 101 initiates a transfer (not shown) to the second user's account in the second banking institute 550.

The banking institute 500 of the first user 101 sends a reply 54 back to the central hub 300. If the reply 54 is a reject, the central hub 300 sends a short

message 55, 56 to the first and the second user 101, 102, respectively, with information, that the transfer has been rejected. If the reply is an acknowledgement, the central hub 300 sends an application type SMS 55 to the second user 102, which application type SMS 55 erases the check from the SIM card of the second user 102.

The generation of digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key is well known per se, but its use in connection with the invention will be described in the following with reference to fig. 3a and 3b.

Asymmetric encryption systems, or public key systems, use two different keys, a public key 4b and a private key 4a, for encryption and decryption. The two keys 4a, 4b are dependent on each other and form a personally unique key pair, but it is not possible to calculate one key from knowledge of the other. Either the public or the private key can be used for encryption. The decryption is then made with the corresponding key of the key pair. For example, a message encrypted with a recipient's public key can be decrypted only with the same recipient's private key. The RSA (Rivest, Shamir, Adleman) algorithm is today a de facto standard for public key systems.

Hash algorithms 2 are used to create a digital fingerprint, or a message digest of a certain piece of information. Even the slightest change in the original message document produces a completely different digital fingerprint. A MAC (Message Authentication Code) is a hashed message encrypted using a symmetric key. A MAC gives message integrity but not non-repudiation. SHA-1 is a commonly used hash algorithm. It produces a 20-byte message digest of any input message.

A digital signature is created in the following way:

- An original message 1 is hashed with a hash algorithm 2 (e.g. SHA-1) and the digital fingerprint 3 of the original message is created.

- The fingerprint 3 is encrypted with the sender's private key 4a.
- The result is a digital signature 5 that is unique for every combination of message 1 and private key 4a. The message 1 and the digital signature 5 form an entity 6.

Upon reception, the digital signature 5 is verified in the following way:

- The original message in the entity 6 containing the original message 1 and the digital signature 5 is run through the hash algorithm 2 that was used in creation of the digital signature 5, thereby providing a digital fingerprint 3'.
- The signature 5 is decrypted with the sender's public key 4b, providing a decrypted, digital fingerprint 3".
- The digital fingerprint 3' and the decrypted, digital fingerprint 3" are compared at 7. If they are identical, the digital signature 5 is valid.

Digital signatures provide the following:

- Authentication of the sender's identity.
- Assurance that any changes to the message will be noticed (integrity).
- Assurance that the sender can not deny sending the message (non-repudiation).

In the method of the invention, the concepts introduced above are used to create secure transactions.

During the activation process of the service for performing the method of the invention, which will be described below, an RSA key pair is generated on the SIM card. The private key is stored in a tamperproof area on the SIM card, and the public key is exported from the mobile phone to the server in the BDC domain. In return, the server sends its own public RSA key to the

mobile phone. All RSA keys (both end-user and BDC keys) have a 1024-bit modulus and a public exponent set to 2^16+1 (=65537).

In order for the server to be able to authenticate the sender of the public key, the user has previously received a One-Time-Password (OTP) from the server on a secure, separate channel (e.g. via Internet Bank). The application on the SIM card calculates a message digest using SHA-1. The input is a concatenated string of all the information sent in the message (including the public key) and the OTP. The generated message digest is 20 bytes, but it is truncated to the first 8 bytes to create an Authentication Code.

The public key together with the other information and the Authentication Code are exported to the BDC domain. The total length of the message will be 139 bytes (1 byte Message Type + 1 byte Protocol Version + 1 byte SIM Application Version + 128 bytes Public Key + 8 bytes Authentication Code), which can be sent in one SM.

The server can then calculate an Authentication Code in the same way on the known OTP and the received information. If a comparison with the received Authentication Code is successful, it can be assumed that the public key has not been corrupted during transfer and that it indeed originates from the user. If the public key of the user is accepted, the server sends the public key belonging to the BDC domain, which will be used for server authentication purposes in subsequent operations. The message contains a new Authentication Code, which makes it possible for the application on the SIM card to verify that the message is originated from the correct source. It also contains an BDC identifier BDC-ID, which is used by the phone to link the public key to the correct BDC (in a multiple BDC scenario). The Authentication Code is again the first 8 bytes of a message digest calculated using SHA-1. The input is a concatenated string of all the information sent in the message (including the public key) and the OTP.

The public key together with the other information and the Authentication Code are sent to the mobile phone. The total length of the message will be 138 bytes (1 byte Message Type + 1 byte BDC-ID + 128 bytes Public Key + 8 bytes Authentication Code), which can be sent in one SM. The application on the SIM card can then calculate an Authentication Code in the same way on the known OTP and the received information. If the comparison with the received Authentication Code is successful, it can be assumed that the public key has not been corrupted during transfer and that it indeed originates from the BDC.

In order for the mobile phone to be able to trust OTA updates and requests from the BDC domain, a mechanism for server authentication is needed.
All information in messages from the server is encrypted using RSA with the BDC's private key according to Public Key Cryptography Standards. This creates a signature, which makes it possible for the application on the SIM card to perform server authentication upon reception of the message. In addition to the application information, the signed message contains the Message Type, the BDC identifier and a sequence number.

Note, that the Message Type and the BDC identifier are also sent unencrypted to the mobile phone, as they are needed by the SIM application before the signed message has been verified (decrypted). The Message Type is used to determine how the message should be handled. The BDC identifier is used to select the public key that should be used to decrypt the message.

The sequence number is a 3-byte integer generated by the BDC, which must be incremented for each new operation that the BDC requests towards a specific user, i.e. a separate counter is used for each user.
Before the encryption operation, the information has to be padded to 128 bytes. Since no hash of the message is calculated, the hash algorithm

identifier will not be included. Basically, the padding is performed in the following way:

- Construct a padding string consisting of (128-[length in bytes of data to sign]-3) octets with the hexadecimal value FF.
- Concatenate the padding string, the message to be signed, and delimiters to form the padded message

The padded message is then signed by the BDC by encrypting the information with the private key of the BDC.When the message is received, the SIM application performs the following steps:

- The message is decrypted using RSA with the BDC's public key. The BDC-D is used to select which public key is used to decrypt the message.
- The padding is checked to verify that the information has not been changed after it was signed, and then removed to recover the signed data. For additional security, the BDC-ID and the Message Type in the signed message can also be compared to the BDC-ID and the Message Type that were sent unencrypted to verify that the information has not been changed.
- The sequence number is compared to the sequence number received with the latest OTA request, in order to prevent replay attempts. The number must be incremented by the server for each new OTA request.

Mobile transactions initiated by the user are signed and can be listed as follows:

- Issue cheque (via SMS)
- Deposit cheque (via SMS)

The transactions are signed using RSA according to Public Key Cryptography Standards.

Below, the parameters and their order as they are signed during the transaction are outlined. The SHA-1 hash is calculated on the following concatenated data in each transaction.

Issue cheque

MSISDN_receiver	(20 bytes)
BDCID_issuer	(1 byte)
AccountID_issuer	(1 byte)
ChequeAmount	(15 bytes)
ChequeID	(3 bytes)

The format on the telephone number of the receiver, MSISDN_receiver, when signed is the complete international phone number, entered by the user, without the leading '+' or "00" string.

Deposit cheque

BDCID_receiver	(1 byte)
AccountID_receiver	(1 byte)
SignID	(3 bytes)
ChequeIssueDate	(8 bytes)
Signature_issuer	(128 bytes)

In the transaction summary a 7-digit reference number (RefNo) is displayed to the user. The RefNo is usually a 4-digit transaction identifier (TrxID) concatenated with the user's 3-digit signature identifier (SignID). During a deposit cheque transaction, however, no interaction with a pay-box takes place and no TrxID can therefore be received. To keep the RefNo in a uniform format to the user the TrxID is in this operation replaced with a dummy value ("0000") which is not signed.

In signature calculation, the 20-byte result of the SHA-1 operation above is padded to 128 bytes and encrypted using RSA with the user's private key.

The padding is done according to the EMSA-PKCS1-v1_5 encoding operation. Basically, the padding is performed in the following way:

- Hash the message using SHA-1.
- Construct a SHA-1 hash algorithm identifier using DER (Distinguished Encoding Rules). This results in the following octet string:

  30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14
- Construct a padding string consisting of 90 octets with the hexadecimal value FF.
- Concatenate the padding string, the algorithm identifier, the hashed message, and delimiters to form the padded message:

00 || 01 || FF FF [...86xFF...] FF FF || 00 || 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 || [hashed message]

The signature verification is done in the following way:

- Hash the original transaction using SHA-1 and apply the padding described above.
- Decrypt the signature using RSA and the user's public key.
- Compare the hashed and padded transaction with the decrypted signature. If they match, the signature is valid.

The user registration, i.e. the activation of the applications on the SIM card, will be described below. The registration described takes place via an Internet bank. It is presumed, that the user has received a new SIM card from the operator and has been instructed to activate the service for performing the method of the invention through the Internet Bank. Therefore, it is implicitly presumed, that the user is a registered user of an Internet Bank and that a trusted relationship thus already exists between the user and the bank. Moreover it is presumed, that the user has registered to the service for performing the method of the invention via the Internet Bank, and that the bank thereafter has sent a request to an operator for issuing and distributing

a new SIM card supporting the applications for performing the method of the invention to the user. Moreover, it is presumed, that the mobile telephone is switched on and the new SIM card is inserted.

The user selects a menu choice in the Internet Bank for activation of the service for performing the method of the invention. Then an 8-digit One-Time-Password (OTP) is displayed to the user on the screen. This information is used in the SIM application to provide user authentication and initiate the key generation. The user is instructed to select the menu choice for activation of the service for performing the method of the invention on the mobile phone.

The user selects an option "Service activation" in the menu on the mobile phone and enters the OTP. Entering the OTP triggers generation of the RSA key pair on the SIM card. The private key is stored in a tamperproof location on the SIM card. The application on the SIM card calculates an Authentication Code. The input is all information in the message, i.e. the message type, the OTA protocol version, the SIM application version, and the public key of the user, concatenated with the OTP. The generated 8-byte Authentication Code is then sent together with the other parameters in a SM to the BDC domain.

Note that an SME address (phone number) is needed on the SIM card to send messages to the BDC domain. The SME address can be pre-configured on the SIM card, but in a multiple BDC environment, the SME address may preferably be displayed to the user on the computer screen together with the OTP, and then entered into the mobile phone after the OTP.

Before the public key is accepted for use within the BDC domain, the Authentication Code received from the mobile phone is compared with an Authentication Code calculated locally in the BDC domain on the same parameters. If the comparison is successful the public key is stored.

If the public key of the user is accepted, the BDC domain exports its own public key, which will be used for server authentication purposes in subsequent operations. The message contains a new Authentication Code, which makes it possible for the application on the SIM card to verify that the message is originated from the correct source. It also contains the BDC-ID, which is used by the phone to link the public key to the correct BDC (in a multiple BDC scenario).

The Authentication Code is calculated, and the input is all information in the message, i.e. the message type, the BDCID, and the public key of the BDC, concatenated with the OTP. The generated 8-byte Authentication Code is then sent together with the other parameters in a SM to the mobile phone.

When the message is received, the application on the SIM card validates the Authentication Code by comparing it with an Authentication Code calculated locally in the mobile phone on the same parameters. If the validation is successful, the public key is stored and the BDC domain is notified of the result.

The BDC domain then sends a message to the mobile phone containing the information required for configuration of the application on the SIM card. The information package is signed (encrypted) with the BDC's private key before it is sent to the mobile phone. This makes it possible for the SIM application to perform server authentication upon reception of the message.

In addition to the application information, the signed message contains the Message Type, the BDC-ID and a sequence number. The Message Type and the BDC-ID are also sent unencrypted, as the SIM application needs these parameters in order to handle the message. The message is then signed**Error! Reference source not found.**.

IPR2025-00645 Page 00601

When the message is received, the SIM application verifies the signed message and checks the sequence number. The BDC-ID is used to select the public key that should be used to verify the message.

If the validation is successful, the application data is stored and the BDC domain is notified of the result. The sequence number received in the request from the BDC is returned in the response and could be used on the server side to link the result to the corresponding request.

The user is requested to select a PIN code of 4 digits, which will be used to get access to the key files on the SIM card. This PIN code is referred to as PIN-RSA herein. Finally, the user is informed that the service for performing the method of the invention has been activated through a text message on the mobile phone display.

A useful functionality that can be provided by the central hub is to handle a cheque book via a web server. When a user sends a cheque to another user, the transmission passes through the central hub and the SMS-server. When the central hub registers the cheque, it can send a "Cheque issued" message to the web server. The "cheque issued" message contains the telephone number of the issuer and of the receiver, account index, cheque identification, the amount of money to be transferred and the date. The web server writes these data in a cheque book table.

When the receiver of an electronic payment cheque deposits the cheque, this will be performed via the central hub. When the central hub receives an acknowledgement of the transfer of money from the issuer's banking institute, the central hub sends a "cheque cleared" message to the web server. This "cheque cleared" message contains cheque identification, the telephone number of the issuer and of the receiver, the amount of money to be transferred and the date. The web server puts this cheque into a "cheque cleared" table. Hereby, the issuer as well as the receiver automatically has an updated cheque book of issued and received cheques.

Via a web interface a user (i.e. an issuer and/or a receiver) can connect to the web server and see all issued cheques. For instance, the following five possibilities might exist: "All cheques", "cleared cheques", "issued cheques", "received cheques" and "cashed cheques".

"All cheques" shows a list of all the cheques the user have issued and/or received with the status thereof (deposited or not deposited at an account in a banking institute). "Cleared cheques" shows a list of the cheques that the user has sent and which have been deposited by the receiver(s) thereof. "Issued cheques" shows a list of the cheques that the user has sent but which have not been deposited yet by the receiver(s) thereof. "Received cheques" shows a list of the cheques that the user has received but which have not yet been deposited and "Cashed cheques" shows a list of the cheques that the user has received and which have been deposited at an

account in a banking institute. The facility "Cleared cheques" provides the user with the possibility to determine whether a cheque has been deposited, which could be of relevance in the situation of a receiver asserting not to have received the cheque. If a receiver asserts not to have received a sent cheque, the cheque can be retransmitted. This re-transmittal is secure, in that the banking institute would reject any duplicate cheques.

Moreover, this cheque book service can include general filtering mechanisms such that a user can choose only to see cheques issued and/or received within a chosen time interval, from and/or to chosen telephone numbers, etc.

A cheque will expire after a specified number of days. The web sever can notify a user who has an "un-cashed" cheque, when the expiration date thereof is approaching by means of a Short Message.

Above, it has been explained that messages can be sent as Short Messages via the SMS service. However, due to the large amount of information and the signature in a cheque, a cheque issued and sent from an issuer to a receiver has to be sent as two short messages. The signature of the first user is split into two parts and the cheque is then sent as two SM, with one part of the signature in each. To be able to associate the messages again on the receiver's side each message must contain a reference to the other part of the message; this parameter is called the MessageReference and is a one-byte counter that is unique for each user. Both messages must include the phone number (MSISDN) of the receiver to allow the SMS proxy to forward the messages to the receiver. The second part of the cheque sent from the issuer to the receiver, containing the second part of the signature.

As explained in detail above, the deposit of a cheque issued by an issuer and sent to a receiver at the banking institute of the receiver can be started up by means of Short Messages sent from the receiver. Again, due to the large amount of information and the need to include both the issuer's and the receiver's signatures, the request message has to be sent as three short

messages. The first SM contains the cheque information and the next two short messages contain the signatures of the receiver and the issuer respectively. To be able to associate the messages again on the receiver's side each message must contain a reference to the other parts of the message; this parameter is called the MessageReference and is a one-byte counter that is unique for each user.

It is well known to use mobile telephones provided with IrDA, fast IrDA or Bluetooth facilities to withdraw money from Automatic Teller Machines ATM. If the electronic payment cheque service is implemented in the SIM card of a mobile telephone with the IrDA, fast IrDA or Bluetooth facility, the mobile telephone can be used to withdraw the amount of money in the electronic payment cheque by means of an ATM. Moreover, the user could choose to withdraw some of the amount of money indicated in the electronic payment cheque from the ATM and deposit the remaining part of the amount into an account.

In general, it should be noted that point-to-point communication between a mobile station (mobile telephone) and another mobile station also could be in accordance with the IrDA or fast IrDa standard, the Bluetooth standard, Wi-Fi standard and/or any other near-range communication standard

CLAIMS:

1. A method of processing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute (500) to an account of a second user in a second banking institute (550), which processing includes generating digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key, characterized in that, the method comprises the following steps:

in a first SIM card (101a) of the first user, creating an electronic payment cheque and signing the electronic payment cheque with a first signature generated by means of a first private key of a first asymmetric key pair, which first private key resides on the first SIM card (101a) hosted by a first mobile equipment (101b) ,

via the first mobile equipment (101b) hosting the SIM card (101a) of the first user, transmitting the signed electronic payment cheque to a second SIM card (102a) hosted in a second mobile equipment (102b) of the second user,

in the second SIM card (102a), signing the electronic payment cheque, which has been signed with the first signature, with an additional second signature generated on the second SIM card (102a) by means of a second private key of a second asymmetric key pair, which second private key resides on the second SIM card (102a) hosted by the second mobile equipment (102b),

transmitting the electronic payment cheque signed with the first and the second digital signatures from the second mobile equipment (102b) to a central hub (300), which central hub (300) is in communication with the first and the second banking institutes (500, 550),

IPR2025-00645 Page 00606

in the central hub (300), initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user by initialising a verification of the second signature at the banking institution (550) of the second user and a verification of the first signature at the banking institution of the first user (500).

2. A method according to claim 1, wherein the first and the second private key are generated on the first and the second SIM card (101a, 102a), respectively.

3. Method according to claim 1, wherein the transmittal of the signed electronic payment cheque from the first mobile equipment (101b) hosting the SIM card (101a) of the first user to the second SIM card (102a) hosted in a second mobile equipment (102b) of the second user, is performed via a digital mobile telephone system.

4. A method according to any of the claims 1 to 3, wherein the signed payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system.

5. A method according to any of the claims 1 to 3, wherein the signed payment cheque is transmitted as a Short Message by means of Ir, Bluetooth or Wi-Fi standards.

6. A method according to any of the claims 1 to 5, wherein creating of an electronic payment cheque comprises indicating a telephone number associated to the second SIM card (102a), an amount to be transferred and an index to the account, wherefrom the amount should be withdrawn.

7. A method according to any of the claims 1 to 6, wherein the method further comprises:

via the first mobile equipment (101b), prompting the first user to confirm creation of an electronic payment cheque, which prompting is initiated at the first SIM card (101a) hosted by the first mobile equipment (101b).

8. A method according to claim 7, wherein the conformation comprises entering of a PIN-RSA number.

9. A method according to any of the claims 1 to 8, wherein the encrypted electronic payment cheque is transmitted via a message proxy in the central hub (300).

10. A method according to claim 9, wherein the encrypted electronic payment cheque at the message proxy is converted to an SMS Point-to-point data download message, which subsequently is transmitted to the second SIM card hosted by the second mobile equipment.

11. A method of issuing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute (500) to an account of a second user in a second banking institute (550), which issuing includes generating a digital signature by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key, characterized in that, the method comprises the following steps:

in a first SIM card (101a) of the first user, creating an electronic payment cheque and signing the electronic payment cheque with a first signature generated by means of a first private key of a first asymmetric key pair, which first private key resides on the first SIM card (101a) hosted by a first mobile equipment (101b) ,

via the first mobile equipment (101b) hosting the SIM card (101a) of the first user, transmitting the signed electronic payment cheque to a second SIM card (102a) hosted in a second mobile equipment (102b) of the second user.

12. A method according to claim 11, wherein the first private key is generated on the first SIM card (101a).

13. Method according to claim 11 or 12, wherein the transmittal of the signed electronic payment cheque from the first mobile equipment (101b) hosting the SIM card (101a) of the first user to the second SIM card (102a) hosted in a second mobile equipment (102b) of the second user, is performed via a digital mobile telephone system.

14. A method according to any of the claims 11 to 13, wherein the signed payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system.

15. A method according to any of the claims 11 to 14, wherein the signed payment cheque is transmitted as a Short Message by means of Ir, Bluetooth or Wi-Fi standards.

16. A method according to any of the claims 11 to 15, wherein creating of an electronic payment cheque comprises indicating a telephone number associated to the second SIM card (102a), an amount to be transferred and an index to the account, wherefrom the amount should be withdrawn.

17. A method according to any of the claims 11 to 16, wherein the signed electronic payment cheque is transmitted via a message proxy.

18 A method according to claim 17 wherein the signed electronic payment cheque at the message proxy is converted to an SMS Point-to-point data download message, which subsequently is transmitted to the second SIM card (102a) hosted by the second mobile equipment (102b).

19. A method of depositing a received electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute (500) to an account of a second user in a second banking

institute (550), which processing includes generating digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key, characterized in that, the method comprises the following steps:

in the second SIM card (102a), signing the received electronic payment cheque, which has been signed with a first signature, with an additional second signature generated on the second SIM card (102a), by means of a second private key of a second asymmetric key pair, which second private key resides on the second SIM card (102a) hosted by the second mobile equipment (102b),

transmitting the electronic payment cheque signed with the first and the second digital signatures from the second mobile equipment (102b) to the central hub (300), which central hub (300) is in communication with the first and the second banking institutes (500, 550),

in the central hub (300), initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user by initialising a verification of the second signature at the banking institution (550) of the second user and a verification of the first signature at the banking institution (500) of the first user.

20. A method according to claim 19, wherein the second private key is generated on the second SIM card (102a).

21. A method according to claim 19 or 20, wherein the signed received payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system.

22. A method according to any of the claims 19 to 21, wherein the signed received electronic payment cheque is transmitted via a message proxy in the central hub (300).

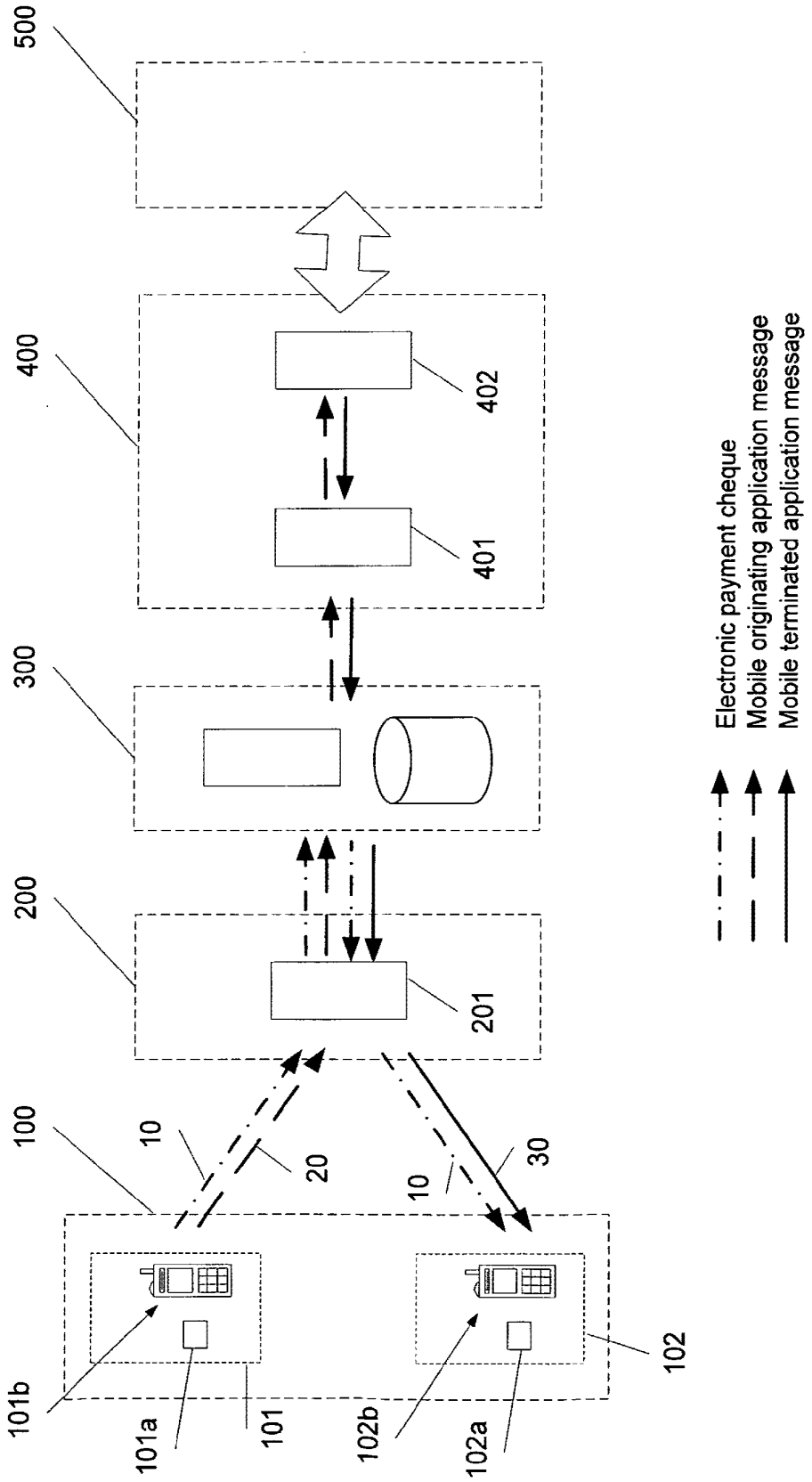

500
400
402
401
300
200
201
100
10
20
10
30
101b
101a
101
102b
102a
102
Electronic payment cheque
Mobile originating application message
Mobile terminated application message

Fig. 1a

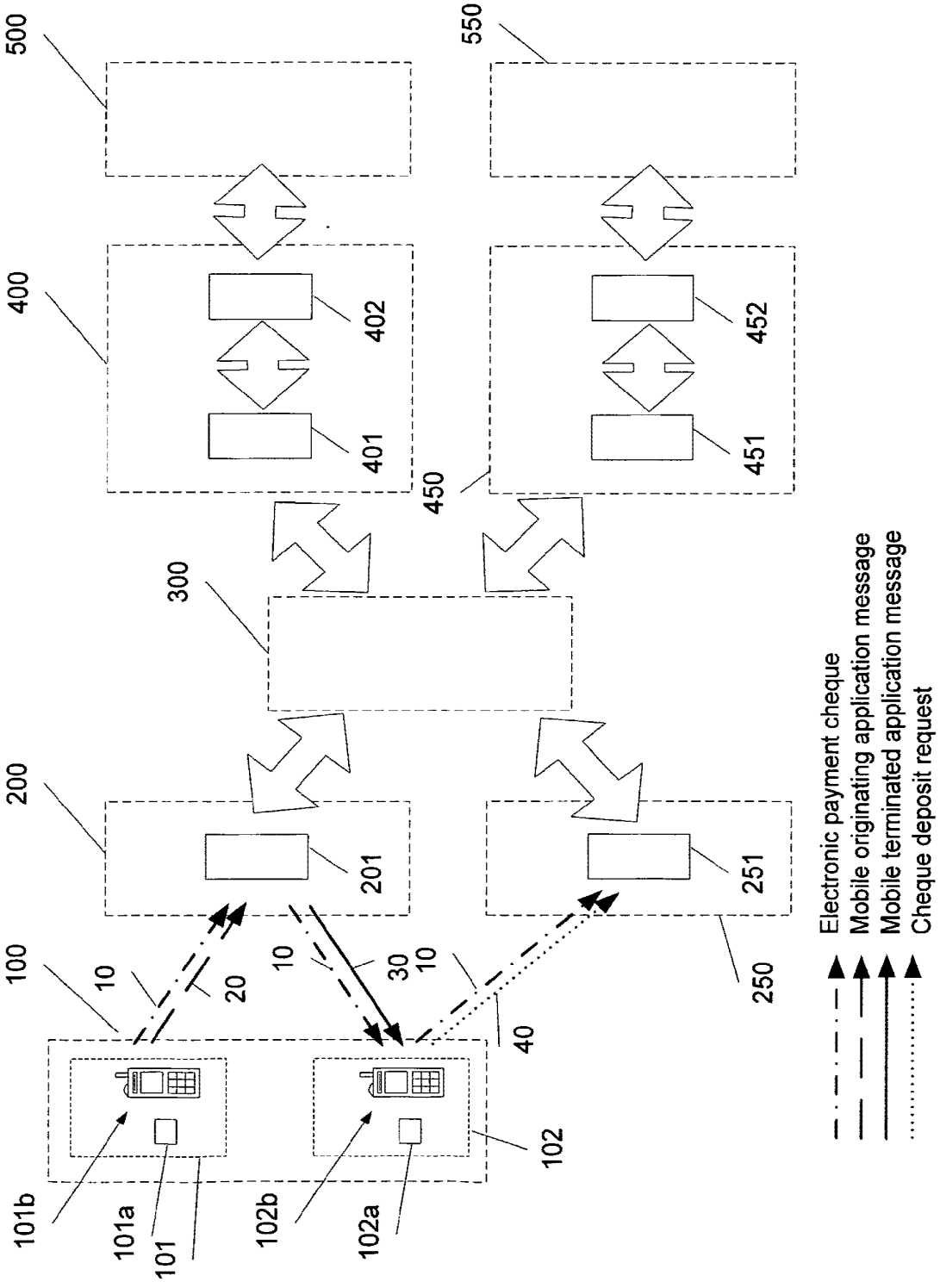

500
550
400
402
401
452
451
450
300
200
201
251
250
100
10
20
10
30
10
40
101b
101a
101
102b
102a
102
Electronic payment cheque
Mobile originating application message
Mobile terminated application message
Cheque deposit request

Fig. 1b

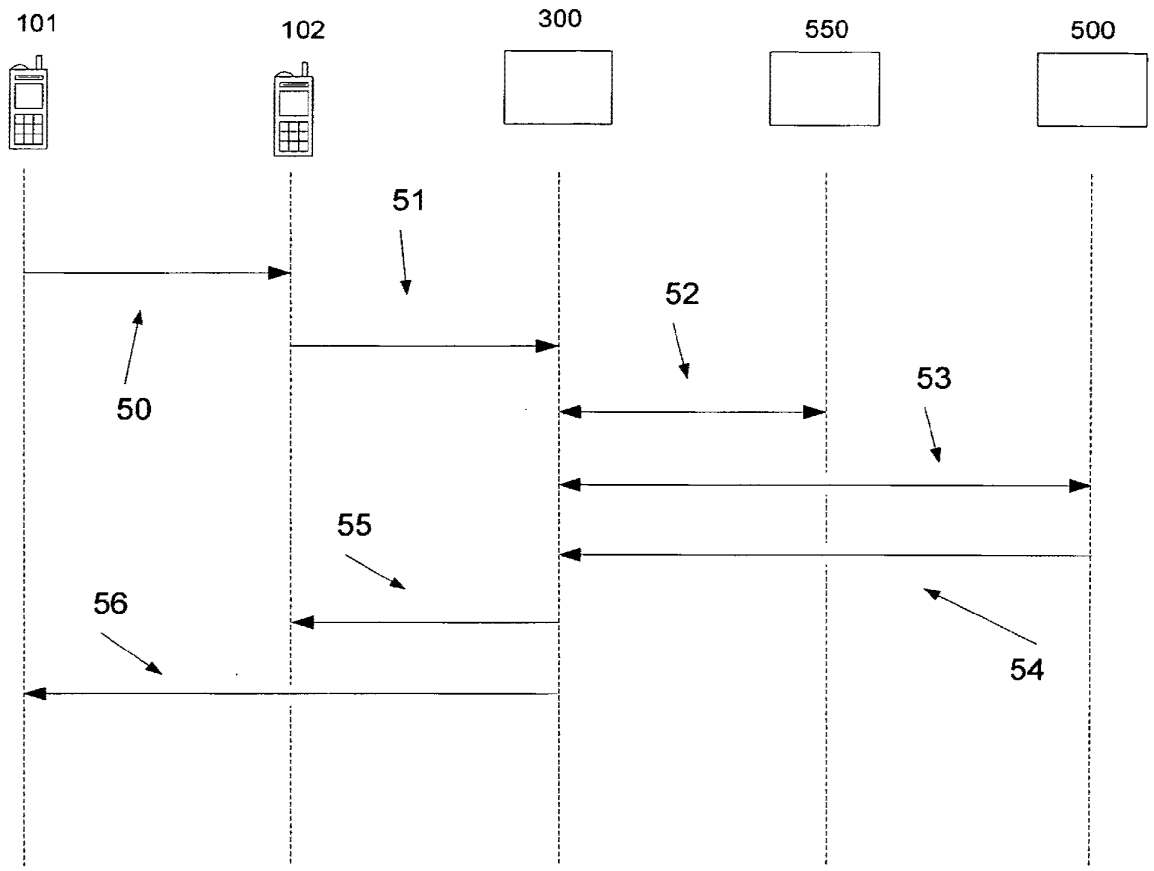


Fig. 2

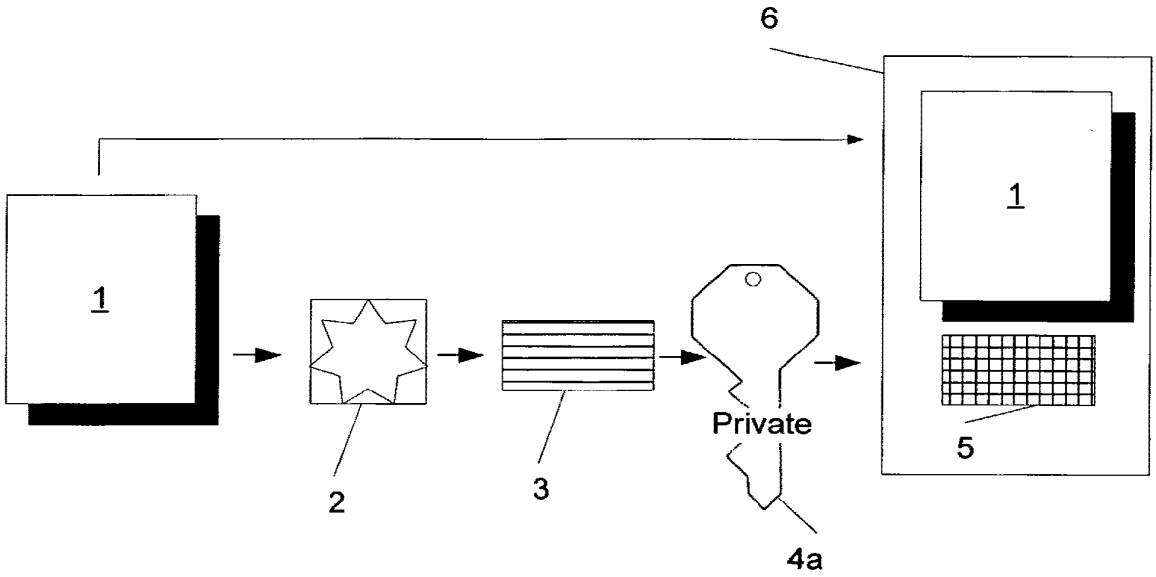


Fig. 3a

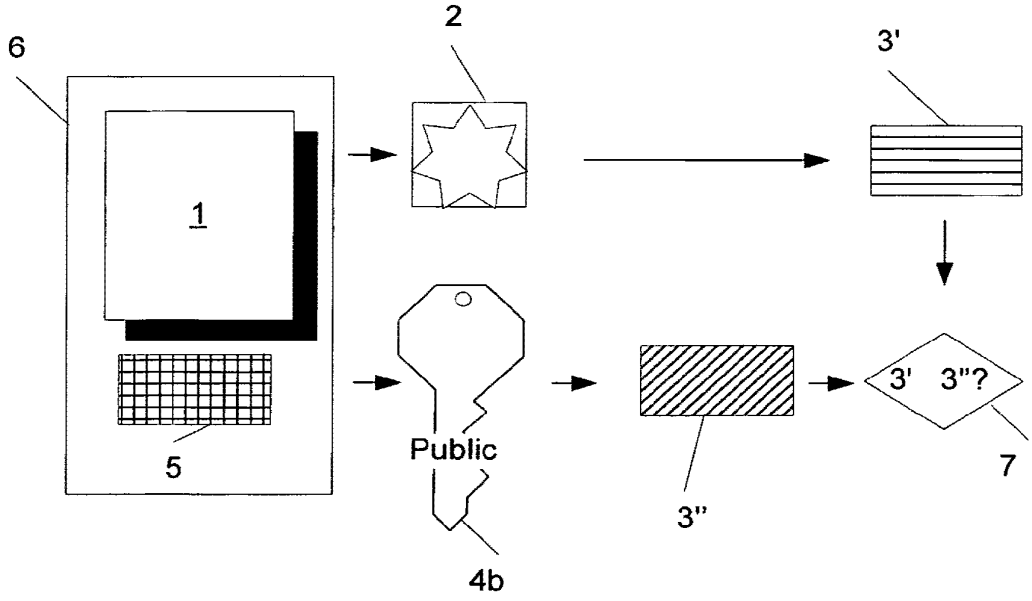


Fig. 3b

INTERNATIONAL SEARCH REPORT

Int[illegible]onal Application No
PCT/DK 03/00163

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28 G07F19/00

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 H04L 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)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 677 955 A (ANDERSON MILTON M ET AL) 14 October 1997 (1997-10-14) cited in the application column 3, line 2 -column 6, line 41	1-3,5,6, 8,11-13, 15,16, 19,20
A	EP 0 986 275 A (SWISSCOM AG) 15 March 2000 (2000-03-15) column 3, line 49 -column 5, line 12	1-22
A	US 5 511 121 A (YACOBI YACOV) 23 April 1996 (1996-04-23) column 8, line 40-45 column 9, line 29 -column 10, line 1	1-22

☐ 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
13 May 2003	20/05/2003

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	Weinmiller, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ›nal Application No
PCT/DK 03/00163

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5677955	A	14-10-1997	BR	9608448 A	07-12-1999
			CA	2217593 A1	10-10-1996
			EP	0819345 A1	21-01-1998
			JP	11503541 T	26-03-1999
			WO	9631965 A1	10-10-1996
EP 0986275	A	15-03-2000	EP	0986275 A1	15-03-2000
			JP	2000163487 A	16-06-2000
			US	6415156 B1	02-07-2002
US 5511121	A	23-04-1996	CA	2182173 A1	31-08-1995
			EP	0746923 A1	11-12-1996
			JP	9505169 T	20-05-1997
			WO	9523465 A1	31-08-1995

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2003 (02.10.2003)

PCT

(10) International Publication Number
WO 03/081519 A2

(51) International Patent Classification[7]: G06K 7/00

(21) International Application Number: PCT/US03/08638

(22) International Filing Date: 19 March 2003 (19.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/366,098 19 March 2002 (19.03.2002) US
60/379,964 13 May 2002 (13.05.2002) US

(71) Applicant: CHAMELEON NETWORK INC. [US/US]; Suite 1400, 950 Winter Street, Waltham, MA 02451 (US).

(72) Inventors: THOMAS, Joseph, A.; 34 Warren Street, Westborough, MA 01581 (US). JESSEN, Karlin, B.; 97 Pleasant Street, Reading, MA 01867 (US). BURGER, Todd, O.; 386 Lincoln Street, Lexington, MA 02421 (US). HASSOL, Joshua, L.; 28 Wachusett Drive, Lexington, MA 02421 (US).

(74) Agent: PRITZKER, Randy, J.; Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210 (US).

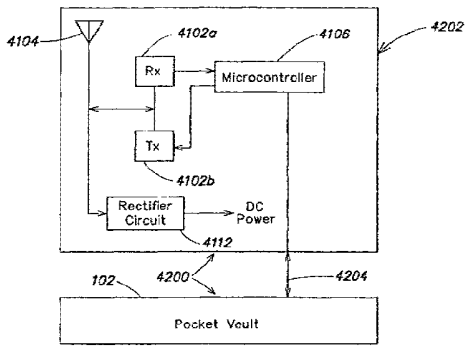
(81) Designated State *(national)*: CA.

(84) Designated States *(regional)*: European patent (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).

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: PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD



(57) Abstract: In one embodiment, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user. In another embodiment, an apparatus comprises, a memory, a user input, and a transponder. The memory stores at least first and second distinct codes. The user input permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal. The transponder emits a wireless signal representing the selected one of the at least first and second code sin response to an interrogation signal. In yet another embodiment, a token that may be used to engage in a transaction at a point of sale comprises a substrate, a rewritable memory, and a reconfigurable display. The rewriteable memory is supported by the substrate and can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale. The substrate and memory are configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The reconfigurable display is also supported by the substrate and displays at least some of the information that is stored in the rewritable memory.

WO 03/081519 A2

PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD

RELATED APPLICATIONS

This application is a Continuation-in-Part (CIP) of Application Serial No. 09/968,628, filed October 1, 2001, and now pending, which is a CIP of U.S. Application Serial No. 09/675,438, filed September 28, 2000, and now pending, which claims the benefit of each of: (1) Application Serial No. 60/156,356, filed September 28, 1999; (2) Application Serial No. 60/167,050, filed November 23, 1999; (3) Application Serial No. 60/184,425, filed February 23, 2000; and (4) Application Serial No. 60/217,542, filed July 12, 2000. This application also claims the benefit of each of (1) Application Serial No. 60/366,098, filed March 19, 2002, and (2) Application Serial No. 60/379,964, filed May 13, 2002.

FIELD OF THE INVENTION

The present inventions are directed to novel systems and methods for engaging in transactions involving financial and/or non-financial media.

BACKGROUND OF THE INVENTION

People often times carry wallets with them when they engage in their day to day activities. A typical wallet is made of leather or other suitable material, and is generally a foldable structure that readily fits into a pocket or purse. A wallet typically includes a number of pockets, pouches, or the like for storing items such as a driver's license, a social security card, identification cards, credit cards, debit cards, membership cards, commuter passes, access tools, business cards, cash, coupons, event tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipts, photographs, etc.

Wallets are frequently stolen, lost, or misplaced. When any of these events occurs, not only must the wallet itself be replaced, but all of the contents of the wallet must be replaced as well. As anyone who has lost a wallet can testify, replacing the contents of a wallet can be cumbersome and expensive. In addition, if a wallet is stolen or if a lost wallet falls into the wrong hands, the contents of the wallet may be used to engage in unauthorized activities which financially detriment the wallet owner, as well as

any banks, credit issuers, and/or other institutions that issued financial media to the wallet owner.

While the wallet owner is generally able to "cancel" financial media in such situations by contacting the respective financial media issuers, often times this is done too late, i.e., after one or more media have been exploited by the unauthorized user. In some cases, the wallet owner may not recall all of the contents of the now stolen wallet, and so may fail to report theft of one or more items. Further, in addition to any cash contained in a lost or stolen wallet, many media issued by non-financial media issuers have a significant cash value, e.g., transportation tickets, event tickets, commuter passes, and the like, and therefore represent an immediate (and often times unrecoverable) financial loss to the wallet owner. Moreover, the misappropriation of media issued by non-financial media issuers that contain personal information, e.g., a drivers license, social security card, identification card, etc., present the opportunity for an unauthorized possessor of a wallet to engage in the practice known as "identity theft," whereby the possessor may assume the identity of the wallet owner for various fraudulent purposes, e.g., using the assumed identity to obtain and exploit one or more new financial media.

Another device commonly used to engage in or authorize transactions is a radio frequency identification (RFID) tag. In an RFID system, an "interrogator" broadcasts a radio frequency (RF) signal which, if received by an RFID tag, causes the RFID tag to return an RF signal to the interrogator that includes information from the tag that may be used to authorize a transaction. Situations in which such tags have been employed include, e.g., automated toll booths and gasoline service stations. RFID tags may be made relatively small in size and therefore may be kept virtually anywhere, e.g., on a keychain or clipped to an automobile visor. Unfortunately, while this aspect of these devices make them convenient, it also makes them highly susceptible to loss or theft. Whenever an RFID tag falls into the wrong hands, there is potential for it to be misused for a long period of time before it is discovered to be missing and some action is take to disable the account associated with it so that it can no longer be used to authorize transactions.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal

representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user.

According to another aspect, an apparatus comprises, a memory, a user input, and a transponder. The memory stores at least first and second distinct codes. The user input permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal. The transponder emits a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

According to yet another aspect, a token that may be used to engage in a transaction at a point of sale comprises a substrate, a rewritable memory, and a reconfigurable display. The rewriteable memory is supported by the substrate and can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale. The substrate and memory are configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The reconfigurable display is also supported by the substrate and displays at least some of the information that is stored in the rewritable memory.

According to another aspect, a method for using an apparatus comprises steps of using the apparatus to authenticate an identity of a user of the apparatus, and after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal.

According to another aspect, a method for using an apparatus comprises steps of manipulating a user input on the apparatus to select one of at least first and second codes stored in memory, and permitting a transponder of the apparatus to emit a wireless signal representing the selected one of the at least first and second codes in response to a wireless interrogation signal.

According to yet another aspect, a method for configuring a token to be used to engage in a transaction at a point of sale involves a step of configuring a rewritable memory of the token to store information that identifies an account that may be used to engage in the transaction at the point of sale. The memory is configured and arranged on the token such that the token can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The method further

involves a step of configuring a display on the token to display at least some of the information that is stored in the rewritable memory.

According to another aspect, a method is disclosed for enabling a software module on a computer operated by a user to access restricted information on a server. With an electronic device distinct from the computer, an identity of the user is authenticated to determine that the user is permitted to access the restricted information on the server. In response to the electronic device authenticating the identity of the user, the software module on the computer is permitted to access the restricted information on the server.

According to another aspect, a method is disclosed for altering settings on a computer to correspond to settings on an electronic device distinct from the computer. With the electronic device, an identity of a user is authenticated to determine that the user is authorized to use the electronic device. In response to authenticating the identity of the user, the settings on the computer are altered to correspond to settings on the electronic device.

According to another aspect, a system for enabling a software module on a computer operated by a user to access restricted information on a server includes an electronic device which includes a user-authenticator to authenticate an identity of the user to determine that the user is permitted to access the restricted information on the server. The system further comprises means for, in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

According to yet another aspect, a system for altering settings on a computer to correspond to settings on an electronic device distinct from the computer comprises a user authenticator included in the electronic device to authenticate an identity of a user to determine that the user is authorized to use the electronic device. The system further comprises means for, in response to authenticating the identity of the user, altering the settings on the computer to correspond to settings on the electronic device.

According to another aspect, an apparatus includes a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory, supported by the housing, that stores transaction information for at least first and second media; and at least one output, supported by the housing, that releases at

least a portion of the transaction information to a point-of-sale (POS) terminal after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: (a) storing transaction information for at least first and second media in a memory of a device (b) using the device to authenticate an identity of a user; and (c) after authenticating the identity of the user with the device, transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus.

According to another aspect, a method involves steps of: storing transaction information for at least one media in a memory of a first device; using the first device to authenticate an identity of a user; and after authenticating the identity of the user with the first device, releasing an embedded identification code of the apparatus from the housing that enables a second device receiving the embedded identification code to authenticate the identity of the first device.

According to another aspect, an apparatus includes: at least one memory that stores transaction information for at least first and second media; at least one input that enables a user to select one of the at least first and second media; a display that provides a visual indication to the user regarding which of the at least first and second media has been selected with the at least one input; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect, a method involves steps of: storing transaction information for at least first and second media in a memory of a device; receiving as input a user's selection of one of the at least first and second media; displaying a visual indication to the user regarding which of the at least first and second media has been selected; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, an apparatus includes: at least one memory that stores transaction information for at least one financial media and at least one non-financial media; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect, a method involves steps of: storing transaction information for at least one financial media and at least one non-financial media in a memory of a device; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, a system includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a device releasably attached to the housing; and configuring means, supported by the housing, for selectively configuring the device to hold the transaction information so that the device may be used to engage in a transaction involving the at least one media.

According to another aspect, a method involves steps of: (a) storing transaction information for at least one media in a memory of a first device, the first device having a second device releasably attached thereto; (b) while the second device is attached to the first device, configuring the second device to hold the transaction information for the at least one media based on the contents of the memory; (c) detaching the second device from the first device; and (d) using the second device to engage in a transaction involving the at least one media.

According to another aspect, a system includes: a first device including a user authenticator that authenticates an identity of a user; and a second device releasably attached to the first device, wherein the second device holds transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media, and wherein the second device is detached from the first device after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: with a first device, authenticating an identity of a user; and after authenticating the identity of a user with the first device, detaching a second device from the first device, the second device holding transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media.

According to another aspect, a system includes: a first device; a second device that has the first device releasably attached thereto, the second device including means for selectively configuring the first device to hold transaction information for a first media but not for a second media so that the first device may be used to engage in a transaction involving the first media but not the second media, and the second device further including means for selectively configuring the first device to hold transaction information for the second media but not for the first media so that the first device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect, a method involves steps of: selectively configuring a device to hold transaction information for a first media but not for a second media so that the device may be used to engage in a transaction involving the first media but not the second media; and selectively configuring the device to hold transaction information for the second media but not the first media so that the device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect, a system includes: at least one memory that stores first transaction information for a first media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively add second transaction information for a second media to the memory.

According to another aspect, a method involves steps of: storing first transaction information for a first media in a memory of a device; releasing at least a portion of the first transaction information to a point-of-sale (POS) terminal; and in response to a request by the person to whom the first transaction information is issued, adding second transaction information for a second media to the memory.

According to another aspect, a system includes: at least one memory that stores first transaction information for a first media and second transaction information for a second media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively remove at least a portion of the second transaction information from the memory.

According to another aspect, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in a memory of a device; releasing at least a portion of the first transaction information to a

point-of-sale (POS) terminal; and, in response to a request by the person to whom the second media is issued, removing at least a portion of the second transaction information from the memory.

According to another aspect, a system includes: at least one memory that stores transaction information for at least one media; at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal; and means for enabling at least one functional characteristic of the at least one media to be altered by altering the contents of the least one memory.

According to another aspect, a method involves: storing transaction information for at least one media in a memory of a device; releasing at least a portion of the transaction information to a point-of-sale (POS) terminal; and altering at least one functional characteristic of the at least one media by altering the contents of the least one memory.

According to another aspect, an apparatus includes: a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory that, supported by the housing, stores first transaction information for a first media and second transaction information for a second media; and at least one output, supported by the housing, that releases the first transaction information only after the user authenticator has authenticated the identity of the user, and that releases the second information without requiring the user authenticator to have authenticated the identity of the user.

According to another aspect, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in at least one memory of a device; using the device to authenticate an identity of a user; releasing the first transaction information only after the identity of the user has been authenticated; and releasing the second transaction information without requiring the identity of the user to be authenticated.

According to another aspect, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device causes the first device to generate a machine-readable code for only a predetermined, finite period of time after the first device is detached from the second device.

According to another aspect, a method involves a step of generating a machine-readable code on a device for only a predetermined, finite period of time.

According to another aspect, an apparatus includes: a portable substrate; a power supply supported by the substrate; and at least one controller supported by the substrate and powered by the power supply, the at least one controller being configured to generate a simulated magnetic stripe on the substrate.

According to another aspect, an method involves a step of generating a simulated magnetic stripe on a portable device.

According to another aspect, a system includes: at least one memory that stores transaction information for at least one media; a user authenticator that authenticates an identity of the user; and a display that provides a visual indication to the user regarding the at least one media, the visual indication being displayed for only a predetermined, finite period of time after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: authenticating an identity of a user; and displaying a visual indication to the user regarding the at least one media for only a predetermined, finite period of time after authenticating the identity of the user.

According to another aspect, a system includes a portable device that can be used to engage in point-of-sale (POS) transactions; and a device remote from the portable device, that can disable an ability of the portable device to engage in POS transactions.

According to another aspect, a method involves steps of: providing a portable device that can be used to engage in point-of-sale transactions; and at a location remote from the portable device, disabling an ability of the portable device to engage in POS transactions.

According to another aspect, a method involves steps of: storing transaction authorization information for at least two media in a first memory of a first device; and storing the transaction authorization information for the at least two media in a second memory, which is disposed at a location remote from the first device.

According to another aspect, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device can cause the first device to generate a machine-readable code after the first device is detached from the second device, the second device including at least one controller configured so as to be capable of causing

the first device to generate the machine-readable code only for a finite, predetermined period of time.

According to another aspect, a method involves a step of configuring a first device such that the first device is capable, for only a predetermined, finite period of time, of generating a machine-readable code on a second device.

According to another aspect, a method involves steps of: receiving information at a first device that has been transmitted over an electronic communication link; and after receiving the information at the first device, using a media at the first device to access a quantity of credit or cash reserves that could not be accessed prior to the first device receiving the information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating an example of a network system in which a portable electronic authorization device (also referred to herein as a "Pocket Vault") may be employed according to one embodiment of the invention;

Fig. 2 is a block diagram showing an illustrative embodiment of the Pocket Vault shown in Fig. 1;

Fig. 3 is a block diagram showing an illustrative embodiment of one of the interface stations shown in Fig. 1;

Fig. 4 is a block diagram showing an illustrative embodiment of the network server(s) shown in Fig. 1;

Fig. 5 is a diagram showing an example of how the memory of the Pocket Vault shown in Fig. 2 may be configured in accordance with one embodiment of the invention;

Fig. 6 is a block diagram showing an illustrative embodiment of the token (e.g., a card) associated with the Pocket Vault shown in Fig. 2;

Fig. 7 is a flow diagram illustrating a primary routine that may be executed by the controller of the Pocket Vault shown in Fig. 2;

Fig. 8 is a flow diagram illustrating an example implementation of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7;

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine shown in Fig. 10;

Fig. 12 is a flow diagram illustrating an example implementation of the VERIFY CARD RETURN routine shown in Fig. 7;

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the pocket vault interface unit shown in Fig. 3;

Fig. 14 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the interface station computer shown in Fig. 3;

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine shown in Fig. 14;

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 14;

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine in Fig. 14;

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine shown in Fig. 14;

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller(s) of the network server(s) shown in Fig. 4;

Fig. 20 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO REGISTER NEW POCKET VAULT HOLDER routine shown in Fig. 19;

Fig. 21 is a flow diagram illustrating an example implementation of the PROCESS REQUEST BY MEDIA ISSUER/ADVERTISER TO UPDATE NETWORK SERVER routine shown in Fig. 19;

Fig. 22 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 19;

Fig. 23 is a flow diagram illustrating an example implementation of the PROCESS REQUEST FROM HOLDER TO LOAD NEW FILE ONTO NETWORK SERVER routine shown in Fig. 19;

Fig. 24 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine shown in Fig. 19;

Fig. 25 is a flow diagram illustrating an example implementation of the AUTHORIZED POCKET VAULT USE? routine shown in each of Figs. 20, 22, and 24; and

Figs 26a-26p are illustrations of the portable electronic authorization device, as well as the token (e.g., a card) associated therewith, as these items may appear when in use;

Fig. 27 is a block diagram illustrating several additional features that may optionally be added to a network system such as that shown in Fig. 1 so as to enhance the functionality of the network;

Fig 28 is a block diagram illustrating example components that may optionally be added to software executing on a controller of the Pocket Vault, such as the software described in connection with Figs. 7-12, so as to enhance the functionality of the Pocket Vault in a network environment;

Fig 29 is a data flow diagram illustrating an example of how data may flow between the Pocket Vault and a user interface of an interface station computer to which the Pocket Vault is interfaced/docked;

Fig. 30 is a flow diagram illustrating an example of a primary routine that may be executed by a website on the network server(s) shown in Fig. 27, which website may be accessed, for example, by a browser executing on the interface station computer shown in Fig. 27;

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine shown in Fig. 30;

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine shown in Fig. 33;

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine shown in Fig. 33;

Fig. 36 is a flow diagram illustrating an example implementation of the RECOVERY routine shown in Fig. 33;

Fig. 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine shown in Fig. 33;

Fig. 38 is a flow diagram illustrating an example implementation of the BACKUP routine shown in Fig. 33;

Fig. 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine shown in Fig. 33;

Fig. 40 is a flow diagram illustrating an example implementation of the RFID TAG LOADING routine shown in Fig. 33;

Fig. 41 is a block diagram showing a prior art RFID tag; and

Fig. 42 is a block diagram showing an example embodiment of an RFID system in which a Pocket Vault such as that shown in Fig. 2 is used to selectively provide data to an RFID tag.

DETAILED DESCRIPTION

Disclosed herein is a new method and system for producing, distributing, storing, and using the typical contents of a person's wallet, as well as the multiple, separate transaction authorization devices, e.g., RFID tags, owned by the person. Essentially, the system may enable individuals to replace nearly all of the paper and plastic contents of their wallets and all of their other transaction authorization implements with a single, hand-held portable electronic authorization device. The system may include the portable electronic authorization devices, removable morphing tokens or cards associated with such devices, associated computer peripherals, software and certain network capabilities. As a whole, the system may eliminate virtually all of the distribution costs and security concerns associated with paper and plastic media.

Because the device may incorporate many different media that are commonly stored in a person's wallet or elsewhere, possibly including both financial and non-financial media, it is much more than a simple point-of-sale (POS) device. Therefore, the device may be more appropriately referred to as a multi-purpose, "point-of-transaction" device. In any situation of presentment, whether for purposes such as

building security, demonstrating membership or using credit or debit capacity, the system is designed to perform tasks more safely, securely and with greater ease than is possible with prior art systems. Further, while certain computer technologies are involved, the preferred embodiment is such that some people may barely recognize it as a computer, seeing instead a more comfortable to carry, easier-to-use, safer and more securely packaged means of transporting typical wallet contents and other items.

The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various financial and non-financial media, that also may enable individuals and retailers to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns.

A network system 100 configured according to one illustrative embodiment of the invention is shown in Fig. 1. As shown, the network system 100 may include a portable electronic authorization device 102 (alternatively referred to herein as a "Pocket Vault") and an associated token 102a (alternatively referred to herein as a "Chameleon Card"). Each person desiring to use the network system 100 may possess his or her own the Pocket Vault 102 and associated token 102a. Some individuals may choose to own multiple Pocket Vaults or Chameleon Cards. The system and software therefore may accommodate the use of multiple Pocket Vaults and multiple Chameleon Cards by one individual.

Referring to Fig. 1, in addition to the Pocket Vault 102, the network system 100 may include one or more network servers 114 to which various other network components are coupled. Although multiple, load-sharing network servers 114 may be employed in a typical application, the network server(s) 114 will hereinafter, for convenience, occasionally be referred to as a single network server 114. Coupled to the network server 114 are: several different types of interface stations 104 (i.e., a validation interface station 104a, a personal interface station 104b, and a commercial interface station 104c), one or more commercial card readers 106, one or more commercial bar code readers 107, one or more RFID interrogators 116, and several computers 108, 110,

and 112 operated by one or more advertisers, non-financial media issuers, and financial media issuers, respectively. The structure and functionality of each of the components of the network system 100 in accordance with illustrative embodiments of the invention are described below.

As shown in Fig. 1, the network server 114 may form the hub of the network system 100, with each of the interface stations 104, the commercial card readers 106, the commercial bar code readers 107, the RFID interrogators 116, and the computers 108, 110, and 112 being coupled thereto. As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders.

Any of a number of techniques may be used to interconnect the various elements of the network system 100, and the invention is not limited to any particular networking technique. In one illustrative embodiment, for example, the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between most of the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links).

As shown in Fig. 1, the Pocket Vault 102 may be interfaced with any of the interface stations 104a-c so as to permit information to be uploaded from the network server 114 to the Pocket Vault 102, or to be downloaded from the Pocket Vault 102 to the network server 114. In one illustrative embodiment, each of the interface stations 104 includes a docking mechanism that permits a Pocket Vault 102 to be physically, as well as electronically, interfaced therewith. In such an embodiment, once the Pocket Vault 102 is physically "docked" with an interface station 104, the Pocket Vault 102 may communicate with the interface station 104 using any now known or later discovered technique. For example, physical contact may be made between respective electrodes or plugs, a line of sight (e.g., infrared) wireless link may be established, or any other interfacing technique may be employed.

The Pocket Vault 102 may additionally or alternatively be configured such that it need not be physically docked with or even in the same room as the interface station 104, as a wireless network such as Bluetooth may be employed to permit communication between devices on the network system 100. In fact, in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114, without the interface stations 104a-c facilitating communication therebetween. In addition, in some embodiments, Pocket Vaults 102 may communicate directly with one another. In such embodiments, such inter-device communication may permit value to be exchanged directly between Pocket Vaults 102.

The personal docking station 104b may allow setting or changing of user preferences, recording of miscellaneous information by the Pocket Vault holder, replenishment or deletion of information regarding particular media, and may also permit additional media (e.g., a library card) to be added to the device. The Pocket Vault holder may, for example, directly add non-value-based media (e.g., a membership number for the local Historical Society) and notes to the Pocket Vault 102. In one embodiment, value-based and certain identification media (a driver's license, passport, building security ID, etc.) may be added or reinstated only through a secure connection to the network server 114 (as described below), in response to an update request from the Pocket Vault holder. In addition, the personal interface station may provide a mechanism to download transaction activity involving the Pocket Vault 102 into an individual's home computer. There are many users of home finance software. These applications can be relatively "data hungry," and commonly require users to download checking and debit card data from their banks (or key it in manually) and to key in the details of credit card and cash purchases. All of this keying and internet file downloading from third parties may be replaced by a simple docking procedure, i.e., when the Pocket Vault 102 is interfaced with the personal docking station 102b.

As shown in Fig. 1, and as described below in more detail, the Pocket Vault 102 may be equipped to generate the token 102a such that the token 102a has transactional information regarding a media (e.g., an actual or simulated magnetic stripe or a bar code) produced thereon. In such an embodiment, after the token 102a has been generated, the token 102a may be used by the Pocket Vault holder to engage in a transaction wherein an entity swipes the magnetic stripe portion of the token 102a through a card reader 106 or

scans the bar code on the token 102a using a bar code reader 107. Additionally or alternatively, the token 102a may include a suitable Smartcard interface so that it may be used with Smartcard compatible devices.

Because the token 102a may be caused to take on a different personality each time it is released from the Pocket Vault 102, a plurality of media may be stored electronically in memory of the Pocket Vault 102, and the token 102a may, upon request, be generated to take on the personality selected by the Pocket Vault holder. The respective media stored on the Pocket Vault 102 may be issued by different and unrelated media issuers. As used herein, two media issuers are "unrelated" if there exists no legal relationship between them.

The token 102a may also have display capacity. Such a display may, for example, indicate the media personality the token 102a has taken on. In addition, for security purposes, the account number of the media, and perhaps other information, for example, the three digit security code typically found on credit cards, may be shown on the display of the token 102a after it is ejected from the Pocket Vault. The display of this information may help prevent fraudulent uses of the token 102a because the entity accepting it would be able to verify that the displayed information matched that read by the device used to read the token 102a, e.g., a magnetic card reader.

In some embodiments, value may be exchanged between two Pocket Vaults 102 when one the Pocket Vault 102 generates a token 102a having a value-based or value-linked media stored thereon, and the token 102a so generated is passed to the other the Pocket Vault 102, which then may then access the media and extract value therefrom or add value thereto. As mentioned above, this sort of value exchange may also be accomplished directly between two Pocket Vaults 102 over a wireless network, such as Bluetooth.

As discussed in more detail below, in addition to or in lieu of the token 102a, the Pocket Vault 102 may also generate a bar code for a selected media on the Pocket Vault's display (not shown in Fig. 1), and the bar code reader 107 may be used to scan the displayed bar code to process a transaction. Further, a transaction may be processed via a commercial interface station 104c either by use of a docking terminal or via a wireless network scheme such a Bluetooth. In one embodiment, some commercial interface stations 104c may comprise an interface station linked to a standard commercial