NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims,description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
115.001WO1		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2006/006361	21/02/2006	22/02/2005
Applicant		
TYFONE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/006361

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K19/073

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)
G06Q G06K G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 316 908 A (JOHN * COWLING) 11 March 1998 (1998-03-11) page 2, paragraph 2 - page 5, paragraph 4; figure 1	1
Y		2-8, 11-14, 19,20
A	US 2004/087339 A1 (GOLDTHWAITE SCOTT ET AL) 6 May 2004 (2004-05-06) abstract	1-8, 15-20
A	US 6 721 196 B1 (GRASSL THOMAS) 13 April 2004 (2004-04-13) abstract	1-8,19, 20

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
11 September 2006	22/09/2006

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	Beatty, John

1

Form PCT/ISA/210 (second sheet) (April 2005)

IPR2025-00645 Page 01304

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/006361

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96/26500 A (PEEK, GARRY) 29 August 1996 (1996-08-29) page 6, line 7 - page 10, line 18	9,10,15, 17
Y	the whole document	2-8, 11-14, 19,20

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

IPR2025-00645 Page 01305

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/006361

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2316908 A	11-03-1998	NONE	
US 2004087339 A1	06-05-2004	AU 2003288963 A1	07-06-2004
		EP 1563697 A2	17-08-2005
		WO 2004043048 A2	21-05-2004
US 6721196 B1	13-04-2004	AT 239296 T	15-05-2003
		AU 5683500 A	31-01-2001
		BR 0011868 A	09-04-2002
		CA 2377175 A1	04-01-2001
		CN 1358315 A	10-07-2002
		DE 19928733 A1	04-01-2001
		WO 0101418 A1	04-01-2001
		EP 1198797 A1	24-04-2002
		ES 2193968 T3	16-11-2003
		JP 2003503834 T	28-01-2003
WO 9626500 A	29-08-1996	AU 4498296 A	11-09-1996

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2006/006361	21.02.2006	22.02.2005

International Patent Classification (IPC) or both national classification and IPC
INV. G06K19/073

Applicant
TYFONE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Beatty, John Telephone No. +49 89 2399-7562

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-8,11-14,18-20
	No:	Claims	9,10,15-17
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Documents

Reference is made to the following documents:

D1: GB-A-2 316 908 (JOHN COWLING) 11 March 1998 (1998-03-11)
D2: US 2004/087339 A1 (GOLDTHWAITE SCOTT ET AL) 6 May 2004 (2004-05-06)
D3: US-B1-6 721 196 (GRASSL THOMAS) 13 April 2004 (2004-04-13)
D4: WO 96/26500 A (PEEK, GARRY) 29 August 1996 (1996-08-29)

2. Article 6 PCT

The subject-matter of claim 1 defines a memory card in part through its compatibility with a memory card slot in a mobile phone. However, the memory card slot in the mobile phone is not defined by any technical feature. Therefore, this feature of the memory card is unclear. For the purposes of the search, this feature has therefore been considered as being a standard card wherein the mobile phone has a standard card interface.

3. Article 33(2) PCT

3.1 Independent Claim 9

The subject-matter of independent claim 9 is not new for the following reasons.

The document D4 discloses (the references in parentheses applying to this document):

An apparatus (figure 1) comprising:

means for communicating through a memory card slot in an electronic device (standard magcard reader in combination with a personal computer; figure 5; page

7, lines 4-24);
means for producing at least one time-varying magnetic field to represent financial transaction data (page 7, lines 11-14; page 6, lines 7-16); and
means for storing the financial transaction data (personal computer; page 7 last paragraph).

3.2 Independent Claim 15

The subject-matter of independent claim 15 is not new for the following reasons.

The document D4 discloses (the references in parentheses applying to this document):

An electronic transaction card comprising:

a memory card slot transaction interface (magnetic stripe; figures 3 and 5; page 7, lines 4-17); and
circuitry for producing a time-varying magnetic field compatible with a magnetic card reader (figure 5; page 7, lines 4-17).

3.3 Dependent Claim 10

The subject-matter of dependent claim 10 is not new since personal computers may at any time comprise software to be installed upon them.

3.4 Dependent Claims 16-17

The subject-matter of dependent claims 16-17 is not new over D4. See D4, page 7, line 4 - page 10, line 18.

4. Article 33(3) PCT

4.1 Independent Claim 1

The document D1 discloses a memory card (figure 1; page 2, paragraph 2 - page 5, paragraph 4) compatible with a memory card slot (page 4, paragraph 3), the memory card including non-volatile memory accessible by a device (ROM (12);

page 2, paragraph 2), a point-of -sale interface to communicate with a point-of-sale terminal (magnetic stripe; page 2, paragraph 4), and second non-volatile memory to hold financial transaction data (1 Mb Flash ROM (14); page 2, paragraph 4).

Thus, the memory card claimed differs from that of D1 in that:

i) The memory card is accessible by a mobile phone via the memory card slot being in a mobile phone; and
ii) the second memory is volatile memory as opposed to non-volatile memory.

The two features do not appear to combine to solve any particular problem but rather are directed at two separate respective problems namely:

i) How to enable a mobile phone to read data from a card.
ii) How to ensure financial transaction data is accessed rapidly.

With respect to problem i), the use of memory card slots is known in mobile phones (see D2, Abstract) and therefore the skilled person when presented with the task of enabling a mobile phone to read data from the card of D1 would consider it a normal design choice to provide the mobile phone with an appropriate card reader.

With respect to problem ii), the skilled person would be aware of that the contents of a Random Access Memory (RAM), which is volatile memory, can be accessed rapidly by storing said data in a volatile memory. He would be aware that a semiconductor memory chip for a smart card may comprise both volatile and non-volatile memory (see D3, abstract) and would therefore store data in either a volatile or non-volatile memory according to design choice in order to provide the desired function.

Thus, the skilled person would arrive at the subject-matter of claim 1 without making an inventive step.

4.2 Dependent Claims 2-8,11-14,18-20

The skilled person when starting from D1 as the closest prior art and with

knowledge of the documents D2-D4 would solve the respective problem posed without making an inventive step. See the relevant citations in the International Search Report.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 115.002WO1	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2006/013603	International filing date *(day/month/year)* 07 April 2006 (07.04.2006)	Priority date *(day/month/year)* 07 April 2005 (07.04.2005)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant TYFONE, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☒	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 09 October 2007 (09.10.2007)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Beate Giffo-Schmitt e-mail: pt03.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2006/013603	07.04.2006	07.04.2005

International Patent Classification (IPC) or both national classification and IPC
INV. G07F7/10 G07F7/08 G06K19/077

Applicant
TYFONE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Mülthaler, E Telephone No. +49 89 2399-7625

Form (PCT/ISA/237) (Cover Sheet) (April 2005)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-25
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-25
Industrial applicability (IA)	Yes:	Claims	1-25
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item VIII

Certain observations on the international application

The application contains more than one independent claim in the same category without meeting one of the following points: (a) a plurality of interrelated products (such as a plug and a socket), (b) different uses of a product, or (c) alternative solutions to a particular problem which cannot be covered by a single claim. None of this applies to the present application. Independent claims 1, 9, 15 and 20 are all apparatus/system claims disclosing the same subject-matter.

Moreover, the set of claims should be formulated concisely. A diversity of wording for defining one and the same invention should be avoided in order not to render the claims inconsistent with each other and thus unclear.

Consequently, in the present case, it is appropriate to use only one independent claim, namely one for an apparatus/system.

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: WO 98/12674 A (WAVE HOLDINGS LIMITED; WHITE, MARTIN, DAVID; FIELD, JOHN, DESMOND) 26 March 1998 (1998-03-26)

D2: EP-A-1 117 068 (C. MEDIA CO. LTD; ITOCHU CORPORATION) 18 July 2001 (2001-07-18)

D3: EP-A-1 014 290 (NOKIA CORPORATION; NOKIA MOBILE PHONES LTD) 28 June 2000 (2000-06-28)

D4: US-B1-6 189 786 (ITOU SHINJU ET AL) 20 February 2001 (2001-02-20)

D5: WO 00/14678 A (IC TV INTERACTIVE CYBER TELEVISION INC; COMBALUZIER, PIERRE, MICHEL) 16 March 2000 (2000-03-16)

The present application does not meet the criteria of Article 33(1) PCT, because the

subject-matter of claims 1, 9, 15 and 20 is not new in the sense of Article 33(2) PCT.

1. Independent claim 1:
The document D1 discloses (the references in parentheses applying to this document):
An apparatus (fig. 1) comprising:
- a body portion having a contour to receive an intelligent electronic device (fig. 1: ref. 14 and fig. 8b);
- a first interface to provide communication with the electronic device (fig. 1: ref. 14 and fig. 8b) and;
- a second interface to provide communication with an electronic transaction card (fig. 1: ref.25 and figure 5)

Therefore, the subject-matter of independent claim 1 is **not new (Article 33(2) PCT)**.

2. Independent claim 9:
Document D2 discloses (the references in parentheses applying to this document):
A sleeve to provide communication between a handheld intelligent electronic device and an electronic transaction card (figure 12c: ref. J1), the sleeve comprising:
- an add-on slot to receive the electronic transaction card (fig. 12c: ref. 85); and
- an interface to communicate with the handheld intelligent electronic device (fig. 12c: ref. D1)

Therefore, the subject-matter of independent claim 9 is **not new (Article 33(2) PCT)**.

3. Independent claims 15 and 20:
The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 15 and 20 which are also considered not new.

4. Dependent claims:
Dependent do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step, see documents D1-D5 and the corresponding passages cited in the search report.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 115.012WO1	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2006/027847	International filing date *(day/month/year)* 18 July 2006 (18.07.2006)	Priority date *(day/month/year)* 18 July 2005 (18.07.2005)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant TYFONE, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 10 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☒	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☒	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☒	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 22 January 2008 (22.01.2008)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Yoshiko Kuwahara e-mail: pt07.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2006/027847	18.07.2006	18.07.2005

International Patent Classification (IPC) or both national classification and IPC
INV. G06K19/06 G06K19/07

Applicant
TYFONE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☒ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Berger, Christian Telephone No. +49 89 2399-2689

Form (PCT/ISA/237) (Cover Sheet) (April 2005)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of

☐ the entire international application

☒ claims Nos. 13-23

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international search *(specify)*:

☐ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. are so unclear that no meaningful opinion could be formed *(specify)*:

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed *(specify)*:

☒ no international search report has been established for the whole application or for said claims Nos. 13-23

☐ a meaningful opinion could not be formed without the sequence listing; the applicant did not, within the prescribed time limit:

- ☐ furnish a sequence listing on paper complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
- ☐ furnish a sequence listing in electronic form complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
- ☐ pay the required late furnishing fee for the furnishing of a sequence listing in response to an invitation under Rules 13*ter*.1(a) or (b).

☐ a meaningful opinion could not be formed without the tables related to the sequence listings; the applicant did not, within the prescribed time limit, furnish such tables in electronic form complying with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions, and such tables were not available to the International Searching Authority in a form and manner acceptable to it.

☐ the tables related to the nucleotide and/or amino acid sequence listing, if in electronic form only, do not comply with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions.

☐ See Supplemental Box for further details

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees, the applicant has, within the applicable time limit:

   ☐ paid additional fees

   ☐ paid additional fees under protest and, where applicable, the protest fee

   ☐ paid additional fees under protest but the applicable protest fee was not paid

   ☒ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

   ☐ complied with

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, this report has been established in respect of the following parts of the international application:

   ☐ all parts.

   ☒ the parts relating to claims Nos. 1-12

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-12
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-12
Industrial applicability (IA)	Yes:	Claims	1-12
	No:	Claims	

2. Citations and explanations

   see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Re Item IV.

The separate inventions/groups of inventions are:

Claims 1 - 12:
Independent apparatus claim 1 claims an electronic stripe card comprising a conductive path with two portions in sufficient distance to each other in order to allow the first portion to mimic a magnetic track without interference from a magnetic field from the second portion.
Independent apparatus claim 4 claims an electronic stripe card comprising two layers and a conductive path alternating between the two layers wherein the two path portions on the respective layers are in sufficient distance to each other in order to avoid magnetic interference.
The claims concern the problem of how to provide a magnetic track mimic using less material.

Claims 13 - 23:
Independent apparatus claim 13 claims an electronic stripe card having two conductive paths, each path to mimic a track in a magnetic card, further having a swipe sensor and an interleaved track driver circuit.
Independent method claim 19 claims a method comprising the step of detecting a swipe by swipe sensor and the step of interleaved driving first and second conductive paths to mimic a respective magnetic track.
Both claims concern the problem of how to save power in the reading mode and how to eliminate cross talk between two tracks.

They are not so linked as to form a single general inventive concept (Rule 13.1 PCT) for the following reasons:

Document WO2005/027030 (24.03.2005) shows in its figures 1 - 3 a magnetic stripe card having a conductive path for mimicking a magnetic track (cf. fig. 3A). Hence, the common features of the independent claims are known from the prior art. The remaining features of independent claims 1 and 4 on one hand and of independent claims 13 and 19 on the other hand concern mutually exclusive objective problems (cf. above claim analysis) and

their solutions (Rule 13.2 PCT).

Re Item V.

1 Reference is made to the following document:

D1 : WO 2005/027030 A (HUMAN TECHNOLOGIES INC [JP]; KUROKAWA FUJIO [JP]; HIGUCHI TSUYOSHI [JP) 24 March 2005 (2005-03-24)

2 INDEPENDENT CLAIM 1

2.1 The present application does not meet the criteria of Article 33(1) PCT, because the subject matter of claim 1 does not involve an inventive step in the sense of Article 33(3)PCT.

2.1.1 Document D1, which is considered to represent the most relevant state of the art to the subject matter of claim 1, discloses (the references in parentheses applying to this document) an electronic stripe card (1) comprising
a conductive path having first portions oriented to carry current in a "z" direction (cf. fig. 5: 133(13)) and having second portions oriented to carry current in a "-z" direction (135(13)),
wherein the first and second portions are separated (cf. fig. 5).

2.1.2 The subject-matter of independent claim 1 differs from the disclosure of D1 in that D1 does not explicitly state in its English abstract (the rest of the document being provided in Japanese) that the first and second portions are separated by a sufficient distance to allow a magnetic field created by the first portions to mimic a magnetic track without interference from a magnetic field created by the second portions.

2.1.3 Figures 3B, 4B and 5B of D1, however, provide a strong hint to the skilled person by the shown magnetic field lines that the distance between the upper

and the lower portion should be large enough in order avoid interference of the magnetic field of the upper portion by the lower portion, thereby arriving at the subject-matter of claim 1.

2.1.4 Therefore, the subject-matter of claim 1 does not involve an inventive step (Article 33(3) PCT).

3 INDEPENDENT CLAIM 4

3.1.1 Document D1, which is considered to represent the most relevant state of the art to the subject matter of claim 1, discloses (the references in parentheses applying to this document) an electronic stripe card (1) comprising
a top metal layer (cf. fig. 5: 133(13)) and a bottom metal layer (135(13)) without magnetic material therebetween, and
a conductive path alternating between the top metal layer and the bottom metal layer (cf. fig. 5A: the conductive path can be interpreted as alternating).

3.1.2 The subject-matter of independent claim 1 differs from the disclosure of D1 in that D1 does not explicitly state in its English abstract that the conductive path on the top metal layer is remote from the conductive path on the bottom metal layer to reduce magnetic flux interference.

3.1.3 For the same reasons as given in above paragraph 2.1.3 for claim 1 the subject-matter of claim 4 does not involve an inventive step (Article 33(3) PCT).

4 DEPENDENT CLAIMS 2, 3, 5 - 12

Dependent claims 2, 3 and 5 - 12 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of inventive step (Article 33(3) PCT).

Re Item VII.

5 Claims 2 and 3 are obviously erroneously dependent on claim 4 instead of being dependent on claim 1.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 115.019WO1	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2008/057588	International filing date *(day/month/year)* 20 March 2008 (20.03.2008)	Priority date *(day/month/year)* 30 March 2007 (30.03.2007)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant TYFONE, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 06 October 2009 (06.10.2009)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Nora Lindner e-mail: pt11.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
DANA LEMOINE
LEMOINE PATENT SERVICES
C/O INTELLEVATE
900 SECOND AVE SOUTH, SUITE 1700
MINNEAPOLIS, MN 55402

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	07 AUG 2008
Applicant's or agent's file reference 115.019WO1	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 08/57588	20 March 2008 (20.03.2008)	30 March 2007 (30.03.2007)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06F 12/00 (2008.04)
USPC - 711/103

Applicant TYFONE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	31 July 2008 (31.07.2008)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. type of material

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing

      ☐ contained in the international application as filed

      ☐ filed together with the international application in electronic form

      ☐ furnished subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	None	YES
	Claims	1-26	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-26	NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-26 lack novelty under PCT article 33(2) as being anticipated by US 2005/0022002 A1 to Poisner.

As to claim 1, Poisner discloses a method comprising: receiving a memory access command, the memory access command including an address field and a data field (see para [0050]); comparing at least a portion of the data field to a predetermined data value to determine if there is a match ('the data field may contain one or more bits indicating whether the command is a protected command' see para [0050]-[0051]); if there is not a match, performing a memory access according to the memory access command (' If not, the command is determined to be directed to non-protected configuration space, and processing continues in FIG. 3B at point "B" of the flow chart' see Fig 3B, para [0049]); and if there is a match, diverting the memory access command for further interpretation (' If the command is determined to be a protected command, processing may continue in FIG. 3B at point "A" of the flow chart' see Fig 3B, para [0051]).

As to claim 2, Poisner discloses a method further comprising comparing the address field with a predetermined address value to determine if there is an address match, and diverting the memory access command only when there is also an address match ('After the command is detected by interface logic and the destination address of the command is decoded, it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space' see Fig 3A, para [0047]).

As to claim 3, Poisner discloses a method wherein diverting the memory access command comprises passing at least some of the data field to a non-memory controller component for further interpretation (' Configuration "space" is a conceptual term that refers to the range(s) of addresses that are reserved for implementation in logic circuit 120 for various activities, with accesses that are targeted to any address within the configuration space being redirected to various portions of logic circuit 120 rather than to memory 140 or to input-output devices' see para [0011], para [0049]).

As to claim 4, Poisner discloses a method further comprising reading a password from the data field to authenticate access to the non-memory controller component ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 5, Poisner discloses an article having a machine readable medium with instructions stored thereon that when accessed result in a machine (see para [0008]): comparing data received with a memory write command to a predetermined data value to determine whether the memory write command should be interpreted as a memory write command or whether the memory write command should be interpreted as a command other than a memory write command ('Read or write commands to at least a portion of the addresses in the configuration space are redirected to configuration registers in logic circuit 120. In some embodiments, another portion of the addresses in the configuration space are used for commands that trigger some type of action within the logic circuit 120 rather than being used to store data in, or read data from, a register' see para [0011]).

As to claim 6, Poisner discloses an article wherein the instructions, when accessed, further result in the machine forwarding the memory write command to a memory controller component when the memory write command should be interpreted as a memory write command. (see para [0011]-[0013]).

As to claim 7, Poisner discloses an article wherein the instructions, when accessed, further result in the machine forwarding the memory write command to a non-memory controller component when the memory write command should be interpreted as a command other than a memory write command ('Configuration space may be implemented with addresses that would otherwise be part of memory address space or input-output (I/O) address space. Read or write commands to at least a portion of the addresses in the configuration space are redirected to configuration registers in logic circuit 120' see abstract, para [0010]-[0012]).

As to claim 8, Poisner discloses an article having a machine readable medium with instructions stored thereon (see para [0008]) that when accessed result in a machine: comparing an address field received with a memory write command to a predetermined address value to determine whether the memory write command should be interpreted as a memory write command or whether the memory write command should be interpreted as a command other than a memory write command ('the address itself may be sufficient to indicate whether the command is a protected command' see Fig 3A-3B, para [0049]-[0051]).

--(Continued in Supplemental Box)--

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Box V, 2. Citations and explanations:

As to claim 9, Poisner discloses a method comprising populating fields in a memory write command to be sent to a memory card interface (interface logic) by populating at least a first portion of a data field with a data pattern to identify the memory write command as a command to be diverted for purposes other than a memory write ('the data field may contain one or more bits indicating whether the command is a protected command,' see para [0047], para [0050]).

As to claim 10, Poisner discloses a method further comprising prior to populating the fields, receiving a copy of the data pattern from a device coupled to the memory card interface ('placing predetermined data on the data lines' see para [0010]).

As to claim 11, Poisner discloses a method further comprising populating an address field with an address value to further identify the memory write command as a command to be diverted for purposes other than a memory write ('placing a predetermined address on the address lines' see para [0010]).

As to claim 12, Poisner discloses a method further comprising populating a second portion of the data field with a command index to specify a purpose other than a memory write ('For example, a command may set or clear a hardware flag, initiate a microcode sequence, or cause some other event to happen' see para [0053]).

As to claim 13, Poisner discloses a method further comprising populating a second portion of the data field with a password to authenticate access to a device coupled to the memory card interface ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 14, Poisner discloses a method further comprising: issuing the memory write command to a device coupled to the memory card interface followed by issuing a memory read command to the device coupled to the memory card interface ('in response to the address being directed to configuration space, determine which of the following actions is associated with that particular address and perform that action' see para [0018]).

As to claim 15, Poisner discloses an article having a machine readable medium with instructions stored thereon (see para [0008]) that when accessed result in a mobile computing device: accessing a non-memory control function in a device coupled to a memory card interface (interface logic) of the mobile computing device by populating a data field of a memory card write command with a data pattern to identify the memory card write command as a command to be diverted for a purpose other than a memory write ('the data field may contain one or more bits indicating whether the command is a protected command,' see para [0047], para [0050]).

As to claim 16, Poisner discloses an article wherein the instructions, when accessed, further result in the mobile computing device populating the data field with a password to authenticate access to the device coupled to the memory card interface ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 17, Poisner discloses an article wherein the instructions, when accessed, further result in the mobile computing device populating the data field with a command index to specify a purpose other than a memory write ('For example, a command may set or clear a hardware flag, initiate a microcode sequence, or cause some other event to happen' see para [0053]).

As to claim 18, Poisner discloses a memory card compatible device (see para [0008]) comprising: a host interface to receive memory write commands ('interface logic' see para [0047]); non-memory controller component coupled to the host interface to interpret data included within the memory write commands as non-memory related commands ('it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space. If not, processing may proceed at block 315 in a manner labeled in FIG. 3A as "normal processing", which may be any processing not involving the configuration space' see para [0047]).

As to claim 19, Poisner discloses a memory card compatible device further comprising: non-volatile memory; a memory controller component coupled to the non-volatile memory; and a memory command routing component coupled to the host interface and the non-memory controller component, the memory command routing component including logic to determine whether to route a memory write command to the memory controller or the non-memory controller based on the data included within the memory write command ('placing predetermined data on the data lines' see para [0008], para [0010]).

As to claim 20, Poisner discloses a device comprising: a host interface compatible with a memory card interface of a mobile computing device ('computing devices', see Fig 1, para [0010], 'interface logic' see para [0047]); and a memory command routing component to interpret memory card write commands to determine whether the memory card write command should be diverted for a purpose other than a memory write based on at least a portion of the data to be written, wherein the memory command routing component is coupled to receive the memory card write command from the host interface ('After the command is detected by interface logic and the destination address of the command is decoded, it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space', 'the data field may contain one or more bits indicating whether the command is a protected command' see para [0047]-[0050]).

--(Continued in Supplemental Box)--

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V, 2. Citations and explanations:

As to claim 21, Poisner discloses a device further comprising: a memory controller component coupled to receive memory write commands from the memory command routing component (see para [0013]).

As to claim 22, Poisner discloses a device further comprising: a non-memory controller component coupled to receive diverted memory write commands from the memory command routing component ('Configuration "space" is a conceptual term that refers to the range(s) of addresses that are reserved for implementation in logic circuit 120 for various activities, with accesses that are targeted to any address within the configuration space being redirected to various portions of logic circuit 120 rather than to memory 140 or to input-output devices' see para [0011]).

As to claim 23, Poisner discloses a device comprising: a host interface compatible with a memory card interface of a mobile computing device (see para [0047]); and a memory command routing component to interpret memory card write commands to determine whether the memory card write command should be diverted for a purpose other than a memory write based on at least a portion of an address to be written, wherein the memory command routing component is coupled to receive the memory card write command from the host interface ('After the command is detected by interface logic and the destination address of the command is decoded, it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space', 'the address itself may be sufficient to indicate whether the command is a protected command' see para [0047]-[0050]).

As to claim 24, Poisner discloses a method comprising: receiving, at a non-memory control component in a memory card compatible device, an activation code in a data field of a memory write command ; comparing the activation code to a known value to detect a match ('Microcode that initiates a command over processor bus 130 may identify the command as a protected command in various ways, including but not limited to:.. placing predetermined data on the data lines' see para [0008], para [0010]); and if there is a match, requesting a password to be used in subsequent authentications to the non-memory control component in a memory card compatible device ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 25, Poisner discloses a method further comprising receiving non-memory related commands hidden in the data field of memory write commands, wherein the non- memory related commands include the password ('cryptographic keys' see para [0041], para [0048]-[0050]).

As to claim 26, Poisner discloses a method further comprising receiving a plurality of activation codes, wherein each of the plurality of activation codes corresponds to the activation of a different non-memory control component in the memory card compatible device (' The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data. In one embodiment, this entire space may be implemented as read-only registers that hold a single embedded key, but other embodiments may implement this space in other ways' see para [0041]).

Claims 1-26 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 115.019WO1	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2008/057588	International filing date *(day/month/year)* 20 March 2008 (20.03.2008)	Priority date *(day/month/year)* 30 March 2007 (30.03.2007)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant TYFONE, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 06 October 2009 (06.10.2009)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Nora Lindner e-mail: pt11.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
DANA LEMOINE
LEMOINE PATENT SERVICES
C/O INTELLEVATE
900 SECOND AVE SOUTH, SUITE 1700
MINNEAPOLIS, MN 55402

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	07 AUG 2008
Applicant's or agent's file reference 115.019WO1	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 08/57588	20 March 2008 (20.03.2008)	30 March 2007 (30.03.2007)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06F 12/00 (2008.04)
USPC - 711/103

Applicant TYFONE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	31 July 2008 (31.07.2008)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. type of material

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing

      ☐ contained in the international application as filed

      ☐ filed together with the international application in electronic form

      ☐ furnished subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	None	YES
	Claims	1-26	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-26	NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-26 lack novelty under PCT article 33(2) as being anticipated by US 2005/0022002 A1 to Poisner.

As to claim 1, Poisner discloses a method comprising: receiving a memory access command, the memory access command including an address field and a data field (see para [0050]); comparing at least a portion of the data field to a predetermined data value to determine if there is a match ('the data field may contain one or more bits indicating whether the command is a protected command' see para [0050]-[0051]); if there is not a match, performing a memory access according to the memory access command (' If not, the command is determined to be directed to non-protected configuration space, and processing continues in FIG. 3B at point "B" of the flow chart' see Fig 3B, para [0049]); and if there is a match, diverting the memory access command for further interpretation (' If the command is determined to be a protected command, processing may continue in FIG. 3B at point "A" of the flow chart' see Fig 3B, para [0051]).

As to claim 2, Poisner discloses a method further comprising comparing the address field with a predetermined address value to determine if there is an address match, and diverting the memory access command only when there is also an address match ('After the command is detected by interface logic and the destination address of the command is decoded, it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space' see Fig 3A, para [0047]).

As to claim 3, Poisner discloses a method wherein diverting the memory access command comprises passing at least some of the data field to a non-memory controller component for further interpretation (' Configuration "space" is a conceptual term that refers to the range(s) of addresses that are reserved for implementation in logic circuit 120 for various activities, with accesses that are targeted to any address within the configuration space being redirected to various portions of logic circuit 120 rather than to memory 140 or to input-output devices' see para [0011], para [0049]).

As to claim 4, Poisner discloses a method further comprising reading a password from the data field to authenticate access to the non-memory controller component ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 5, Poisner discloses an article having a machine readable medium with instructions stored thereon that when accessed result in a machine (see para [0008]): comparing data received with a memory write command to a predetermined data value to determine whether the memory write command should be interpreted as a memory write command or whether the memory write command should be interpreted as a command other than a memory write command ('Read or write commands to at least a portion of the addresses in the configuration space are redirected to configuration registers in logic circuit 120. In some embodiments, another portion of the addresses in the configuration space are used for commands that trigger some type of action within the logic circuit 120 rather than being used to store data in, or read data from, a register' see para [0011]).

As to claim 6, Poisner discloses an article wherein the instructions, when accessed, further result in the machine forwarding the memory write command to a memory controller component when the memory write command should be interpreted as a memory write command. (see para [0011]-[0013]).

As to claim 7, Poisner discloses an article wherein the instructions, when accessed, further result in the machine forwarding the memory write command to a non-memory controller component when the memory write command should be interpreted as a command other than a memory write command ('Configuration space may be implemented with addresses that would otherwise be part of memory address space or input-output (I/O) address space. Read or write commands to at least a portion of the addresses in the configuration space are redirected to configuration registers in logic circuit 120' see abstract, para [0010]-[0012]).

As to claim 8, Poisner discloses an article having a machine readable medium with instructions stored thereon (see para [0008]) that when accessed result in a machine: comparing an address field received with a memory write command to a predetermined address value to determine whether the memory write command should be interpreted as a memory write command or whether the memory write command should be interpreted as a command other than a memory write command ('the address itself may be sufficient to indicate whether the command is a protected command' see Fig 3A-3B, para [0049]-[0051]).

--(Continued in Supplemental Box)--

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Box V, 2. Citations and explanations:

As to claim 9, Poisner discloses a method comprising populating fields in a memory write command to be sent to a memory card interface (interface logic) by populating at least a first portion of a data field with a data pattern to identify the memory write command as a command to be diverted for purposes other than a memory write ('the data field may contain one or more bits indicating whether the command is a protected command,' see para [0047], para [0050]).

As to claim 10, Poisner discloses a method further comprising prior to populating the fields, receiving a copy of the data pattern from a device coupled to the memory card interface ('placing predetermined data on the data lines' see para [0010]).

As to claim 11, Poisner discloses a method further comprising populating an address field with an address value to further identify the memory write command as a command to be diverted for purposes other than a memory write ('placing a predetermined address on the address lines' see para [0010]).

As to claim 12, Poisner discloses a method further comprising populating a second portion of the data field with a command index to specify a purpose other than a memory write ('For example, a command may set or clear a hardware flag, initiate a microcode sequence, or cause some other event to happen' see para [0053]).

As to claim 13, Poisner discloses a method further comprising populating a second portion of the data field with a password to authenticate access to a device coupled to the memory card interface ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 14, Poisner discloses a method further comprising: issuing the memory write command to a device coupled to the memory card interface followed by issuing a memory read command to the device coupled to the memory card interface ('in response to the address being directed to configuration space, determine which of the following actions is associated with that particular address and perform that action' see para [0018]).

As to claim 15, Poisner discloses an article having a machine readable medium with instructions stored thereon (see para [0008]) that when accessed result in a mobile computing device: accessing a non-memory control function in a device coupled to a memory card interface (interface logic) of the mobile computing device by populating a data field of a memory card write command with a data pattern to identify the memory card write command as a command to be diverted for a purpose other than a memory write ('the data field may contain one or more bits indicating whether the command is a protected command,' see para [0047], para [0050]).

As to claim 16, Poisner discloses an article wherein the instructions, when accessed, further result in the mobile computing device populating the data field with a password to authenticate access to the device coupled to the memory card interface ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 17, Poisner discloses an article wherein the instructions, when accessed, further result in the mobile computing device populating the data field with a command index to specify a purpose other than a memory write ('For example, a command may set or clear a hardware flag, initiate a microcode sequence, or cause some other event to happen' see para [0053]).

As to claim 18, Poisner discloses a memory card compatible device (see para [0008]) comprising: a host interface to receive memory write commands ('interface logic' see para [0047]); non-memory controller component coupled to the host interface to interpret data included within the memory write commands as non-memory related commands ('it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space. If not, processing may proceed at block 315 in a manner labeled in FIG. 3A as "normal processing", which may be any processing not involving the configuration space' see para [0047]).

As to claim 19, Poisner discloses a memory card compatible device further comprising: non-volatile memory; a memory controller component coupled to the non-volatile memory; and a memory command routing component coupled to the host interface and the non-memory controller component, the memory command routing component including logic to determine whether to route a memory write command to the memory controller or the non-memory controller based on the data included within the memory write command ('placing predetermined data on the data lines' see para [0008], para [0010]).

As to claim 20, Poisner discloses a device comprising: a host interface compatible with a memory card interface of a mobile computing device ('computing devices', see Fig 1, para [0010], 'interface logic' see para [0047]); and a memory command routing component to interpret memory card write commands to determine whether the memory card write command should be diverted for a purpose other than a memory write based on at least a portion of the data to be written, wherein the memory command routing component is coupled to receive the memory card write command from the host interface ('After the command is detected by interface logic and the destination address of the command is decoded, it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space', 'the data field may contain one or more bits indicating whether the command is a protected command' see para [0047]-[0050]).

--(Continued in Supplemental Box)--

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 08/57588

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V, 2. Citations and explanations:

As to claim 21, Poisner discloses a device further comprising: a memory controller component coupled to receive memory write commands from the memory command routing component (see para [0013]).

As to claim 22, Poisner discloses a device further comprising: a non-memory controller component coupled to receive diverted memory write commands from the memory command routing component ('Configuration "space" is a conceptual term that refers to the range(s) of addresses that are reserved for implementation in logic circuit 120 for various activities, with accesses that are targeted to any address within the configuration space being redirected to various portions of logic circuit 120 rather than to memory 140 or to input-output devices' see para [0011]).

As to claim 23, Poisner discloses a device comprising: a host interface compatible with a memory card interface of a mobile computing device (see para [0047]); and a memory command routing component to interpret memory card write commands to determine whether the memory card write command should be diverted for a purpose other than a memory write based on at least a portion of an address to be written, wherein the memory command routing component is coupled to receive the memory card write command from the host interface ('After the command is detected by interface logic and the destination address of the command is decoded, it may be determined at block 310 whether the destination address is in a range of addresses designated as the configuration space', 'the address itself may be sufficient to indicate whether the command is a protected command' see para [0047]-[0050]).

As to claim 24, Poisner discloses a method comprising: receiving, at a non-memory control component in a memory card compatible device, an activation code in a data field of a memory write command ; comparing the activation code to a known value to detect a match ('Microcode that initiates a command over processor bus 130 may identify the command as a protected command in various ways, including but not limited to:.. placing predetermined data on the data lines' see para [0008], para [0010]); and if there is a match, requesting a password to be used in subsequent authentications to the non-memory control component in a memory card compatible device ('The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data' see para [0041]).

As to claim 25, Poisner discloses a method further comprising receiving non-memory related commands hidden in the data field of memory write commands, wherein the non- memory related commands include the password ('cryptographic keys' see para [0041], para [0048]-[0050]).

As to claim 26, Poisner discloses a method further comprising receiving a plurality of activation codes, wherein each of the plurality of activation codes corresponds to the activation of a different non-memory control component in the memory card compatible device (' The fifth, sixth, and seventh blocks (0400-06FF) may be used to hold one or more cryptographic keys, which may be used during protected processing for encrypting, decrypting, and/or validating data. In one embodiment, this entire space may be implemented as read-only registers that hold a single embedded key, but other embodiments may implement this space in other ways' see para [0041]).

Claims 1-26 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: DANA LEMOINE
LEMOINE PATENT SERVICES, PLLC
C/O CPA GLOBAL
P.O. BOX 52050
MINNEAPOLIS, MN 55402

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing *(day/month/year)*	15 APR 2010
Applicant's or agent's file reference 115024WO1	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2010/025014	International filing date *(day/month/year)* 23 February 2010
Applicant TYFONE, INC.	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver Telephone No. 571-272-7774

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 115024WO1	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2010/025014	International filing date *(day/month/year)* 23 February 2010	(Earliest) Priority Date *(day/month/year)* 24 February 2009
Applicant TYPONE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

   ☒ the text is approved as submitted by the applicant.

   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

   ☒ the text is approved as submitted by the applicant.

   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

   a. the figure of the **drawings** to be published with the abstract is Figure No. 4

   ☐ as suggested by the applicant.

   ☒ as selected by this Authority, because the applicant failed to suggest a figure.

   ☐ as selected by this Authority, because this figure better characterizes the invention.

   b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2010/025014

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06K 19/077 (2010.01)
USPC - 257/679
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(8) - B42D 15/00; G06K 19/07, 19/077 (2010.01)
USPC - 235/380, 488, 492; 257/531, 679; 361/737

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)
PatBase; Google Patents

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/0168339 A1 (ARAI et al) 04 August 2005 (04.08.2005) entire document	1-23
A	US 2001/0002035 A1 (KAYANAKIS) 31 May 2001 (31.05.2001) entire document	1-23
A	US 6,588,660 B1 (BUESCHER et al) 08 July 2003 (08.07.2003) entire document	1-23
A	US 2007/0257797 A1 (RANCIEN et al) 08 November 2007 (08.11.2007) entire document	1-23

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 April 2010	15 APR 2010

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: DANA LEMOINE
LEMOINE PATENT SERVICES, PLLC
C/O CPA GLOBAL
P.O. BOX 52050
MINNEAPOLIS, MN 55402

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	15 APR 2010
Applicant's or agent's file reference 115024WO1	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2010/025014	23 February 2010	24 February 2009

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06K 19/077 (2010.01)
USPC - 257/679

Applicant TYFONE, INC.

1. This opinion contains indications relating to the following items:

- [X] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [X] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	04 April 2010	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2009)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2010/025014

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2010/025014

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	8-23	YES
	Claims	1-7	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-23	NO
Industrial applicability (IA)	Claims	1-23	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-7 lack novelty under PCT Article 33(2) as being anticipated by Arai et al. (hereafter Arai).

Referring to claim 1, Arai discloses an inductive element (Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna) comprising: a bottom surface (10); and a plurality of layers (11, 15, 16, 24; Figs. 1A-3B) substantially parallel to the bottom surface (Figs. 1A-3B), the plurality of layers including a combination of electrically conductive material (18, 22 and 56 are all conductive) and electrically insulating material (27, 55 and 58 are all insulating) such that when bonded together the plurality of layers form at least one conductive coil (11, 13) having a field coupling surface area substantially perpendicular to the bottom surface (Paras. [0082] and [0088]; Figs. 1A-3B).

Referring to claim 2, Arai discloses the inductive element of claim 1, further comprising bonding areas on the bottom surface (Para. [0086]).

Referring to claim 3, Arai discloses the inductive element of claim 1, further wherein the plurality of layers include magnetic material forming a magnetic core within the at least one conductive coil (Para. [0088] – In the present embodiment mode, the antenna structure using an electromagnetic induction type is employed. However, any of an electromagnetic coupling type using mutual induction of a coil due to an AC magnetic field).

Referring to claim 4, Arai discloses a multilayer inductive coupling element (Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna) comprising: a lower layer (11) having at least one conductive surface trace with trace ends (12; Paras. [0073] and [0074]); at least one intermediate layer having conductive through-traces (21) at locations to electrically contact the trace ends on the lower layer (Figs. 4A-7C); and an upper layer having at least one conductive surface trace (21b) aligned to electrically contact the conductive through-traces (21c) to form a conductive coil (11, 12 and 13) having at least one turn (Figs. 1A-3B).

Referring to claim 5, Arai discloses the multilayer inductive coupling element of claim 4, further wherein the at least one intermediate layer (28) comprises magnetic material (Cl. 14 – filler is nickel, which is magnetic) positioned between the through traces (Fig. 2B).

Referring to claim 6, Arai discloses the multilayer inductive coupling element of claim 4, further wherein the lower layer (11) includes magnetic material (Cl. 12 – antenna is Ni, Fe or Co, all of which are magnetic; Cl. 14 – filler is nickel, which is magnetic) positioned beyond the trace ends (12; Fig. 2B).

Referring to claim 7, Arai discloses the multilayer inductive coupling element of claim 4, further comprising a bottom layer (28) beneath the lower layer (11; Fig. 2B), the bottom layer including magnetic material (Cl. 14 – filler is nickel, which is magnetic) to be positioned beneath the at least one conductive trace (12) in the lower layer (Fig. 2B).

Claims 8-23 lack an inventive step under PCT Article 33(3) as being obvious over Arai et al. (hereafter Arai).

Referring to claim 8, Arai discloses an electronic device comprising: a circuit board (Para. [0016]); a contactless communications device affixed to the circuit board (Para. [0008]), the contactless communications device having an antenna port (11, 12); and an inductive element affixed to the circuit board and electrically coupled to the antenna port, the inductive element having a conductive coil with a field coupling surface area substantially perpendicular to the circuit board (Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna), but fails to explicitly disclose of the circuit board comprising a memory card slot interface. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, since the separating of parts which were once integral involves only routine skill in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 9, Arai discloses the electronic device of claim 8, further wherein the inductive element comprises a multilayer surface-mount inductor (11, 12 and 13; Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna; Figs. 1A-9B).

Referring to claim 10, Arai discloses the electronic device of claim 9, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially parallel to the circuit board (Figs. 1A-3B).

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Referring to claim 11, Arai discloses the electronic device of claim 9, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially perpendicular to the circuit board (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10).

Referring to claims 12-14, Arai discloses the electronic device of claim 8, but fails to explicitly disclose [Cl. 12] wherein the memory card slot interface comprises a Secure Digital (SD) compatible interface; [Cl. 13] wherein the memory card slot interface comprises a micro Secure Digital (SD) compatible interface; or [Cl. 14] wherein the memory card slot interface comprises a mini Secure Digital (SD) compatible interface. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, and [Cl. 12] wherein the memory card slot interface comprises a Secure Digital (SD) compatible interface; [Cl. 13] wherein the memory card slot interface comprises a micro Secure Digital (SD) compatible interface; or [Cl. 14] wherein the memory card slot interface comprises a mini Secure Digital (SD) compatible interface, since the separating of parts which were once integral involves only routine skill in the art, and since Secure Digital (SD), micro Secure Digital (SD), and mini Secure Digital (SD) compatible interfaces are well-known in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 15, Arai discloses an apparatus comprising: a substrate having at least one surface (10), an inner edge (right edge of 10 in Fig. 2B), and an outer edge opposite (left edge of 10 in Fig. 2B) the inner edge; electrical contacts (11, 12) on the at least one surface (surface of 10) and situated along the inner edge (Figs. 1A-6B); and a conductive coil (11, 12 and 13) situated along the outer edge (Figs. 1A-6B), the conductive coil having a field coupling surface area substantially perpendicular to the at least one surface (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10), but fails to explicitly disclose of said substrate comprising a memory card compatible substrate. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, since the separating of parts which were once integral involves only routine skill in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 16, Arai discloses the apparatus of claim 15 wherein: the at least one surface includes a top surface (surface of 10 facing 28 in Fig. 2B) and a bottom surface (surface of 10 visible in Fig. 2B) substantially parallel to each other; and the electrical contacts (11, 12) are on the top surface, and the conductive coil (11, 12 and 13) is on the top surface (Fig. 6A).

Referring to claim 17, Arai discloses the apparatus of claim 15 wherein: the at least one surface includes a top surface (surface of 10 visible in 2B) and a bottom surface (surface of 10 facing 28 in Fig. 2B) substantially parallel to each other; and the electrical contacts (11) are on the top surface, and the conductive coil (11, 12 and 13) is on the bottom surface (Fig. 5B).

Referring to claim 18, Arai discloses the apparatus of claim 15 wherein the conductive coil comprises a multilayer surface-mount inductor (11, 12 and 13; Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna; Figs. 1A-9B).

Referring to claim 19, Arai discloses the apparatus of claim 18, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially parallel to the circuit board (Figs. 1A-3B).

Referring to claim 20, Arai discloses the apparatus of claim 18, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially perpendicular to the circuit board (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10).

Referring to claim 21, Arai discloses an apparatus comprising: a substrate having at least one surface (10), an inner edge (right edge of 10 in Fig. 2B), and an outer edge opposite (left edge of 10 in Fig. 2B) the inner edge; electrical contacts (11, 12) on the at least one surface (surface of 10) and situated along the inner edge (Figs. 1A-6B); and a three dimensional conductive coil (11, 12 and 13) situated along the outer edge (Figs. 1A-6B), but fails to explicitly disclose of said substrate comprising a memory card compatible substrate. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, since the separating of parts which were once integral involves only routine skill in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 22, Arai discloses the apparatus of claim 21, but fails to explicitly disclose wherein the apparatus has a micro secure digital (microSD) form factor. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, and wherein the apparatus has a micro secure digital (microSD) form factor, since the separating of parts which were once integral involves only routine skill in the art, and since micro Secure Digital (SD) compatible interfaces are well-known in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 23, Arai discloses the apparatus of claim 22, further wherein the three dimensional conductive coil (11, 12 and 13) has a field coupling surface area substantially perpendicular to the at least one surface of the memory card (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10; Para. [0002] regarding functions as a memory and includes card).

Claims 1-23 meet the criteria set out in PCT Article 33(4) and thus have industrial applicability because the subject matter claimed can be made or used in industry.

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Annex B).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, International Phase, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet or sheets containing a complete set of claims in replacement of all the claims previously filed must be submitted.

Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively in Arabic numerals (Section 205(a)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

IPR2025-00645 Page 01350

SEQUENCE LISTINGS AND TABLES RELATED THERETO IN INTERNATIONAL APPLICATIONS FILED IN THE U.S. RECEIVING OFFICE

The Administrative Instructions (AIs) under the Patent Cooperation Treaty (PCT), in force as of **July 1, 2009**, contain important changes relating to the manner of filing, and applicable fees for, sequence listings and/or tables related thereto (sequence-related tables) in international applications. The complete text may be accessed at http://www.wipo.int/pct/en/texts/index.htm.

Effective July 1, 2009, Part 8 and Annex C-*bis* will no longer form part of the AIs. Part 8 was introduced in 2001 as a temporary solution to problems arising from the filing of very large sequence listings on paper and provided for a *sequence listing forming part of the international application* to be filed in electronic form on physical medium (*e.g.*, CD), together with the remainder of the application on paper. In 2002, Part 8 was expanded to include sequence-related tables and Annex C-*bis* was added to provide technical requirements. All applicants may now file complete international applications in electronic form, eliminating the need for these temporary provisions.

I. AIS PART 8 AND ANNEX C-*BIS DELETED AS OF JULY 1, 2009*

A) **Sequence-related tables cannot be filed as a separate part of the description or in text format.** They must be provided as an integral part of the international application either:
- in PDF format as part of an international application filed in electronic form via EFS-Web; or
- on paper as part of an international application filed on paper.

B) **A *sequence listing forming part of an international application*** may be provided either:
- in electronic form, as part of an international application filed in electronic form via EFS-Web, in
  - Annex C/ST.25 text format (preferred), or
  - PDF format; or
- on paper as part of an international application filed on paper.

C) **A *sequence listing not forming part of the international application* (for search under PCT Rule 13*ter*) in Annex C/ST.25 text format**
- is not required where the *sequence listing forming part of the international application* was filed in Annex C/ST.25 text format as part of an international application filed in electronic form via EFS-Web
- is required for search where the *sequence listing forming part of the international application* was filed in PDF
- is required for search on physical medium (*e.g.*, CD) where the *sequence listing forming part of the international application* was filed on paper as part of an international application filed on paper.

II. CALCULATION OF THE INTERNATIONAL FILING FEE AND FEE REDUCTION UNDER AI § 707

A) **A sequence-related table** must form an integral part of the international application and will incur FULL page fees with no upper limit.

B) **A *sequence listing forming part of an international application*** filed:
- via EFS-Web in Annex C/ST.25 text format will incur NO page fees;
- on paper or in PDF format will incur FULL page fees with no upper limit.

III. AVAILABILITY OF SEQUENCE LISTINGS SUBMITTED FOR SEARCH UNDER PCT RULE *13TER*

International Searching Authorities will be required to transmit to the International Bureau a copy of an Annex C/ST.25 text format sequence listing provided for search under PCT Rule 13*ter*. Any such sequence listing will be made available on PATENTSCOPE® (*sequence listings forming part of the international application* are already available).

IV. JULY 2009 REQUEST (PCT/RO/101)

The Request now has two options for the last sheet: one for paper filings; and one for EFS-Web filings. The July 2009 Request may be accessed at http://www.wipo.int/pct/en/forms/index.htm.

PATENT COOPERATION TREATY

ADVANCE E-MAIL

PCT

From the INTERNATIONAL BUREAU

NOTIFICATION CONCERNING TRANSMITTAL OF COPY OF INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (CHAPTER I OF THE PATENT COOPERATION TREATY)
(PCT Rule 44bis.1(c))

To:

LEMOINE, Dana B.
LeMoine Patent Services, PLLC
c/o CPA Global
P.O. Box 52050
Minneapolis, Minnesota 55402
ETATS-UNIS D'AMERIQUE

80499.030W01

Date of mailing *(day/month/year)*	
09 September 2011 (09.09.2011)	
Applicant's or agent's file reference: 115024WO1	IMPORTANT NOTICE

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2010/025014	23 February 2010 (23.02.2010)	24 February 2009 (24.02.2009)

Applicant: TYFONE, INC. et al

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

CPA GLOBAL
SEP 20 2011
RECEIVED
Coded _____ Verified _____

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Lingfei Bai

e-mail: pt02.pct@wipo.int

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 115024WO1	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2010/025014	International filing date *(day/month/year)* 23 February 2010 (23.02.2010)	Priority date *(day/month/year)* 24 February 2009 (24.02.2009)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant TYFONE, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 30 August 2011 (30.08.2011)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Lingfei Bai e-mail: pt02.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: DANA LEMOINE
LEMOINE PATENT SERVICES, PLLC
C/O CPA GLOBAL
P.O. BOX 52050
MINNEAPOLIS, MN 55402

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	15 APR 2010
Applicant's or agent's file reference 115024WO1	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2010/025014	23 February 2010	24 February 2009

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06K 19/077 (2010.01)
USPC - 257/679

Applicant TYFONE, INC.

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	04 April 2010	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2009)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2010/025014

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2010/025014

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	8-23	YES
	Claims	1-7	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-23	NO
Industrial applicability (IA)	Claims	1-23	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-7 lack novelty under PCT Article 33(2) as being anticipated by Arai et al. (hereafter Arai).

Referring to claim 1, Arai discloses an inductive element (Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna) comprising: a bottom surface (10); and a plurality of layers (11, 15, 16, 24; Figs. 1A-3B) substantially parallel to the bottom surface (Figs. 1A-3B), the plurality of layers including a combination of electrically conductive material (18, 22 and 56 are all conductive) and electrically insulating material (27, 55 and 58 are all insulating) such that when bonded together the plurality of layers form at least one conductive coil (11, 13) having a field coupling surface area substantially perpendicular to the bottom surface (Paras. [0082] and [0088]; Figs. 1A-3B).

Referring to claim 2, Arai discloses the inductive element of claim 1, further comprising bonding areas on the bottom surface (Para. [0086]).

Referring to claim 3, Arai discloses the inductive element of claim 1, further wherein the plurality of layers include magnetic material forming a magnetic core within the at least one conductive coil (Para. [0088] – In the present embodiment mode, the antenna structure using an electromagnetic induction type is employed. However, any of an electromagnetic coupling type using mutual induction of a coil due to an AC magnetic field).

Referring to claim 4, Arai discloses a multilayer inductive coupling element (Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna) comprising: a lower layer (11) having at least one conductive surface trace with trace ends (12; Paras. [0073] and [0074]); at least one intermediate layer having conductive through-traces (21) at locations to electrically contact the trace ends on the lower layer (Figs. 4A-7C); and an upper layer having at least one conductive surface trace (21b) aligned to electrically contact the conductive through-traces (21c) to form a conductive coil (11, 12 and 13) having at least one turn (Figs. 1A-3B).

Referring to claim 5, Arai discloses the multilayer inductive coupling element of claim 4, further wherein the at least one intermediate layer (28) comprises magnetic material (Cl. 14 – filler is nickel, which is magnetic) positioned between the through traces (Fig. 2B).

Referring to claim 6, Arai discloses the multilayer inductive coupling element of claim 4, further wherein the lower layer (11) includes magnetic material (Cl. 12 – antenna is Ni, Fe or Co, all of which are magnetic; Cl. 14 – filler is nickel, which is magnetic) positioned beyond the trace ends (12; Fig. 2B).

Referring to claim 7, Arai discloses the multilayer inductive coupling element of claim 4, further comprising a bottom layer (28) beneath the lower layer (11; Fig. 2B), the bottom layer including magnetic material (Cl. 14 – filler is nickel, which is magnetic) to be positioned beneath the at least one conductive trace (12) in the lower layer (Fig. 2B).

Claims 8-23 lack an inventive step under PCT Article 33(3) as being obvious over Arai et al. (hereafter Arai).

Referring to claim 8, Arai discloses an electronic device comprising: a circuit board (Para. [0016]); a contactless communications device affixed to the circuit board (Para. [0008]), the contactless communications device having an antenna port (11, 12); and an inductive element affixed to the circuit board and electrically coupled to the antenna port, the inductive element having a conductive coil with a field coupling surface area substantially perpendicular to the circuit board (Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna), but fails to explicitly disclose of the circuit board comprising a memory card slot interface. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, since the separating of parts which were once integral involves only routine skill in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 9, Arai discloses the electronic device of claim 8, further wherein the inductive element comprises a multilayer surface-mount inductor (11, 12 and 13; Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna; Figs. 1A-9B).

Referring to claim 10, Arai discloses the electronic device of claim 9, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially parallel to the circuit board (Figs. 1A-3B).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2010/025014

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Referring to claim 11, Arai discloses the electronic device of claim 9, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially perpendicular to the circuit board (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10).

Referring to claims 12-14, Arai discloses the electronic device of claim 8, but fails to explicitly disclose [Cl. 12] wherein the memory card slot interface comprises a Secure Digital (SD) compatible interface; [Cl. 13] wherein the memory card slot interface comprises a micro Secure Digital (SD) compatible interface; or [Cl. 14] wherein the memory card slot interface comprises a mini Secure Digital (SD) compatible interface. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, and [Cl. 12] wherein the memory card slot interface comprises a Secure Digital (SD) compatible interface; [Cl. 13] wherein the memory card slot interface comprises a micro Secure Digital (SD) compatible interface; or [Cl. 14] wherein the memory card slot interface comprises a mini Secure Digital (SD) compatible interface, since the separating of parts which were once integral involves only routine skill in the art, and since Secure Digital (SD), micro Secure Digital (SD), and mini Secure Digital (SD) compatible interfaces are well-known in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 15, Arai discloses an apparatus comprising: a substrate having at least one surface (10), an inner edge (right edge of 10 in Fig. 2B), and an outer edge opposite (left edge of 10 in Fig. 2B) the inner edge; electrical contacts (11, 12) on the at least one surface (surface of 10) and situated along the inner edge (Figs. 1A-6B); and a conductive coil (11, 12 and 13) situated along the outer edge (Figs. 1A-6B), the conductive coil having a field coupling surface area substantially perpendicular to the at least one surface (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10), but fails to explicitly disclose of said substrate comprising a memory card compatible substrate. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, since the separating of parts which were once integral involves only routine skill in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 16, Arai discloses the apparatus of claim 15 wherein: the at least one surface includes a top surface (surface of 10 facing 28 in Fig. 2B) and a bottom surface (surface of 10 visible in Fig. 2B) substantially parallel to each other; and the electrical contacts (11, 12) are on the top surface, and the conductive coil (11, 12 and 13) is on the top surface (Fig. 6A).

Referring to claim 17, Arai discloses the apparatus of claim 15 wherein: the at least one surface includes a top surface (surface of 10 visible in 2B) and a bottom surface (surface of 10 facing 28 in Fig. 2B) substantially parallel to each other; and the electrical contacts (11) are on the top surface, and the conductive coil (11, 12 and 13) is on the bottom surface (Fig. 5B).

Referring to claim 18, Arai discloses the apparatus of claim 15 wherein the conductive coil comprises a multilayer surface-mount inductor (11, 12 and 13; Para. [0082] - electromagnetic induction type and a non-contact type ID label using a coiled antenna; Figs. 1A-9B).

Referring to claim 19, Arai discloses the apparatus of claim 18, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially parallel to the circuit board (Figs. 1A-3B).

Referring to claim 20, Arai discloses the apparatus of claim 18, further wherein the multilayer surface-mount inductor (11, 12 and 13) is formed with layers substantially perpendicular to the circuit board (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10).

Referring to claim 21, Arai discloses an apparatus comprising: a substrate having at least one surface (10), an inner edge (right edge of 10 in Fig. 2B), and an outer edge opposite (left edge of 10 in Fig. 2B) the inner edge; electrical contacts (11, 12) on the at least one surface (surface of 10) and situated along the inner edge (Figs. 1A-6B); and a three dimensional conductive coil (11, 12 and 13) situated along the outer edge (Figs. 1A-6B), but fails to explicitly disclose of said substrate comprising a memory card compatible substrate. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, since the separating of parts which were once integral involves only routine skill in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 22, Arai discloses the apparatus of claim 21, but fails to explicitly disclose wherein the apparatus has a micro secure digital (microSD) form factor. Arai does, however, teach that the circuit board comprises a memory (Para. [0002]). Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to provide a memory card slot interface on the circuit board of Arai, and wherein the apparatus has a micro secure digital (microSD) form factor, since the separating of parts which were once integral involves only routine skill in the art, and since micro Secure Digital (SD) compatible interfaces are well-known in the art. The motivation being to allow the user the ability to separate the memory from the device for security and/or use in other applications.

Referring to claim 23, Arai discloses the apparatus of claim 22, further wherein the three dimensional conductive coil (11, 12 and 13) has a field coupling surface area substantially perpendicular to the at least one surface of the memory card (Figs. 4A-7C, where 11, 12 and 13 extend perpendicularly from 10; Para. [0002] regarding functions as a memory and includes card).

Claims 1-23 meet the criteria set out in PCT Article 33(4) and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Filer:	Dana B. LeMoine/Theresa LeMoine
Attorney Docket Number:	115.001US9.10

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1720**

MOBILE PHONE WITH MAGNETIC CARD EMULATION

Field

The present invention relates generally to electronic devices, and more specifically to electronic devices that may perform transactions.

Background

Magnetic cards have many purposes. Examples include credit cards, debit cards, stored value cards, identification cards, access entry cards, and the like. Many of these cards have information stored in a magnetic stripe in a static manner. For example, a credit card may have a credit card number, a cardholder's name, and an issuing bank's name statically encoded in a magnetic strip. Likewise, an identification card or access entry card may have statically encoded information that identifies an individual or allows access to a controlled access area. When the card is swiped through a magnetic card reader, the information is transferred to the magnetic card reader to perform a transaction, such as a financial transaction or identification transaction.

Brief Description of the Drawings

Figures 1, 2A, and 2B show intelligent electronic devices and electronic transaction cards;

Figure 3 shows a block diagram of an electronic transaction card;

Figure 4 shows an electronic transaction card in a magnetic card reader;

Figure 5 shows an intelligent electronic device and card in a card reader;

Figures 6-8 show adapters for use with electronic transaction cards;

Figures 9 and 10 show an electronic transaction card having a smartcard interface;

Figure 11 shows an adapter in combination with an electronic transaction card;

Figure 12 shows an adapter having an aperture to receive an electronic transaction card;

Figure 13 shows another adapter embodiment;

Figure 14 shows an electronic transaction card;

Figure 15 shows an electronic transaction card and adapter combination;

Figure 16 shows an example swallow-type card reader;

Figure 17 shows a combination electronic transaction card and adapter being swiped through a magnetic card reader;

Figure 18 shows a financial transaction card;

Figure 19 shows a memory card;

Figure 20 shows a block diagram of a combination memory card and electronic transaction card;

Figure 21 shows a diagram of how a card may be utilized;

Figure 22 shows a block diagram of a combination memory card and electronic transaction card; and

Figure 23 shows a block diagram of a phone and a card.

Description of Embodiments

In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the

appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

Figure 1 shows an intelligent electronic device and an electronic transaction card. Intelligent electronic device 102 is shown as a mobile phone in Figure 1, but this is not a limitation of the present invention. For example, intelligent electronic device 102 may be a personal digital assistant (PDA), a smartphone, a mobile phone, a handheld computer, or any other device capable of operating as described herein.

Intelligent electronic device 102 includes add-on slot 110. Add-on slot 110 is a slot capable of accepting electronic transaction card 104. For example, add-on slot 110 may have physical dimensions compatible with electronic transaction card 104, and may have a communications interface that operates using a protocol compatible with electronic transaction card 104. In some embodiments, electronic transaction card 104 includes an identification number that provides a relationship to intelligent electronic device 102. For example, electronic transaction card 104 may include an ID number that provides a unique pairing relationship or a non-unique pairing relationship between electronic transaction card 104 and intelligent electronic device 102.

In some embodiments of the present invention, add-on slot 110 is a memory card slot designed to accept and communicate with memory cards. As used herein, the term "memory card slot" refers to any add-on slot capable of accepting a card having memory accessible by an intelligent electronic device such as that shown in Figure 1. For example, a memory card slot may be a proprietary card slot designed to accept memory cards that adhere to a proprietary communications protocol. Also for example, a memory card slot may be compatible with an industry standard communications protocol, or may be compatible with a widely accepted communications protocol that is not necessarily formally documented as an industry standard. Examples include slots that are compatible with the Multimedia Memory Card (MMC) protocol, Memory Stick DUO protocol, secure digital (SD) protocol,

and Smart Media protocol. The foregoing list is meant to be exemplary, and not exhaustive. Add-on slot 110 may be compatible with many memory card slot protocols other than those explicitly listed above without departing from the scope of the invention.

Electronic transaction card 104 includes electrical contacts 108 and stripe 106. Electrical contacts 108 are contacts that provide a communications interface to communicate with add-on slot 110. For example, electrical contacts 108 may provide connectivity compliant with a communications protocol for memory cards.

Stripe 106 represents an area on an external face of electronic transaction card 104 at which one ore more time-varying magnetic fields emanate. For example, one or more time-varying magnetic fields may emanate from the location of stripe 106 to communicate with a magnetic card reader. In some embodiments, the time-varying magnetic field may emulate the time-varying magnetic field produced when a typical magnetic card is swiped through a magnetic card reader. For example, a time-varying magnetic field produced at stripe 106 may emulate the swipe of a credit card, a debit card, or any other card having a magnetic stripe compatible with a magnetic card reader.

In some embodiments of the present invention, stripe 106 may be a visible stripe on electronic transaction card 104. When stripe 106 is visible, it may be used to indicate the location at which the time-varying magnetic field will emanate. In other embodiments of the present invention, stripe 106 may not be visible. For example, circuitry may be included within electronic transaction card 106 to produce the time-varying magnetic field and no visible indication may be present on an external face of electronic transaction card 104.

As used herein, the term "stripe" generally refers to a location on an electronic transaction card, whether a visible stripe exists or not. In this description, the term "stripe" may also be used to refer to a visible marking on a face of an electronic transaction card. Further, a "stripe" may include the functionality provided by one or more time-varying magnetic fields that emanate from the card.

For example, the term "stripe" may refer to multiple magnetic tracks, or multiple "stripes," or emulation thereof.

Stripes, as described herein, may be compatible with one or more standards. A stripe may be compatible with a standard by being in compliance with the standard or by being partially in compliance with the standard. For example, stripe 106 may be compatible with an American National Standards Institute (ANSI) magnetic stripe standard, or an International Organization for Standardization (ISO) magnetic stripe standard. In addition, in some embodiments, a stripe may emulate more than one magnetic track, and the emulated tracks may or may not be offset from the location specified in a standard. For example, one or more wires may be utilized to generate time-varying magnetic fields compatible with a standard, and the wires may be located at or near stripe 106 in a location different than the magnetic track offset described in an associated standard.

As used herein, the term "transaction" refers to any beneficial use of an electronic transaction card. For example, any time stripe 106 emits a time-varying magnetic field to be read by a magnetic card reader or a hybrid smartcard reader, a transaction may take place. Transactions may include financial transactions, access control transactions, or any other type of transaction involving any of the electronic transaction card embodiments described herein. Further, as described in more detail below, in some embodiments of the present invention, transactions may utilize smartcard interfaces on electronic transaction cards in addition to, or in lieu of, stripes that emit time-varying magnetic fields.

In operation, intelligent electronic device 102 may program electronic transaction card 104 for use in a transaction involving stripe 106. For example, intelligent electronic device 102 may program electronic transaction card 104 to operate as a credit card, a debit card, or the like. Electronic transaction card 104 may then be used with a magnetic stripe or smartcard based merchant point-of-sale terminal to effect a transaction. Also for example, intelligent electronic device 102 may program electronic transaction card 104 to operate in any other environment where stripe 106 may be beneficially utilized with a magnetic card reader.

Figure 2A shows intelligent electronic device 202 and electronic transaction card 220. Intelligent electronic device 202 includes add-on slot 210 to receive electronic transaction card 220. Intelligent electronic device 202 is shown having add-on slot on one side, but this is not a limitation of the present invention. For example, add-on slot 210 may be located on top, bottom, or any other surface of intelligent electronic device 202. Also for example, an add-on slot may be created by a clamshell design when the shell is closed. In these embodiments, each side of the clamshell may incorporate a portion of the add-on slot such that the add-on slot is "open" when the clamshell is open.

Electronic transaction card 220 may have any form factor compliant with add-on slot 210. Electronic transaction card 220 is shown having a form factor with an aspect ratio different from that of electronic transaction card 104 (Figure 1). Electronic transaction card 220 includes stripe 222 and may have electrical contacts to interface with add-on slot 210. The electrical contacts may be on the back side of electronic transaction card 220, recessed on an edge of electronic transaction card 220, or on the front side of electronic transaction card 220. In some embodiments, electronic transaction card 220 includes a "contactless" interface to add-on slot 210. For example, electronic transaction card 220 may include an interface to add-on slot 210 that communicates using electric or magnetic fields, infrared (IR) light, or any other suitable communications mechanism.

Electronic transaction card 220 may have an area for imprinting. For example, as shown in Figure 2A, electronic transaction card 220 may have space for imprinting a brand (for a bank or otherwise), and a cardholder's name. Further, electronic transaction card 220 may include space for a cardholder's signature. Electronic transaction card 220 may include any other information, coded or unencoded, visible or nonvisible, without departing from the scope of the present invention.

Intelligent electronic device 202 may include a mechanism to allow intelligent electronic device 202 to communicate with a wired or wireless network. For example, intelligent electronic device 202 may include circuitry to communicate

with a cellular phone network. Note that in these embodiments, intelligent electronic device 202 may or may not be a phone. For example, intelligent electronic device 202 may be a cellular telephone with an add-on slot for use with an electronic transaction card. Also for example, intelligent electronic device may be a non-telephonic device that has cellular network connectivity. Examples include personal digital assistants, and handheld devices dedicated to the use of electronic transaction cards. Further, intelligent electronic device 202 may be a non-telephonic device having wired or wireless connectivity to a network other than a cellular network, and in some embodiments, intelligent electronic device 202 may be a device without network connectivity. Examples include, but are not limited to: Blackberry devices available from Research in Motion (RIM), music players such as MP3 players, cameras, and the like.

In operation, intelligent electronic device 202 may program electronic transaction card to perform a transaction. In some embodiments, communications over a network may play a role in the transaction. For example, intelligent electronic device 202 may receive authorization for the transaction over a network. Also for example, intelligent electronic device 202 may program electronic transaction card 220 to perform a transaction, and then report the transaction to an entity using the network.

Electronic transaction card 220 may be utilized in financial transactions. For example, electronic transaction card 220 may be programmed to operate as a credit card or a stored value card. In these embodiments, electronic transaction card 220 may be programmed to emit one or more time-varying magnetic fields to emulate the swiping of a credit card or stored value card. In some of these embodiments, electronic transaction card 220 may use one number repeatedly, or may use a different number for each transaction. For example, electronic transaction card 220 may be programmed to have one number, similar to how a credit card uses the same number repeatedly. Also for example, electronic transaction card 220 may be programmed to use a different number for each transaction. These numbers are referred to herein as "single transaction account numbers" or "STANs."

Single transaction account numbers may be generated by the card issuer or locally by either an intelligent electronic device or an electronic transaction card. Generation of STANs may be accomplished in any of several ways. For example, when an electronic transaction card is issued, the cardholder may receive several pre-assigned single-use transaction numbers. The numbers may also have a pre-specified sequence. In some embodiments, this sequence may be known only to the issuing bank and the cardholder's intelligent electronic device and/or electronic transaction card. A card issuing bank may authorize payments based on the expected sequence of account numbers, and if out-of-sequence account numbers are used, then the issuing bank may consider that transaction as a potentially fraudulent transaction. The issuing bank may also use this feature to track the merchant involved in the potentially fraudulent transaction.

According to another example, a pre-assigned sequence of STANs may be reset to the original starting number on the list depending on user input or other triggers. In addition, the list of numbers may be periodically downloaded via a cellular phone network or other network connectivity.

Figure 2B shows intelligent electronic device 230 and electronic transaction card 240. Intelligent electronic device 230 is an example of a "wearable" device that is capable of communicating with an electronic transaction card. For example, intelligent electronic device 230 is shown having the form factor of a wristwatch. Some embodiments of the present invention may have other wearable form factors. For example, a wearable intelligent electronic device may be worn in such a manner that it contacts human skin, or it may be worn on clothing. Any wearable intelligent electronic device may be employed without departing from the scope of the present invention. Further, intelligent electronic device 230 may have any of the capabilities described herein.

Intelligent electronic device 230 may include an add-on slot to accept electronic transaction card 230. The add-on slot may be any of the add-on slot embodiments described herein. Electronic transaction card 240 may be any

electronic transaction card. For example, electronic transaction card 240 may be any electronic transaction card embodiment described herein.

Figure 3 shows a block diagram of an electronic transaction card. Electronic transaction card 300 is an electronic transaction card capable of communicating with an intelligent electronic device, and capable of communicating with a magnetic card reader. For example, electronic transaction card 300 may be electronic transaction card 104 (Figure 1) or electronic transaction card 220 (Figure 2A).

Electronic transaction card 300 includes electrical contacts 302, intelligent electronic device (IED) interface 304, nonvolatile memory 306, processing device 308, volatile memory 310, magnetic field producing circuits 312, swipe sensor 314, and stripe 320.

Electrical contacts 302 correspond to electrical contacts 108 (Figure 1). IED interface 304 is coupled to electrical contacts 302 to provide a communications interface between electronic transaction card 300 and an intelligent electronic device. For example, IED interface 304 may be an interface compatible with an add-on slot such as add-on slot 110 (Figure 1) or add-on slot 210 (Figure 2A).

Magnetic field producing circuit 312 includes one or more circuits to produce time-varying magnetic fields at or near the location of stripe 320. For example, one or more current carrying conductors may be excited to produce a magnetic field, and the current may be varied in amplitude and reversed in polarity to cause the magnetic field to be time-varying. In some embodiments, the number of magnetic field producing circuits corresponds to the number of tracks being emulated for stripe 320. For example, stripe 320 may emulate two, three, four, or more magnetic tracks on a magnetic card such as a credit card. In these embodiments, electronic transaction card 300 may include two, three, four, or more magnetic field producing circuits 312. Magnetic field producing circuits 312 may also include circuits to allow control of the time-varying magnetic field. For example, magnetic field producing circuits 312 may include voltage drivers, current drivers, registers to hold digital data, sequential circuits to translate the digital data to magnetic fields, and the like.

Swipe sensor 314 senses when electronic transaction card 300 has been swiped in a magnetic card reader, and provides a swipe indication to processing device 308. The swipe sensor may be a mechanical switch, an electronic switch, or any other type of suitable switch. For example, a mechanical switch may get pressed when electronic transaction card 300 is swiped. Also for example, an electrical sensor may include two or more contacts (not shown) that get shorted when swiped past a metal head within a card reader. Further, a Hall effect sensor or light-based sensor may be utilized. The present invention is not limited by the type of swipe sensor utilized. In some embodiments, swipe sensor 314 is omitted.

Processing device 308 represents a processor capable of communicating with the other blocks shown in electronic transaction card 300. For example, processing device 308 may be a microprocessor, a digital signal processor (DSP), a microcontroller, or the like. Further, processing device 308 may be formed from state machines or other sequential logic. In operation, processing device 308 may read instructions from volatile memory 310 and/or nonvolatile memory 306 and perform actions in response thereto. For example, processing device 308 may execute program instructions that influence communications between electronic transaction card 300 and an intelligent electronic device, or between electronic transaction card 300 and a magnetic card reader.

Volatile memory 310 represents memory that may lose its state when power is removed from electronic transaction card 300. For example, volatile memory 310 may be static random access memory (SRAM). Volatile memory 308 may be utilized by processing device 308 when executing programs. For example, a program may be copied into volatile memory 308 prior to execution. Also for example, processing device 308 may use volatile memory 308 to store data during the execution of a program.

Nonvolatile memory 306 represents memory that does not lose its state when power is removed from electronic transaction card 300. Nonvolatile memory 306 may be any suitable type of memory such as Flash memory with floating gate

transistor memory cells. Examples include NOR Flash memory, NAND Flash memory, and multibit/cell Flash memory.

Nonvolatile memory 306 may hold program instructions that are executable by processing device 308. For example, prior to being sold, a manufacturer or distributor may program nonvolatile memory 306 with program information to influence the operation of electronic transaction card 300. Also for example, an intelligent electronic device may provide program information to electronic transaction card 300 through IED interface 304.

Nonvolatile memory 306 may also hold program instructions that are executable by a processing device other than processing device 308. For example, a manufacturer, distributor, reseller, or other participant in the chain of commerce may program nonvolatile memory 306 with program information to be transferred to an intelligent electronic device. Information to be transferred may include device drivers, application software, or the like.

Electronic transaction card 300 may include one or more power sources (not shown). For example, electronic transaction card 300 may include a battery or a capacitor such as a supercapacitor. In some embodiments, a rechargeable battery may be included. The rechargeable battery may accept a charge from an add-on slot in an intelligent electronic device. In some embodiments, a capacitor may accept a charge from an intelligent electronic device. The capacitor may provide power to electronic transaction card 300 for enough time to perform a transaction. Further, the capacitor may be sized to ensure that a transaction may only be performed during a limited time period after removing the electronic transaction card from an add-on slot, thereby ensuring that a stolen card may not be used repeatedly without the cardholder's consent. Also in some embodiments, electronic transaction card 300 may be programmed to go dormant if a transaction is not performed within a limited time period after removing the card from an intelligent electronic device.

Electronic transaction card 300 may include one or more integrated circuits. For example, processing device 308 may be on one integrated circuit die, and the memories may be on another integrated circuit die. In some embodiments, all active

devices are included on a single integrated circuit die. In some embodiments, various integrated circuit dice are mounted on a common substrate to provide a high level of integration using separate dice. Any amount of circuit integration may be practiced without departing from the scope of the present invention.

Electronic transaction card 300 has dimensions "*a*" and "*b*." In some embodiments of the present invention, stripe 320 has a length that is substantially equal to *a*, and in some embodiments, stripe 320 has a length less than *a*. Further, in some embodiments, *a* is less than the stripe length of a standard credit card (approximately three and three eighths inches), and in some embodiments, *a* is much less than the stripe length of a standard credit card. For example, in some embodiments, *a* is less than 75% the length of a standard credit card stripe. Further, in some embodiments, *a* is less than 50% the length of a standard credit card stripe. In still further embodiments, *a* is less than 25% the length of a standard credit card stripe.

In some embodiments, dimensions *a* and *b* are substantially equal to the dimensions of a memory card. For example, dimensions *a* and *b* may conform to the dimensions of an MMC memory card, a Memory Stick PRO DUO memory card, or other memory card. Further, in some embodiments, electronic transaction card 300 has a thickness compatible with a magnetic card reader.

Figure 4 shows an electronic transaction card and a card reader. Electronic transaction card 410 is a card having a stripe compatible with a magnetic card reader. For example, electronic transaction card 410 may be electronic transaction card 104 (Figure 1), electronic transaction card 220 (Figure 2A), electronic transaction card 300 (Figure 3), or any other electronic transaction card described herein. Magnetic card reader 420 is a card reader compatible with magnetic cards. For example, magnetic card reader 420 may operate as part of a merchant point-of-sale terminal, an access control device, or the like. When a magnetic card is swiped through magnetic card reader 420, one or more time-varying magnetic fields are produced relative to the location of a magnetic read head (not shown) in magnetic card reader 420.

In the operation depicted in Figure 4, electronic transaction card 410 is swiped through magnetic card reader 420. During the swiping operation, electronic transaction card 420 produces one or more time-varying magnetic fields to emulate the swiping of a magnetic card. For example, a swipe sensor within electronic transaction card 410 may detect the swiping action depicted in Figure 4, and a magnetic field producing circuit may generate one or more time-varying magnetic fields as electronic transaction card 410 passes by a magnetic read head in magnetic card reader 420.

Figure 5 shows an intelligent electronic device, an electronic transaction card, and a magnetic card reader. Electronic transaction card 510 is shown being swiped through magnetic card reader 520 while attached to intelligent electronic device 500. The operation depicted in Figure 5 represents a transaction occurring while electronic transaction card 510 is coupled to an add-on slot of intelligent electronic device 500.

Figure 6 shows an adapter for use with an electronic transaction card. Adapter 600 includes a body portion having dimensions "*w*" and "*l*", and a receiving portion shown at 610. Adapter 600 is useful to receive an electronic transaction card at receiving portion 610 to provide a larger card having the functionality of an electronic transaction card. For example, in some embodiments of the present invention, dimensions *w* and *l* are compatible with swallow-type magnetic card readers, and a combination of adapter 600 an electronic transaction card may be compatible with such readers.

Receiving portion 610 may include an interface compatible with a connector on an electronic transaction card. For example, an electronic transaction card may have an interface that is compatible with both an add-on slot of an electronic transaction device and receiving portion 610 of adapter 600.

Figure 7 shows adapter 600 having an electronic transaction card 710 coupled thereto. Electronic transaction card 710 includes a stripe capable of emitting one or more time-varying magnetic fields as described above. The combination of electronic transaction card 710 and adapter 600 allow the

functionality of electronic transaction card 710 to be useful in the larger form factor of adapter 600.

In some embodiments, adapter 600 includes active or passive circuitry in support of the operation of electronic transaction card 710. For example, adapter 600 may include electrical contacts, a battery, an integrated circuit, or other circuits. Also for example, adapter 600 may include one or more swipe sensors to provide a swiping indication to electronic transaction card 710.

Figure 8 shows an adapter having a smartcard interface 810. In embodiments represented by Figure 8, an adapter may be utilized to perform a transaction involving a smartcard reader while utilizing an electronic transaction card. For example, an electronic transaction card may be coupled to adapter 800 at receiving portion 820, and the electronic transaction card may provide data useful for a smartcard transaction.

Figure 9 shows an electronic transaction card having a smartcard interface. Electronic transaction card 900 includes electrical contacts 908 and 910. Electrical contacts 908 are similar to electrical contacts 108 (Figure 1). For example, electrical contacts 908 may be compatible with an add-on slot of an intelligent electronic device such as intelligent electronic device 102 (Figure 1). Electrical contacts 910 are arranged to provide the communications interface to a smartcard reader.

In some embodiments, electronic transaction card 900 includes a smartcard interface as well as a stripe to produce the time-varying magnetic field. For example, as shown in figure 10, the backside of electronic transaction card 900 may include stripe1010. The various electronic transaction cards described herein may include a stripe, a smartcard interface, or a combination thereof.

Figure 11 shows an adapter in combination with an electronic transaction card. Adapter 1100 is shown having electronic transaction card 900 coupled in a recessed portion on a side having dimension *w*. In some embodiments, this configuration places electrical contacts 910 at a location expected by smartcard readers.

Figure 12 shows an adapter having an aperture to receive an electronic transaction card. Adapter 1200 includes aperture1210 to receive an electronic transaction card. In some embodiments, aperture 1210 passes completely through adapter 1200, and in other embodiments, aperture 1210 is a recessed portion on the face of adapter 1200. Adapter 1200 may receive electronic transaction cards having a stripe, a smartcard interface, or a combination of the two.

Figure 13 shows and adapter having a body portion 1300, a recessed portion 1310, and stripe 1320. Recessed portion 1310 may receive an electronic transaction card as described above with respect to Figures 6-7. Further, stripe 1320 may be utilized to communicate with a magnetic card reader. For example, adapter 1300 may include a magnetic field producing circuit such as magnetic field producing circuit 312 (Figure 3) to produce a time-varying magnetic field. In operation, an electronic transaction card may be coupled to adapter 1300 at recessed portion 1310, and provide transaction information to be used by stripe 1320 for a transaction with a magnetic card reader. In some embodiments, an electronic transaction card having neither a stripe nor a smartcard interface may be coupled to adapter 1300 at recessed portion 1310 to effect a transaction using stripe 1320.

The various adapters shown in the previous figures may have recessed portions, apertures, or stripes anywhere on the adapter without departing from the scope of the present invention. For example, in some embodiments, a recessed portion may be on the side of the adapter having a smaller dimension, and in other embodiments a recessed portion may be on the side of the adapter having a larger dimension. Also for example, in some embodiments, a stripe may be on the side of the adapter having a smaller dimension, and in other embodiments a stripe may be on the side of the adapter having a larger dimension.

Figure 14 shows an electronic transaction card. Electronic transaction card 1400 includes stripe 1410 and add-on slot compatible portion 1402. Add-on slot compatible portion 1402 includes electrical contacts 1408 to communicate with an add-on slot in an intelligent electronic device. For example, add-on slot compatible

portion 1402 may be physically and electrically compatible with add-on slot 110 (Figure 1) or add-on slot 210 (Figure 2A).

Electronic transaction card 1400 may include any of the circuits, features, or functionality described herein. For example, electronic transaction card 1400 may include magnetic field producing circuits, swipe sensors, processing devices, volatile and nonvolatile memory, various interfaces, and electrical contacts.

Electronic transaction card 1400 is shown having stripe 1410 along an edge having dimension "*l*." In some embodiments, electronic transaction card 1400 may have stripe 1410 along an edge other than that shown in Figure 14.

In operation, electronic transaction card 1400 may be left coupled to an electronic transaction device when being swiped through a magnetic card reader, similar to the operation shown in Figure 5. Further, electronic transaction card 1400 may be removed from an intelligent electronic device prior to being swept through a magnetic card reader, similar to the operation shown in Figure 4.

Figure 15 shows an electronic transaction card and an adapter in combination. The combination of electronic transaction card 1400 and adapter 1500 form a card having dimensions "*w*" and "*l*" as described above with reference to previous figures. The resulting card may be suitable for swallow-type magnetic card readers.

Figure 16 shows a combination electronic transaction card and adapter 1610 being inserted into a swallow-type magnetic card reader. As shown in Figure 16, the swallow-type magnetic card reader is part of an automated teller machine (ATM), but this is not a limitation of the present invention. For example, the swallow-type reader may be part of a point-of-sale device, an access entry device, or any other type of device capable of incorporating a swallow-type magnetic card reader.

Figure 17 shows a combination electronic transaction card and adapter being swiped through a magnetic card reader. Adapter 1710 and electronic transaction card 1720 are shown being swiped through magnetic card reader 1730. Electronic transaction card 1720 maybe any of the electronic transaction card embodiments

described herein. For example, electronic transaction card 1720 may include a stripe, a smartcard interface, or a combination of the two. Although adapter 1710 is shown as an adapter having a recessed portion on one side, the combination adapter/card in Figure 17 represents any of the adapter/ card combinations described herein. For example, adapter 1710 may be any of adapters 600 (Figures 6,7), adapter 800 (Figure 8), adapter 1100 (Figure 11), adapter 1200 (Figure 12), adapter 1300 (Figure 13), or adapter 1500 (Figure 15).

Figure 18 shows a financial transaction card. Financial transaction card 1800 includes stripe 1802, financial card circuits 1804, memory card emulation circuitry 1806, and memory card compatible interface 1808. Financial transaction card 1800 is an example of a financial card that might be issued by a bank or other financial institution. For example, financial transaction card 1800 might be a debit card, a credit card, a stored value card, or other card issued for the purposes of financial transactions.

Financial card circuits 1804 interact with stripe 1802 to produce time-varying magnetic fields compatible with a magnetic card reader. For example, financial card circuits 1804 and stripe 1802 may provide financial transaction data to a point-of-sale terminal. Financial transaction card 1800 also includes memory card emulation circuitry 1806 to emulate the operation of a memory card. The combination of memory card emulation circuitry 1806 and memory card compatible interface 1808 allow financial transaction card 1800 to perform as a memory card. For example, memory card compatible interface 1808 may be compatible with a memory card interface in an add-on slot of an intelligent electronic device.

Figure 19 shows a memory card. Memory card 1900 includes memory card compatible interface 1930, memory card circuits 1920, financial card emulation circuitry 1910, and stripe 1902. Memory card 1900 is an example of a card that may be fabricated and sold by a memory card manufacturer or a manufacturer that is in the business of selling electronic peripheral devices. By including financial card emulation circuitry 1910 and stripe 1902 in memory card 1900, the manufacturer of memory card 1900 may add features desired by consumers. For example, the

combination of stripe 1902 and financial card emulation circuitry 1910 may emulate the operation of a financial card such as a credit card, debit card, stored value card, or the like.

Figure 20 shows a block diagram of a combination memory card and electronic transaction card. Card 2000 includes memory 2010, processing element 2020, magnetic/smartcard circuitry 2030, card reader interface 2040, memory card circuitry 2050, and memory card slot compatible interface 2060. Processing element 2020 may be any processing element suitable to communicate with memory 2010 and the other blocks shown in Figure 20. Magnetic/smartcard circuitry 2030 may include circuits to produce time-varying magnetic fields or signals compatible with a smart card reader. Card reader interface 2040 may include a stripe as described above, or may include electrical contacts compatible with a smartcard reader. Memory card circuitry 2050 may be any type of memory circuitry accessible by an intelligent electronic device. The intelligent electronic device may access memory card circuitry 2050 through memory card slot compatible interface 2060.

Memory 2010 is shown having card software 2012 and application software 2014. In some embodiments, card 2000 is sold or distributed having both card software 2012 and application software 2014 in memory 2010. For example, memory 2010 may be nonvolatile memory having card software 2012 for execution by processing element 2020. Also for example, memory 2010 may have application software 2014 meant to be installed on a device other than card 2000. Application software 2014 may include drivers, user interface software, single transaction account number (STAN) generation software, or any other software that may be installed on a device other than card 2000.

Application software 2014 may operate in any of multiple languages on multiple operating systems. For example, application software 2014 may provide a user interface in any regional language. Also for example, application software 2014 may run on any operating system (OS).

Figure 21 shows a block diagram of how card 2000 (Figure 20) may be utilized. A card issuer 2110 may issue card 2000 to a cardholder 2130. As issued by card issuer 2110, card 2000 may include card software and application software as shown in Figure 21. Cardholder 2130 may couple card 2000 with intelligent electronic device 2140 and install application software on the intelligent electronic device. For example, intelligent electronic device 2140 may be a mobile phone capable of executing application software, and card 2000 may supply application software to be installed on the mobile phone. Also for example, intelligent electronic device 2140 may be a non-telephonic device such as a personal digital assistant (PDA), or other dedicated hardware, capable of receiving card 2000 in an add-on slot.

Figure 22 shows a block diagram of a combination memory card and electronic transaction card. Card 2200 includes processing element 2020, magnetic/smartcard circuitry 2030, card reader interface 2040, memory card circuitry 2050, and memory card slot compatible interface 2060, all of which are described above with reference to Figure 20. Card 2200 also includes nonvolatile memory 2210 and volatile memory 2220. As shown in Figure 22, nonvolatile memory 2210 includes card software 2212 to be executed by processing element 2020. Also as shown in Figure 22, card 2200 includes volatile memory 2220 having financial transaction data 2222 held therein. Financial transaction data 2222 may be programmed into volatile memory 2220 by processing alignment 2020 in response to communications from an intelligent electronic device coupled to memory card slot compatible interface 2060. For example, a mobile phone executing single transaction account number generation software may provide a single transaction account number as financial transaction data that gets stored in volatile memory 2220 in preparation for a transaction. In other embodiments, financial transaction data 2222 represents two, three, four, or more time-varying magnetic fields to be generated by the combination of magnetic/smartcard circuitry 2030 and card reader interface 2040.

Figure 23 shows a block diagram of a phone and a card. Phone 2310 may be a cellular telephone, and card 2350 may be any of the electronic transaction card embodiments described herein. Phone 2310 includes display 2312, processor 2314, single transaction account number (STAN) generation software 2316, and authentication software 2318. Card 2350 includes processor 2352, card software 2354, financial transaction data 2356, and point-of-sale (POS) interface 2358.

Single transaction account number generation software 2316 may be installed on the phone 2310 when card 2350 is inserted in a memory slot. For example, referring now back to Figures 20 and 21, STAN generation software 2316 may correspond to application software 2014. Authentication software 2318 may only allow authorized users access to phone 2310 and/or card 2350.

In operation, a user interacting with phone 2310 may gain access to features by satisfying requirements of authentication software 2318. Using STAN generation software 2316, a user may generate financial transaction data 2356 which is held on card 2350 in preparation for a transaction. Card 2350 may then interact with a card reader using point-of-sale interface 2358 to effect a transaction. This transaction may be effected with card 2350 coupled to phone 2310 or decoupled from phone 2310. Further, the transaction using card 2350 may be effected while card 2350 is coupled to any of the adapter embodiments described herein.

The following paragraphs provide further disclosure of various invention embodiments. Each embodiment is fully defined by the recitation of the corresponding paragraph, and no other elements are to be considered essential for that particular embodiment. The embodiments include:

A. An apparatus comprising:

a stripe to communicate with a magnetic card reader; and

an interface to communicate with an intelligent electronic device;

wherein the apparatus has dimensions smaller than a credit card.

A1. The apparatus of A wherein the stripe includes circuitry to produce at least one time-varying magnetic field.

A2. The apparatus of A wherein the interface is compatible with an add-on slot in the intelligent electronic device.

A3. The apparatus of A2 wherein the interface comprises a memory card interface.

A4. The apparatus of A further comprising a processing element coupled to the interface and to the stripe.

A5. The apparatus of A4 further comprising a memory element to hold programming information for the stripe.

A6. The apparatus of A4 further comprising an embedded swipe sensor to sense when the stripe is swiped through a magnetic card reader.

A7. The apparatus of A further comprising nonvolatile memory accessible by the intelligent electronic device.

B. A financial card comprising:
a point-of-sale compatible electronic transaction stripe;
a memory card compatible interface; and
memory card emulation circuitry coupled to the memory card compatible interface.

C. A memory card comprising:
a memory card compatible interface;
a point-of-sale compatible electronic transaction stripe; and

financial card emulation circuitry coupled to the point-of-sale compatible electronic transaction stripe.

D. A financial card apparatus comprising:

a point-of-sale compatible portion having a stripe to communicate with a point-of-sale transaction device; and

a memory card compatible portion having at least one electrical contact to communicate with a memory card slot in an intelligent electronic device.

E. A memory card comprising:

a memory card interface operable to couple the memory card to an intelligent electronic device;

a nonvolatile memory device accessible through the memory card interface; and

a stripe operable to communicate with a magnetic card reader.

F. A memory card comprising:

a memory card slot interface; and

circuitry for producing a time-varying magnetic field compatible with a magnetic card reader.

F1. The memory card of F wherein the circuitry is configured to produce a plurality of time-varying magnetic fields compatible with a point-of-sale transaction device.

G. An apparatus comprising:

means for communicating through a memory card slot in an intelligent electronic device;

means for producing at least one time-varying magnetic field to represent financial transaction data; and

means for storing the financial transaction data.

H. A card comprising:

a memory card compatible interface;

a smartcard compatible interface; and

a stripe to produce at least one time-varying magnetic field compatible with a magnetic card reader.

I. A memory card compatible with a memory card slot in a mobile phone, the memory card including nonvolatile memory accessible by the mobile phone, a point-of-sale interface to communicate with a point-of-sale terminal, and volatile memory to hold financial transaction data.

I1. The memory card of I wherein the point-of-sale interface comprises circuitry to produce at least one time-varying magnetic field.

I2. The memory card of I1 further including a processing device coupled to the nonvolatile memory, volatile memory, and point-of-sale interface.

J. An electronic financial transaction device having a thickness compatible with a point-of-sale card reader, a width less than a credit card width, a length less than a credit card length, an electronically programmable stripe situated along the length, and at least one electrical contact to provide an interface to an intelligent electronic device.

J1. The electronic financial transaction device of J wherein the at least one electrical contact comprises a memory card interface compatible with a memory card slot in the intelligent electronic device.

J2. The electronic financial transaction device of J wherein the electronically programmable stripe includes a circuit to emulate a magnetic stripe in a credit card.

J3. The electronic financial transaction device of J2 further comprising a swipe sensor to detect when the electronic financial device is swiped through a point-of-sale terminal.

K. A card comprising:

means for storing financial transaction data;

means for communicating with a memory card slot in an intelligent electronic device; and

means for creating a time-varying magnetic field that represents the financial transaction data.

K1. The card of K wherein the means for storing financial transaction data comprises volatile memory.

K2. The card of K wherein the financial transaction data comprises a single transaction account number.

K3. The card of K further comprising a processing device coupled to read the financial transaction data and influence the operation of the means for creating a time-varying magnetic field.

L. An adapter for use with any of A-K, the adapter comprising:

a body portion having exterior dimensions larger than dimensions of A-G; and

a receiving portion to receive any of A-G, wherein the receiving portion is located on the body portion to expose any of A-G for use in magnetic card reader transactions.

M. An apparatus comprising a body portion with dimensions compatible with a swallow-type magnetic card reader, wherein the body portion includes a memory card compatible area to receive a memory card with magnetic stripe functionality.

M1. The apparatus of M further comprising a smartcard interface.

M2. The apparatus of M further comprising at least one electrical component coupled to the memory card compatible area portion to interface to the memory card.

M3. The apparatus of M wherein the memory card compatible area comprises a recessed portion of at least one side of the apparatus.

M4. The apparatus of M wherein memory card compatible area comprises at least one metallic contact on a periphery of an aperture in the apparatus.

N. A financial card to be used with a magnetic card reader at a point-of-sale, the financial card including a memory card interface to allow the financial card to be inserted in a memory card slot of a mobile phone, and including a stripe compatible with the magnetic card reader, wherein the stripe is shorter than a magnetic credit card stripe.

O. A card compatible with a magnetic card reader and compatible with a memory slot in an intelligent electronic device, the card including software to be installed on the intelligent electronic device.

O1. The card of O wherein the software includes a module for single transaction account number generation.

O2. The card of O1 wherein the software is configured to run on a mobile phone.

O3. The card of O wherein the card comprises:

a memory slot compatible portion; and

a magnetic card reader compatible portion.

O4. The card of O3 wherein the magnetic card reader compatible portion comprises circuitry to produce at least one time-varying magnetic field for use in a financial transaction.

P. A card comprising:

a memory card interface mechanically compatible with a memory card slot in an intelligent electronic device;

a processing device coupled to the memory card interface; and

circuitry to produce a time-varying magnetic field compatible with a point-of-sale device.

Q. A card comprising:

a memory card interface electrically compatible with a memory card slot in an intelligent electronic device;

a processing device coupled to the memory card interface; and

circuitry to produce a time-varying magnetic field compatible with a point-of-sale device.

Q1. Any of the cards of P-Q further comprising nonvolatile memory exposed through the memory card interface.

Q2. Any of the cards of P-Q further comprising volatile memory to hold financial transaction information.

Q3. Any of the cards of P-Q further comprising a software component that when executed by the processing device causes the circuitry to produce at least one time-varying magnetic field representing the financial transaction information.

Q4. Any of the cards of P-Q further comprising a visible stripe at which the at least one time-varying magnetic field emanates.

Q5. Any of the cards of P-Q further comprising a battery.

Q6. Any of the cards of P-Q further comprising a capacitor to provide power to the card.

Q7. The card of Q wherein the card has a size substantially equivalent to a credit card.

R. A credit card sized adapter to receive any of the cards of P-Q.

R1. The adapter of R wherein the credit card sized adapter includes a smartcard interface.

R2. The adapter of R wherein the adapter includes a first edge having a width and a second edge having a length, wherein the second edge includes a recessed portion to accept the card.

R3. The adapter of R wherein the credit card sized adapter includes a first edge having a width and a second edge having a length, wherein the first edge includes a recessed portion to accept the card.

S. A combination financial card and memory card apparatus comprising:

electrical contacts to provide an interface to a mobile phone;

a transaction stripe to produce at least one time-varying magnetic field representing transaction information;

a processing device; and

a software component to receive the transaction information from the mobile phone;

wherein the electrical contacts are provided on a physical portion of the combination financial card and memory card apparatus having dimensions compatible with a memory card slot.

S1. The combination financial card and memory card apparatus of S further comprises an application software component to be installed on the mobile phone.

T. In combination:

a memory card having a transaction stripe compatible with a magnetic card reader; and

a credit card sized adapter to receive the memory card and to expose the transaction stripe for use in magnetic card reader transactions.

U. In combination:

a memory card having an interface compatible with a memory card slot in a mobile phone and a smartcard interface; and

a credit card sized adapter to receive the memory card and to expose the smartcard interface for use in smartcard transactions.

V. A financial transaction system comprising:

a mobile phone having a memory card slot;

a memory card compatible with the memory card slot, wherein the memory card includes circuitry to transmit financial transaction data to a point-of-sale device; and

a software component to produce single transaction account numbers for use as financial transaction data.

W. A system comprising:

a wearable intelligent electronic device having a card slot; and

a card comprising a card slot interface and circuitry for producing a time-varying magnetic field compatible with a magnetic card reader.

Although the present invention has been described in conjunction with certain embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention as those skilled in the art readily understand. Such modifications and variations are considered to be within the scope of the invention and the appended claims.

What is claimed is:

1. A mobile phone comprising:

a memory to hold transaction data for repeated use in a plurality of transactions;

a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;

a driver to excite the current carrying conductor; and

a processor coupled to control the driver.

2. The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.

3. The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.

4. The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.

5. The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.

6. The mobile phone of claim 1 wherein the driver comprises a current driver.

7. A mobile phone comprising:

a memory to hold transaction data for repeated use in a plurality of transactions;

a conductor that when excited by a reversing polarity current produces a time-varying magnetic field that represents the transaction data in the plurality of transactions;

a driver to excite the conductor; and

a processor coupled to control the driver.

8. The mobile phone of claim 7 wherein the time-varying magnetic field represents a point-of-sale transaction.

9. The mobile phone of claim 7 wherein the time-varying magnetic field represents an access transaction.

10. The mobile phone of claim 7 wherein the time-varying magnetic field represents a credit card transaction.

11. The mobile phone of claim 7 wherein the time-varying magnetic field emulates a swipe of a magnetic card.

12. The mobile phone of claim 7 wherein the driver comprises a current driver.

13. A mobile phone comprising:

a memory to hold transaction data for repeated use in a plurality of transactions;

a conductor that when excited by a reversing polarity current that varies in amplitude produces a time-varying magnetic field that represents the transaction data in the plurality of transactions;

a driver to excite the conductor; and

a processor coupled to control the driver.

14. The mobile phone of claim 13 wherein the time-varying magnetic field represents a point-of-sale transaction.

15. The mobile phone of claim 13 wherein the time-varying magnetic field represents an access transaction.

16. The mobile phone of claim 13 wherein the time-varying magnetic field represents a credit card transaction.

17. The mobile phone of claim 13 wherein the time-varying magnetic field emulates a swipe of a magnetic card.

18. The mobile phone of claim 13 wherein the driver comprises a current driver.

Abstract of Disclosure

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.

Electronic Acknowledgement Receipt

EFS ID:	40562112
Application Number:	17021347
International Application Number:	
Confirmation Number:	2310
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Customer Number:	35781
Filer:	Dana B. LeMoine/Theresa LeMoine
Filer Authorized By:	Dana B. LeMoine
Attorney Docket Number:	115.001US9.10
Receipt Date:	15-SEP-2020
Filing Date:	
Time Stamp:	15:08:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1720
RAM confirmation Number	E20209EF09555044
Deposit Account	
Authorized User	

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	115_001us9_10_dwgs.pdf	800387 d9428d23f11cba9076409bc3b17214cdc0656d5d	no	16
Warnings:					
Information:					
2	Application Data Sheet	115_001US9_10_USPTO_AIA14_20200915.pdf	1874749 3aecdda7e90fe8ab71c4b2615fb8abb817a8d67b	no	10
Warnings:					
Information:					
3	Power of Attorney	115_001US9_10_USPTO_AIA82_20200915.pdf	738968 bf36d5a66934831e584da1f8dd3dba3b1cdf43a1	no	4
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	115_001US9_10_SB08a_IDS_09-15-2020.pdf	1014150 e4cd08817ff2a73d5b6589c013818a36cc8c1cc8	no	35
Warnings:					
Information:					
5	Foreign Reference	DE10054890A1.pdf	528343 4cbb656e5dd5dd33358ebf65d1880016b3724511	no	7
Warnings:					
Information:					
6	Foreign Reference	DE03632294A1.pdf	242737 8bbd8759db37394bee9c21929029c88801f0610b	no	5
Warnings:					
Information:					

7	Foreign Reference	EP00818757A2.pdf	769903 1ccabea0c52d04cee00ed24e9b2920779bc48711	no	13
Warnings:					
Information:					
8	Foreign Reference	EP1014290A2.pdf	932336 4f6ea0557155fb3157bf65d2661f7f96c8061446	no	25
Warnings:					
Information:					
9	Foreign Reference	EP01117068A1.pdf	545960 53736ac775d49ab7a01cb637e8f7131930da94f5	no	40
Warnings:					
Information:					
10	Foreign Reference	EP01178450A2.pdf	132524 c389857dda747321aa9dbc681f435bd3ddc591b2	no	11
Warnings:					
Information:					
11	Foreign Reference	EP01189465A1.pdf	184817 b412692c91bcbad5901f462814bde956ff2c6ed2	no	10
Warnings:					
Information:					
12	Foreign Reference	EP01291748A2.pdf	208443 c428b77cf26f30dd49dc67a0bff2802a0171ae5d	no	16
Warnings:					
Information:					
13	Non Patent Literature	EP0161060A1.pdf	643951 a5887e80504b29815ec348a5d5f87b811fbcba3f	no	17
Warnings:					
Information:					

14	Foreign Reference	GB2316908.pdf	347076 2733a1059d2826543d66b07475a86076858b2a7c	no	11
Warnings:					
Information:					
15	Foreign Reference	JP2000010668A.pdf	370491 79b6268755b9f627092a5b9f3fe0c81abd6aefc9	no	8
Warnings:					
Information:					
16	Foreign Reference	JP2005018671A.pdf	373304 e6fa4f42cf25d619635c245dd806c5393527c259	no	11
Warnings:					
Information:					
17	Foreign Reference	JP2007199847A.pdf	365016 530d8a70e8613ff66af3d84cd3c216cfeac46917	no	11
Warnings:					
Information:					
18	Foreign Reference	JP2007328689A.pdf	339431 0a2cdd29f568f74fe516daeb2f565120b44a1b56	no	10
Warnings:					
Information:					
19	Foreign Reference	JP04102112A.pdf	35806 31639066f6e47f2e3e14f8692ac7ba9b39a47a59	no	3
Warnings:					
Information:					
20	Foreign Reference	200905471.pdf	1279477 ea03b4a0a5a9091a82c2f34d6f9087f1657bdf74	no	39
Warnings:					
Information:					

21	Foreign Reference	201023662.pdf	1749731 c87e194b663206dcb0ce85943690af3e9a686964	no	52
Warnings:					
Information:					
22	Foreign Reference	TW201126422.pdf	1071266 38940acbc069a132597187e7151054c19c505824	no	33
Warnings:					
Information:					
23	Foreign Reference	TW2001I336449B.pdf	184566 afe0786cda44b296ad14803cf86f5c5261e92522	no	6
Warnings:					
Information:					
24	Foreign Reference	W0014678.pdf	977746 d13f91a1120fdbc61e876facc9cdc17f1d8720cf	no	31
Warnings:					
Information:					
25	Foreign Reference	WO01088659A3.pdf	2872144 a26a9595c31f87f7609ab6e1d74fe5a694c0a9bb	no	62
Warnings:					
Information:					
26	Foreign Reference	WO03029942A2.pdf	6679466 b2c3b30f2800d15b67136de1b599745399741987	no	134
Warnings:					
Information:					
27	Foreign Reference	WO03077473A1.pdf	1600438 3c50a93d76155d81dc3d65de6fd0bef030a0f633	no	39
Warnings:					
Information:					

28	Foreign Reference	WO03081519A2.pdf	7633617 0f23cf57fd11ecabf046d92124a598046ae32819	no	163
Warnings:					
Information:					
29	Foreign Reference	WO2004012352A1.pdf	1562988 503ba35417d0d681bb930f5debd92ab8744e43cf	no	33
Warnings:					
Information:					
30	Foreign Reference	Wo2004095169.pdf	2466942 0201489e02f499548be99f3c25791ea4ba999bec	no	57
Warnings:					
Information:					
31	Foreign Reference	WO05027030A1.pdf	1236670 f42b3f8d8e7d834377d046e2c81e4549a17df329	no	40
Warnings:					
Information:					
32	Foreign Reference	WO2005119607.pdf	1629011 06ddc137404d2fbc572f2e0cd42838e58c19ad7b	no	52
Warnings:					
Information:					
33	Foreign Reference	WO2005119607A3.pdf	130095 23ec757835d7319f167a302ba3086620b8d51206	no	3
Warnings:					
Information:					
34	Foreign Reference	WO2005119608.pdf	1660357 d83f3324391ae93adad3a4b06a266f72e47d15fc	no	45
Warnings:					
Information:					

35	Foreign Reference	WO06091709A2.pdf	1589162 01cef81ab0c9b492c1ba520e963c8d68c6a284f4	no	50
Warnings:					
Information:					
36	Foreign Reference	WO06091709A3.pdf	154488 3bcf5ae9bc639d5205805 1437403e32c782e1b7c	no	5
Warnings:					
Information:					
37	Foreign Reference	06108184.pdf	1309816 a43323b470cd137af37fd8a8cac7965aefd39074	no	40
Warnings:					
Information:					
38	Foreign Reference	WO27011937A2.pdf	514645 461e1ddc2adfbc75737560975af8525b167452a9	no	17
Warnings:					
Information:					
39	Foreign Reference	WO28121566A1.pdf	1075067 a34193fe4c5c7d41b96c7bb7b063b83d8f14427c	no	29
Warnings:					
Information:					
40	Foreign Reference	WO09147548A2.pdf	800304 b642deb28cd28d051e352308d1eef16e0fdb6128	no	21
Warnings:					
Information:					
41	Foreign Reference	10099093.pdf	870360 bb08a9e0a66d664c6d2f0a73df49ff792192a2fe	no	24
Warnings:					
Information:					

42	Foreign Reference	WO09626500A1.pdf	687257 abf8b38678bdf2b9d68a46f89c1eda94409 2c2ce	no	23
Warnings:					
Information:					
43	Foreign Reference	98012674.pdf	856749 67951bee3dbaf2096b965a99517c38d0e2a 39886	no	33
Warnings:					
Information:					
44	Other Reference-Patent/App/Search documents	PCTUS2005019988_ISR.pdf	177122 0cf2ee34697bc7b885c7438f5b68b2f8232d 11c5	no	5
Warnings:					
Information:					
45	Other Reference-Patent/App/Search documents	PCTUS2005022993_ISR_10_21_05.pdf	102439 43e97bd4b44a72939390019fe5dafecd334 06fb1	no	3
Warnings:					
Information:					
46	Other Reference-Patent/App/Search documents	PCTUS2006013603_ISR_01_09_06.pdf	141065 6e4b7bc72787ed01006cc906c86e37f04c2 12a19	no	3
Warnings:					
Information:					
47	Other Reference-Patent/App/Search documents	PCTUS2006027847_ISR_29_03_2007.pdf	160849 2c719d9838080c3b9adfee71e8a4804b73a 5e1d0	no	5
Warnings:					
Information:					
48	Other Reference-Patent/App/Search documents	PCTUS2008057588_ISR_08_07_2008.pdf	55072 9d7c9fa438a52e52fd15bd83a92ead82ae3f 87fa	no	1
Warnings:					
Information:					

49	Other Reference-Patent/App/Search documents	PCT_US2005_019988_12-4-06.pdf	455374 20d9aa3e9c50ecd9d7086225ecc0ad8869244f42	no	9
Warnings:					
Information:					
50	Other Reference-Patent/App/Search documents	PCTUS2005019988_IPRP.pdf	455162 08901e45c2380c73499e4288a143e72a9cec6120	no	9
Warnings:					
Information:					
51	Other Reference-Patent/App/Search documents	PCT_US2005_022993_12-4-06.pdf	246769 f822a9b8f8fee99295b82b8f63562f469df0d6ef	no	6
Warnings:					
Information:					
52	Other Reference-Patent/App/Search documents	PCT_US2006_006361_IPRP.pdf	281733 462fe0cb4a881cc11b34f40932e3ed494a60effc	no	8
Warnings:					
Information:					
53	Other Reference-Patent/App/Search documents	PCT_US2006_006361_PCT_Search_Report_80150-001WO1.pdf	635693 002aa3d1c9244624af1732a68e3af3bfc112ba55	no	13
Warnings:					
Information:					
54	Other Reference-Patent/App/Search documents	PCTUS2006013603_IPRP_WO_10_09_07.pdf	252849 6f1c63bc0a9791565fb7a1d6314952946398dd8f	no	7
Warnings:					
Information:					
55	Other Reference-Patent/App/Search documents	PCTUS2006027847_IPRP_WO_22_01_2008.pdf	368512 e842075edd46bf0df0bdeea75d45c79a34934fb2	no	10
Warnings:					
Information:					

56	Other Reference-Patent/App/Search documents	PCTUS2008057588_IPRP_WO_10_06_2009.pdf	347950 ce28a769c5d0b8dbb9983556c200d67c3c884c42	no	6
Warnings:					
Information:					
57	Other Reference-Patent/App/Search documents	PCTUS2008057588_IPRP_and_WO_10_06_2009.pdf	347214 94a2e83ef746bbc5e39197abc113f0b4e315f904	no	6
Warnings:					
Information:					
58	Other Reference-Patent/App/Search documents	PCTUS2010025014_ISR_WR_04_15_2010.pdf	570152 b1d05b9635824dcbd93a78c8f4b02ab76edf773e	no	9
Warnings:					
Information:					
59	Other Reference-Patent/App/Search documents	PCT_US2010_025014_IPRP.pdf	333036 24ab6071a41f2cec60996763e30c6bef4cb0ea89	no	6
Warnings:					
Information:					
60	Non Patent Literature	Lee_Antenna_Circuit_Design_.pdf	1701592 77c29c31b2b56bbe03575248ff9307c9547d5f59	no	50
Warnings:					
Information:					
61	Fee Worksheet (SB06)	fee-info.pdf	34747 6cf579af73491393744c274cf670eae55e6cdef8	no	2
Warnings:					
Information:					
62	Specification	2020_09_15_13_42_08_0203_872d6c0b-44b8-40ff-8fe8-d0eda1d0eb39.docx	32855 10664ff63f71974e4d2f1edafbc7fd7438eb26eebd30baebaf41db66dc5e04a7d967ac4eb2c2d40df79d24488b0f3aeb700e425d4867fbc27514b2b076696a16	no	30
Warnings:					
Information:					

63	Specification	3fa259f7-0cbb-4932-a7cb-0401d6929061.pdf	200721 b7ee1e2ac8f4860e3dfe7006decdd2630fc215fa	no	30
Warnings:					
Information:					
64	Claims	2020_09_15_13_42_09_0688_fe73dba0-7ecc-44f9-823d-0029bbdf7c35.docx	21162 a729fbc399fbd4f7c16c5fba2c4b3123731d8bb995e37f68f09e8ee3d47193028bd2a9659a4e2153e84557bf9fd072dee228888c2e35a2a194c77e181ebf9b4b	no	4
Warnings:					
Information:					
65	Claims	e4fc940d-48fc-457a-991d-a792fc9e0125.pdf	10999 f6012f4b18abe9aca4948f916a8df48369080a66	no	4
Warnings:					
Information:					
66	Abstract	2020_09_15_13_42_10_0922_18805ba4-f362-4bda-8473-29241ea98c5f.docx	18007 1681fc58324352d102d8967863e7f9845454abf81388a094c08fd66ac37b574f5383ebc5f108b40f2c82baefb9e364a3421cd7548464c81829d58e5f0086cb5b	no	1
Warnings:					
Information:					
67	Abstract	1ed49e4f-c264-474a-9d7c-6fd56c268e53.pdf	4399 d670843467 25f619f4475e5428fdecfe46c0060f	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	57996227	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

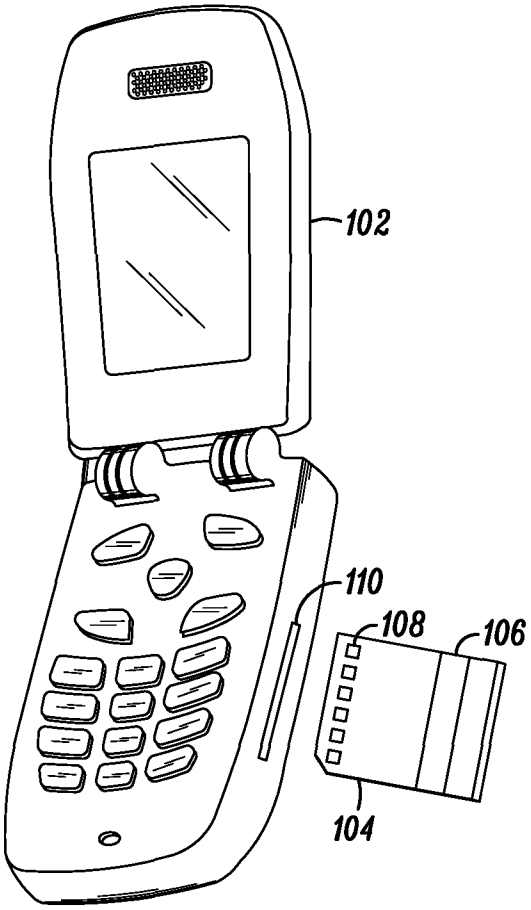


FIG. 1

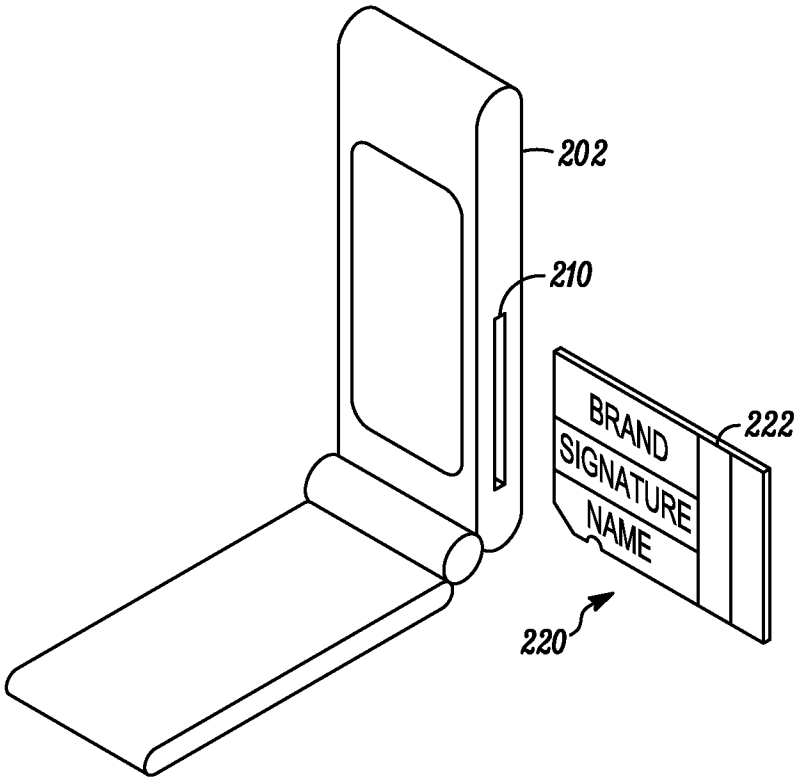


FIG. 2A

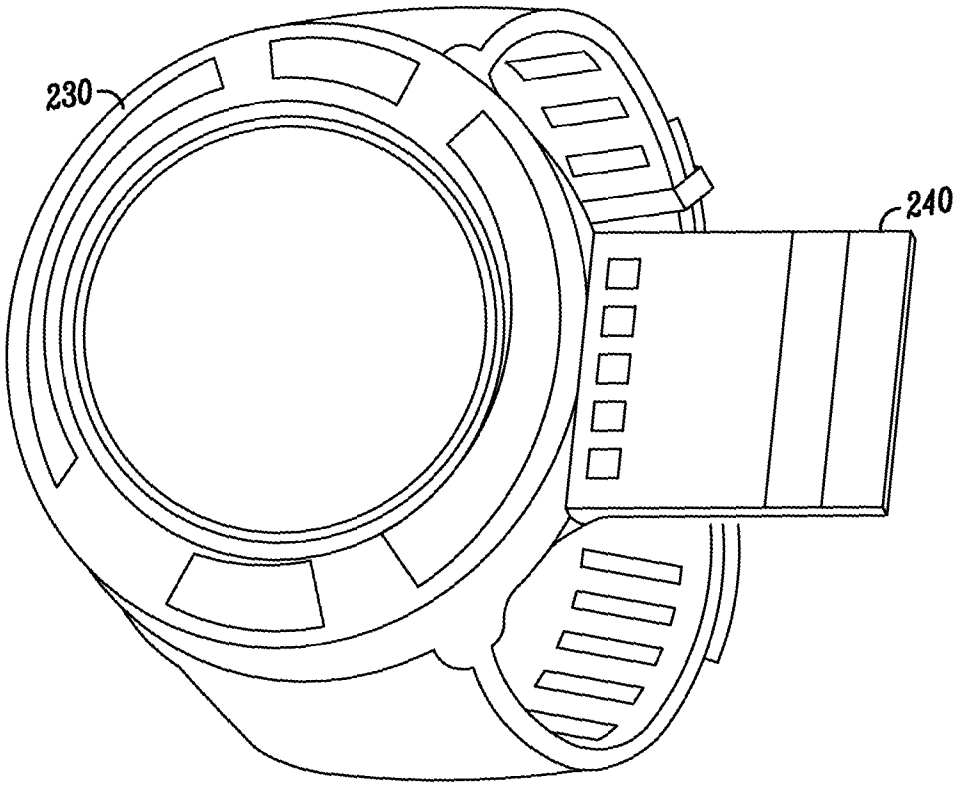


FIG. 2B

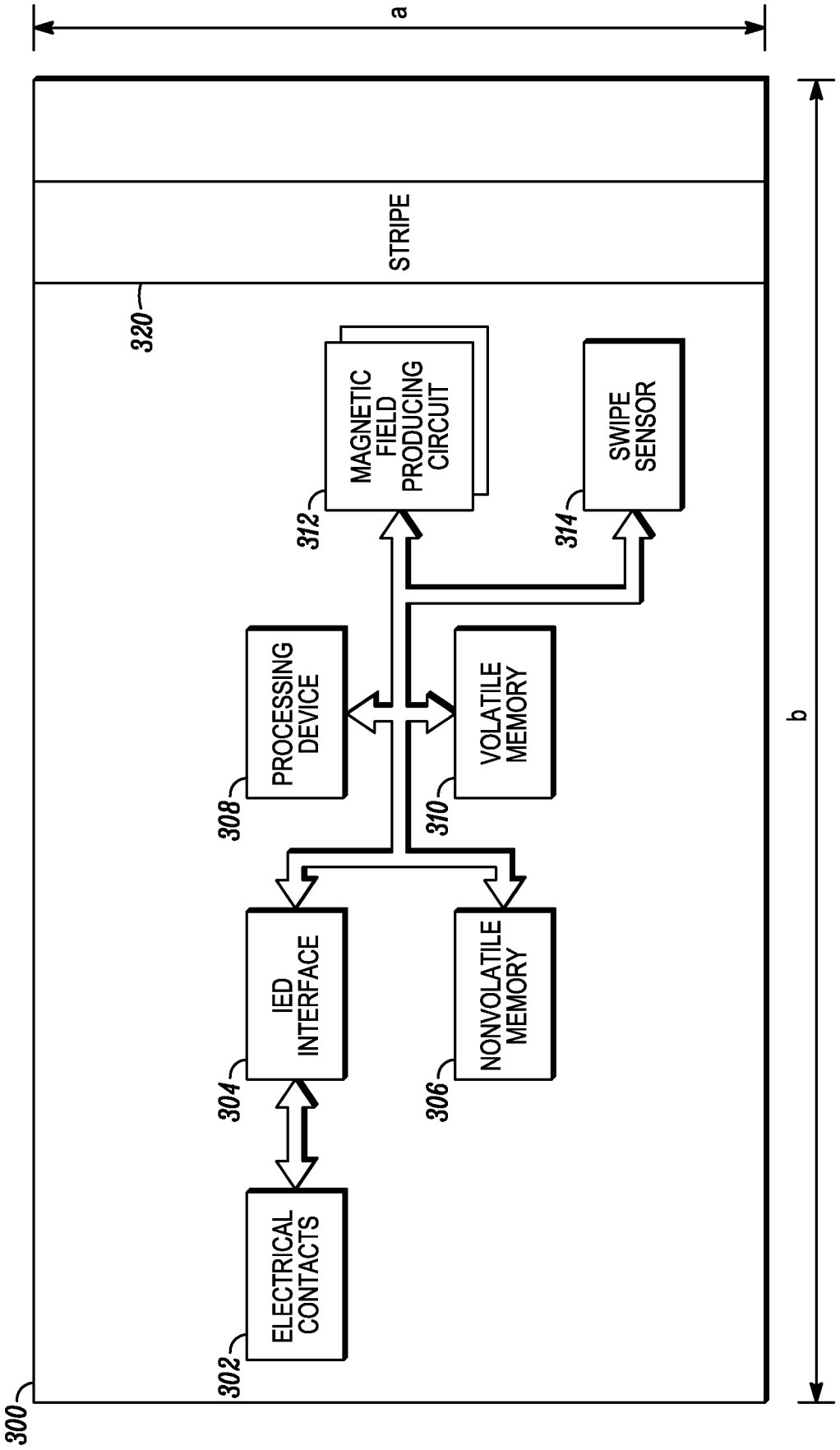

a
b
STRIPE
320
MAGNETIC FIELD PRODUCING CIRCUIT
312
SWIPE SENSOR
314
PROCESSING DEVICE
308
VOLATILE MEMORY
310
IED INTERFACE
304
NONVOLATILE MEMORY
306
ELECTRICAL CONTACTS
302
300

FIG. 3

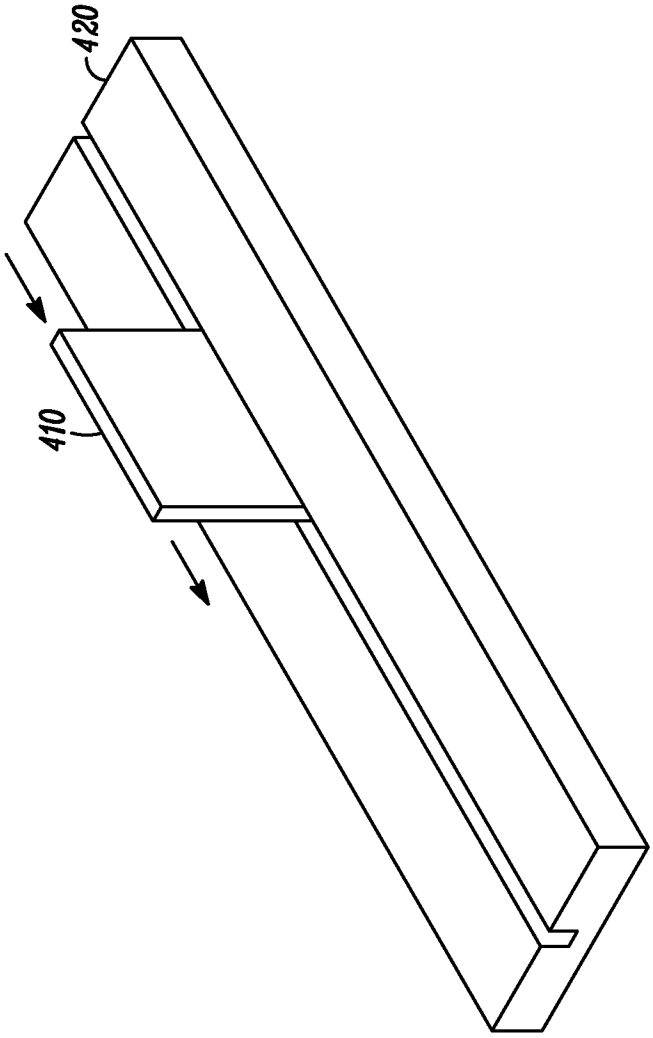


FIG. 4

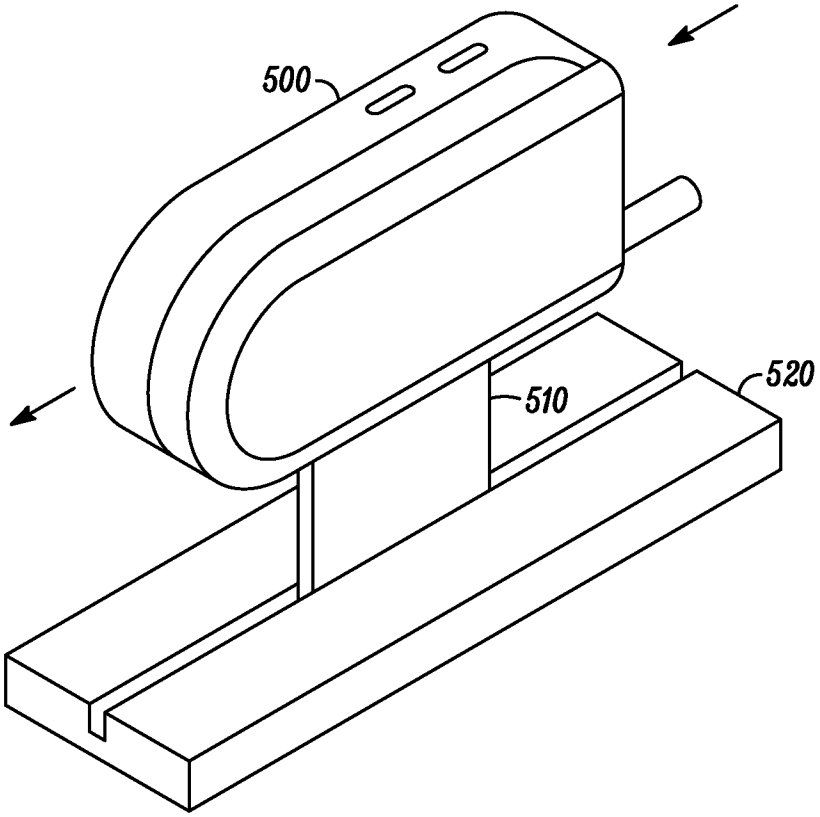


FIG. 5

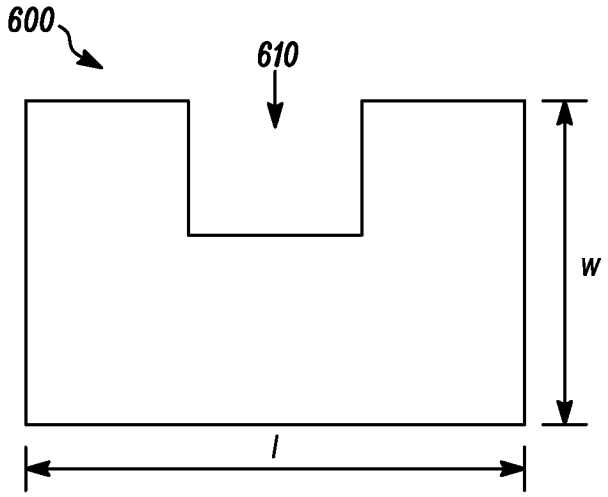


FIG. 6

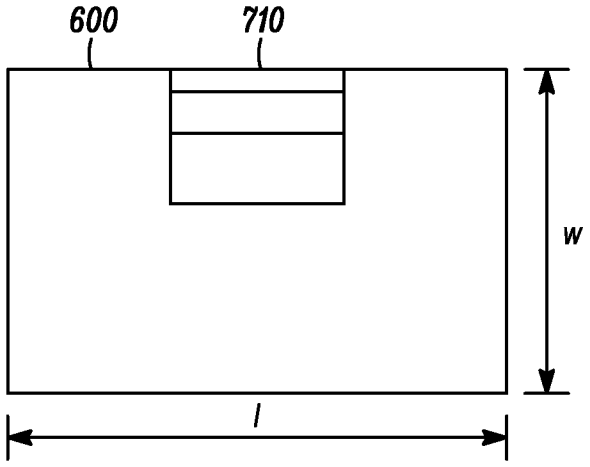


FIG. 7

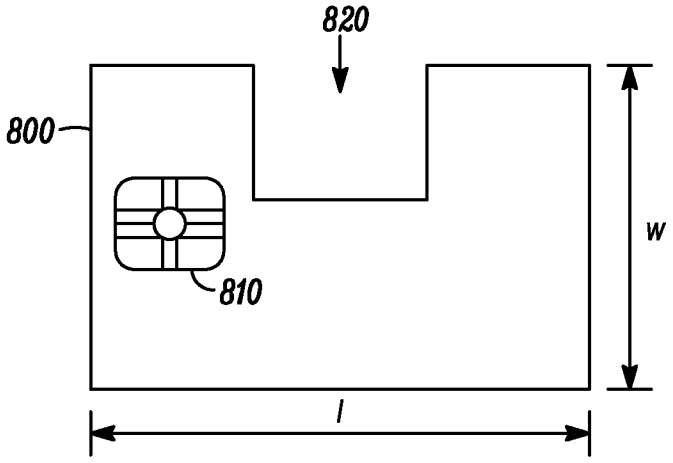


FIG. 8

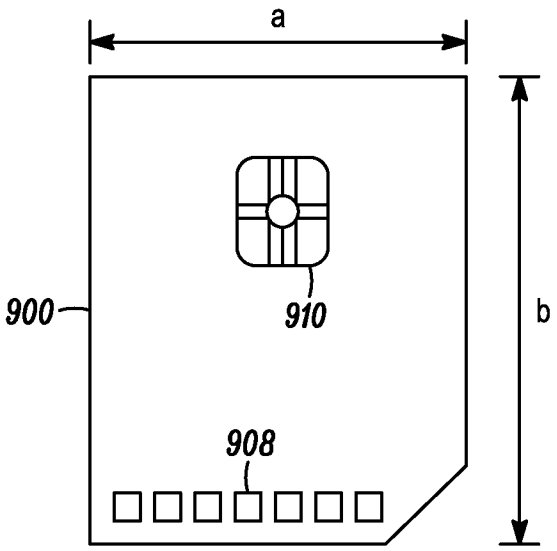


FIG. 9

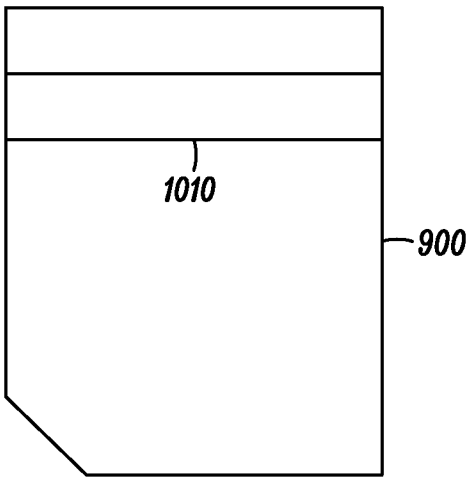


FIG. 10

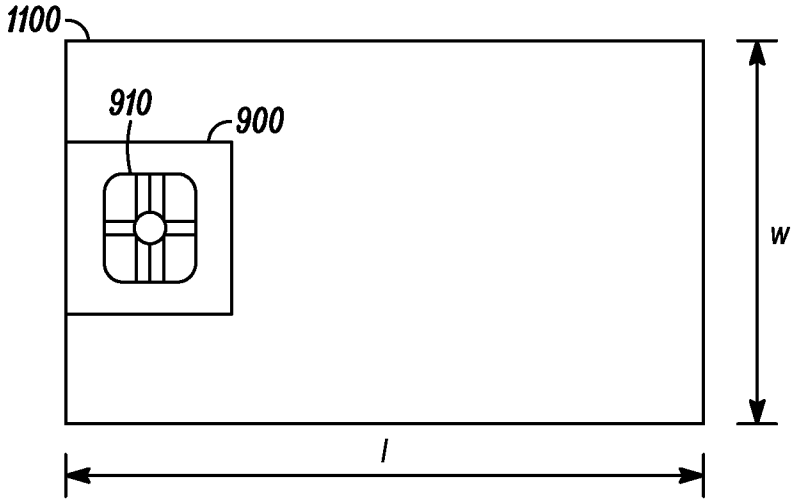


FIG. 11

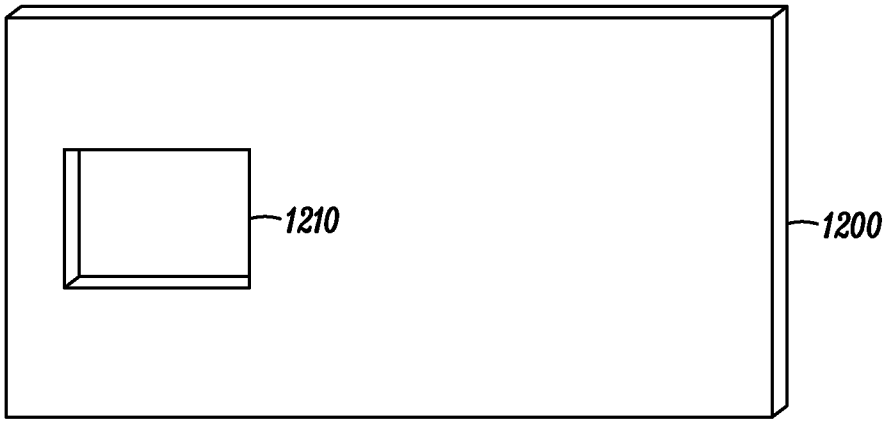


FIG. 12

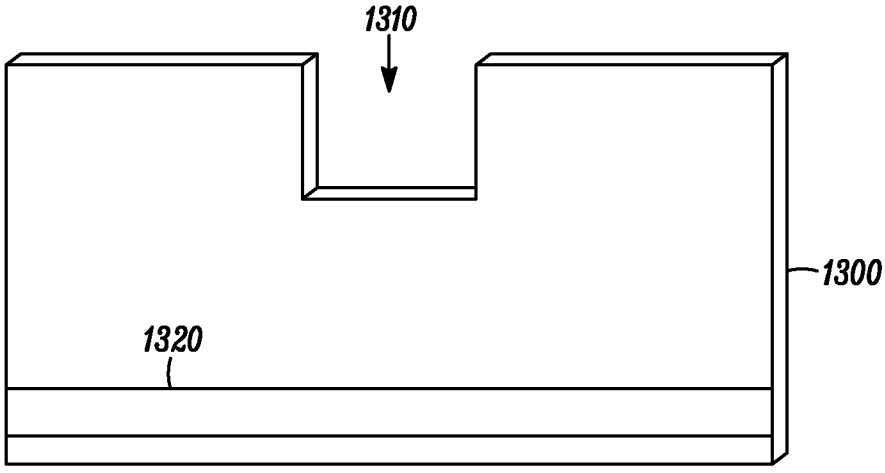


FIG. 13

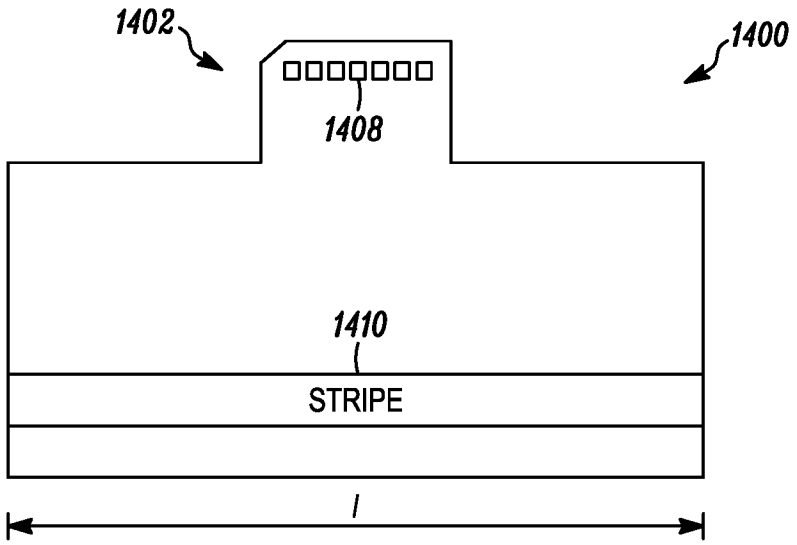


FIG. 14

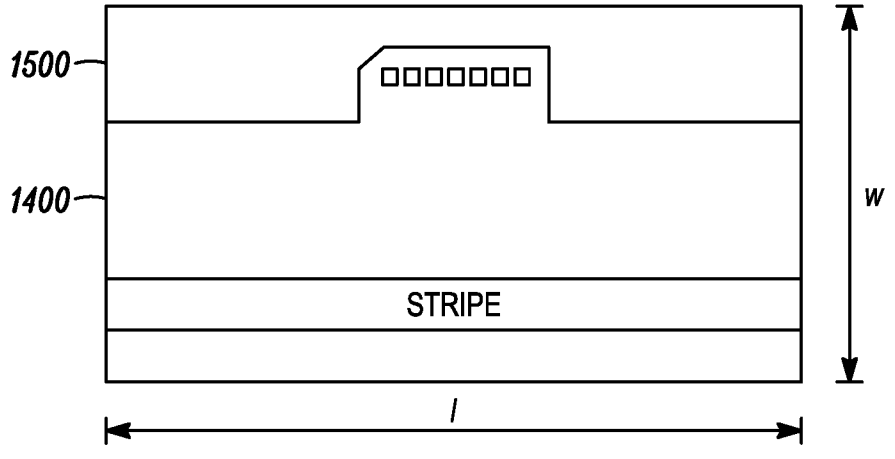


FIG. 15

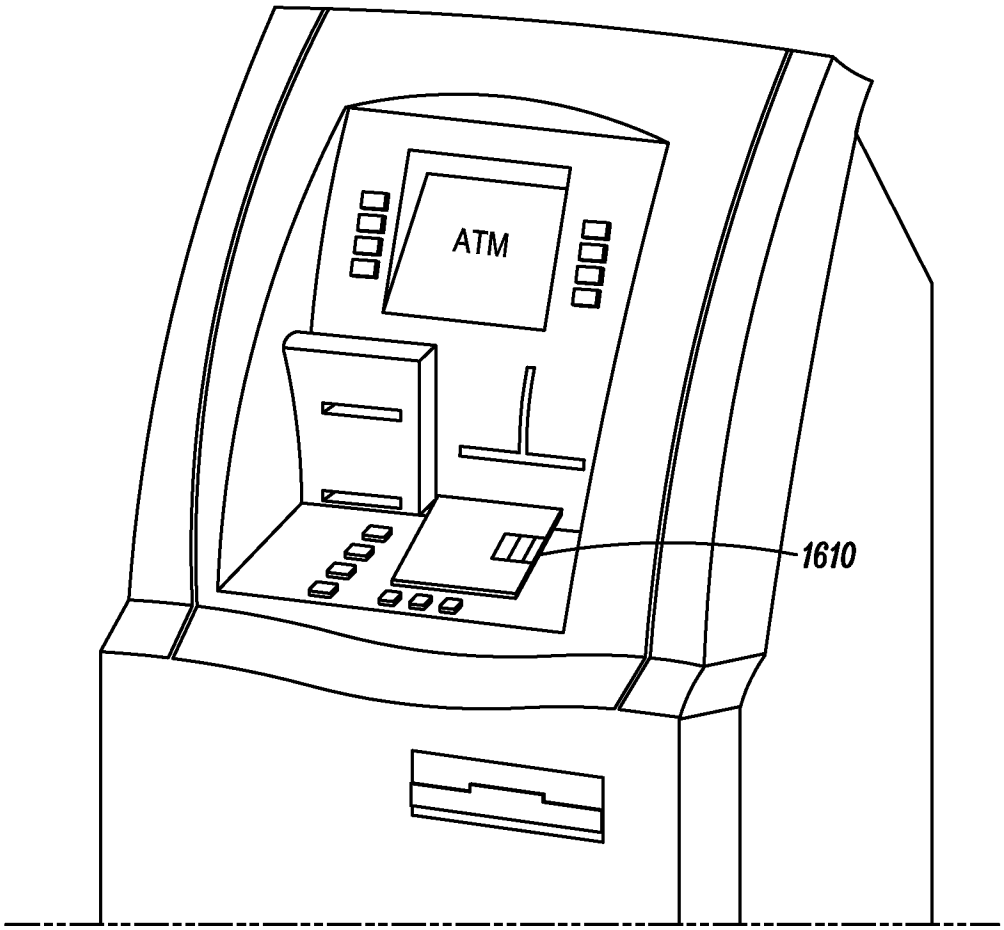


FIG. 16

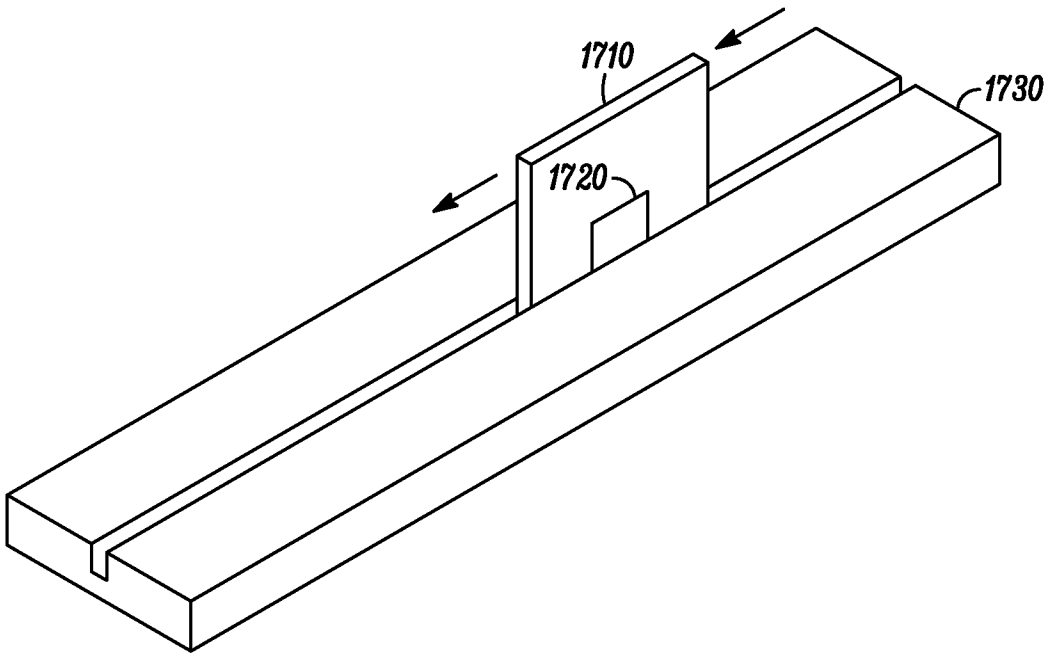


FIG. 17

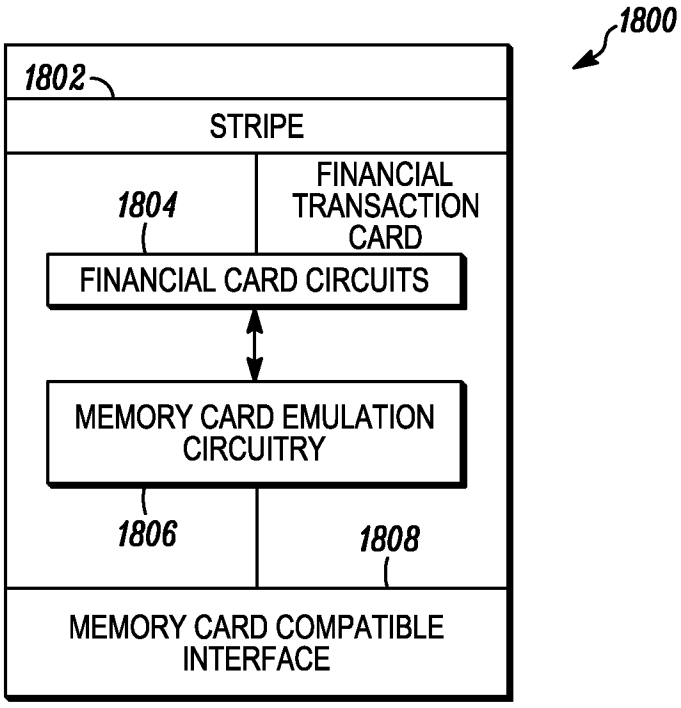

1800
1802
STRIPE
1804
FINANCIAL TRANSACTION CARD
FINANCIAL CARD CIRCUITS
MEMORY CARD EMULATION CIRCUITRY
1806
1808
MEMORY CARD COMPATIBLE INTERFACE

FIG. 18

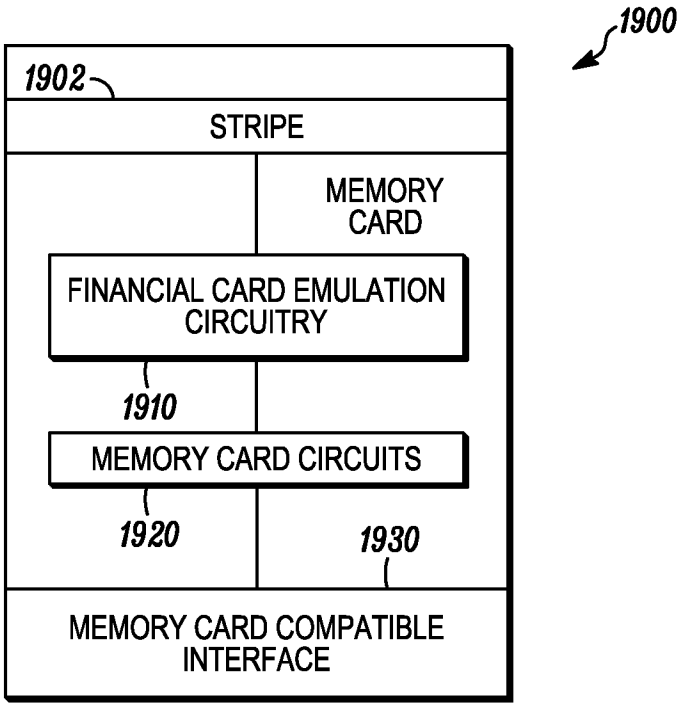

1900
1902
STRIPE
MEMORY CARD
FINANCIAL CARD EMULATION CIRCUITRY
1910
MEMORY CARD CIRCUITS
1920
1930
MEMORY CARD COMPATIBLE INTERFACE

FIG. 19

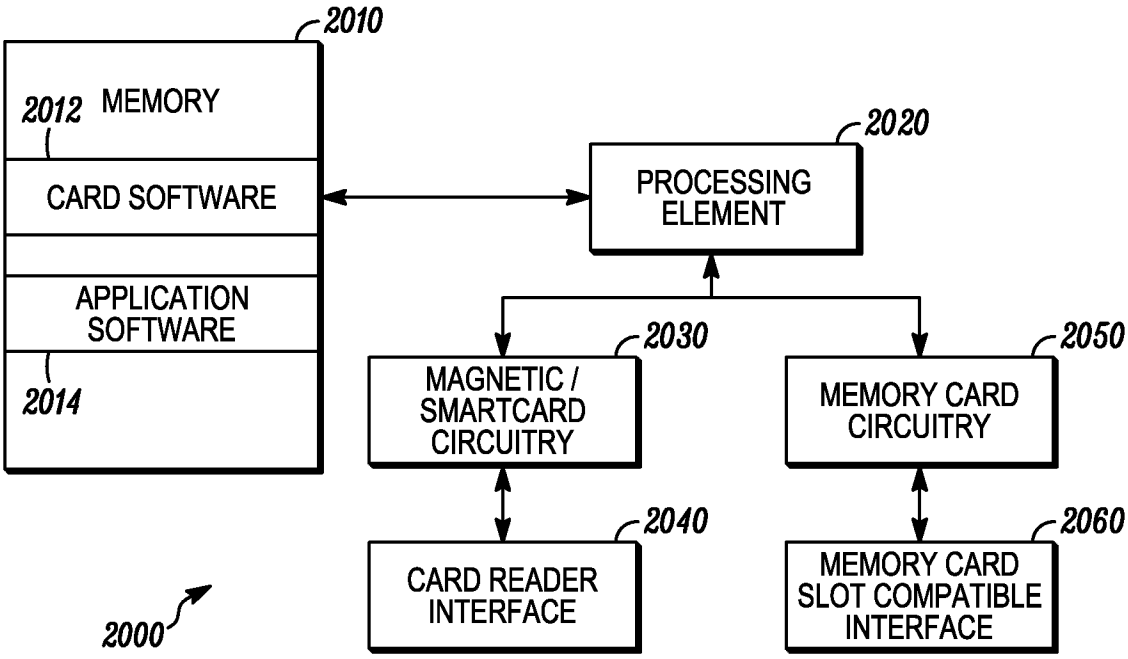

2010
2012 MEMORY
CARD SOFTWARE
APPLICATION SOFTWARE
2014
2020
PROCESSING ELEMENT
2030
MAGNETIC / SMARTCARD CIRCUITRY
2050
MEMORY CARD CIRCUITRY
2040
CARD READER INTERFACE
2060
MEMORY CARD SLOT COMPATIBLE INTERFACE
2000

FIG. 20

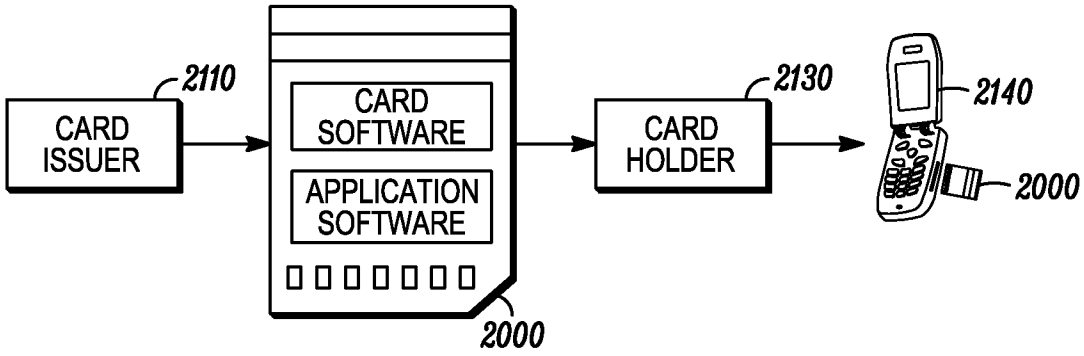

2110
CARD ISSUER
CARD SOFTWARE
APPLICATION SOFTWARE
2000
2130
CARD HOLDER
2140
2000

FIG. 21

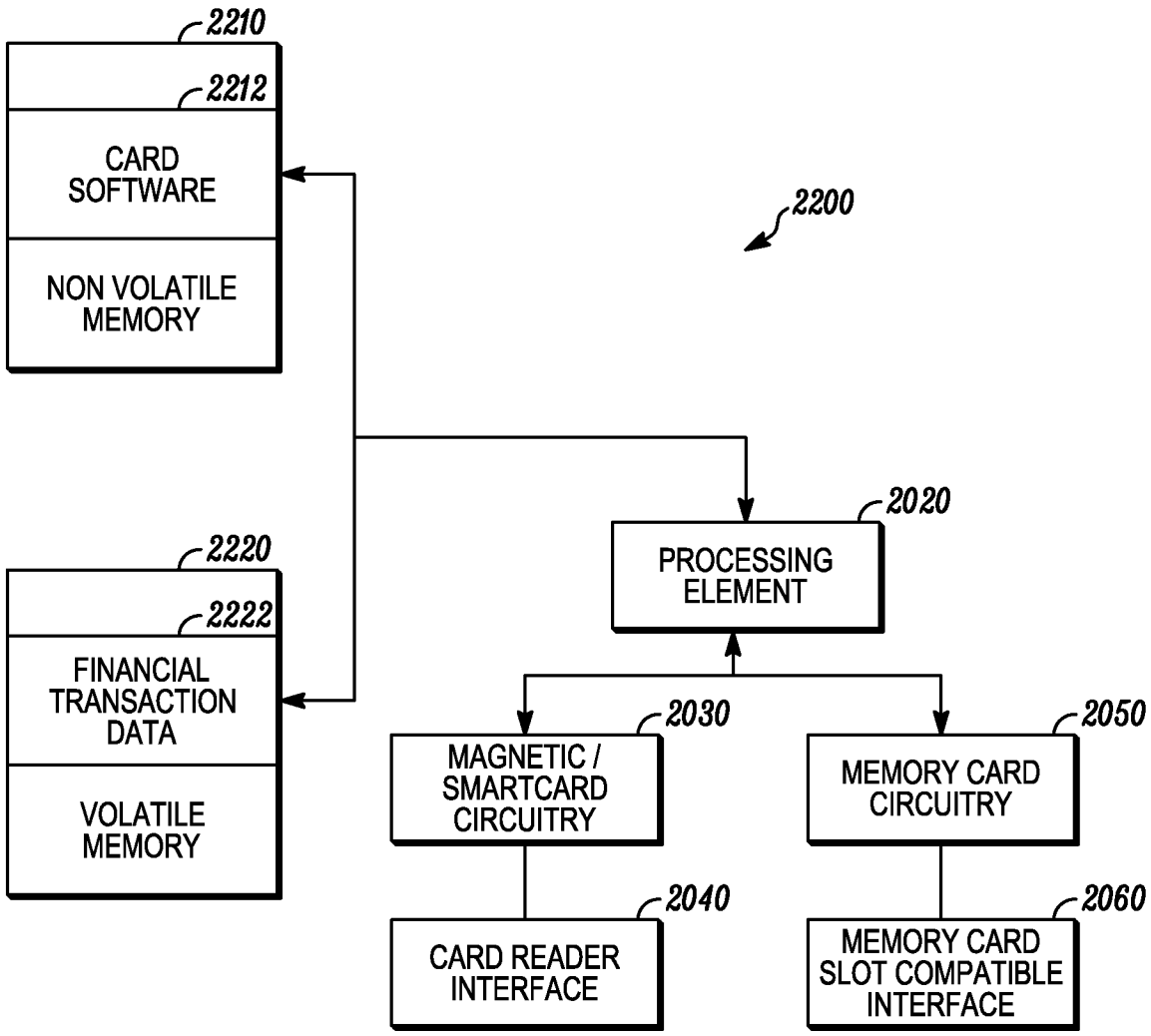

2210
2212
CARD SOFTWARE
NON VOLATILE MEMORY
2200
2020
PROCESSING ELEMENT
2220
2222
FINANCIAL TRANSACTION DATA
VOLATILE MEMORY
2030
MAGNETIC / SMARTCARD CIRCUITRY
2050
MEMORY CARD CIRCUITRY
2040
CARD READER INTERFACE
2060
MEMORY CARD SLOT COMPATIBLE INTERFACE

FIG. 22

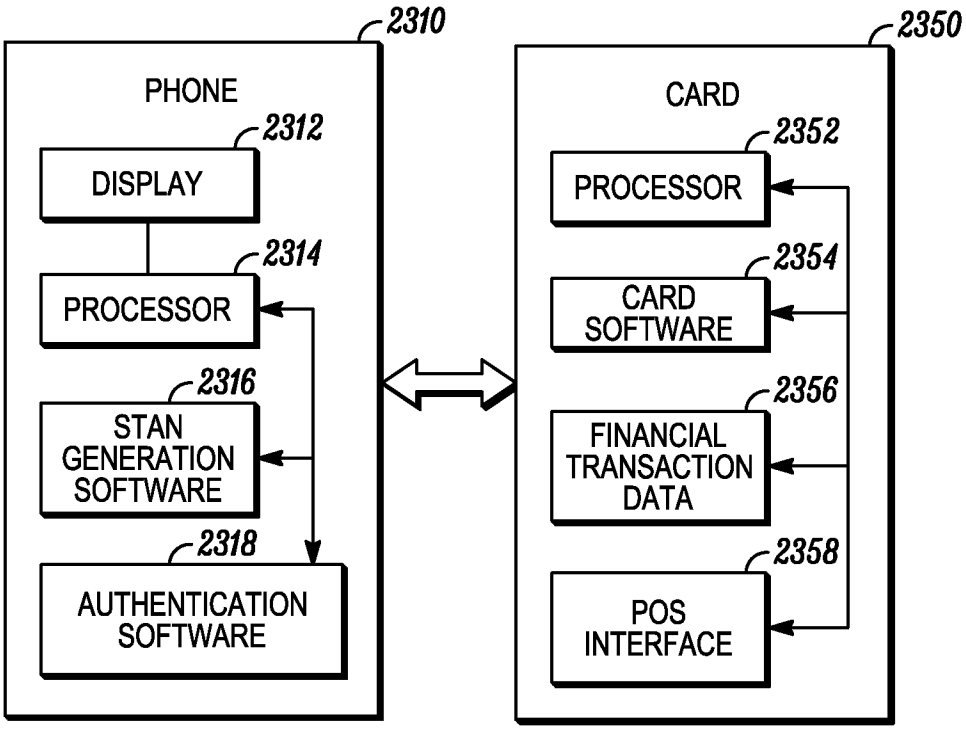

2310
PHONE
2312
DISPLAY
2314
PROCESSOR
2316
STAN GENERATION SOFTWARE
2318
AUTHENTICATION SOFTWARE
2350
CARD
2352
PROCESSOR
2354
CARD SOFTWARE
2356
FINANCIAL TRANSACTION DATA
2358
POS INTERFACE

FIG. 23

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Siva	G.	Narendra	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Portland	OR	US

Mailing Address of Inventor:

Address 1	7180 SW 84th Ave.
Address 2	
City	Portland
State/Province	OR
Postal Code	97223
Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Thomas	N.	Spitzer	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Portland	OR	US

Mailing Address of Inventor:

Address 1	2642 SW Bucharest Ct.
Address 2	
City	Portland
State/Province	OR
Postal Code	97225
Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Prabhakar		Tadepalli	

Residence Information (Select One) ○ US Residency ● Non US Residency Active US Military Service

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

City	Bangalore	Country of Residence [i]	IN

Mailing Address of Inventor:

Address 1	E24 Chaithanya Smaran		
Address 2	Whitefield Hoskote Road		
City	Bangalore	**State/Province**	Ka
Postal Code	560067	**Country** [i]	IN

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	35781		
Email Address	dana.lemoine@tyfone.com	Add Email	Remove Email

Application Information:

Title of the Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION		
Attorney Docket Number	115.001US9.10	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	16	**Suggested Figure for Publication (if any)**	23

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country [i]

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	35781		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	16218733	2018-12-13

Prior Application Status	Patented		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
16218733	Continuation of	15658208	2017-07-24

Prior Application Status	Patented		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
15658208	Continuation of	14948325	2015-11-22

Prior Application Status	Patented		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14948325	Continuation of	14747770	2015-06-23

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16218733	Continuation of	15658208	2017-07-24	10185909	2019-01-22
15658208	Continuation of	14948325	2015-11-22	9715649	2017-07-25
14948325	Continuation of	14747770	2015-06-23	9202156	2015-12-01

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14747770	Continuation of	14680684	2015-04-07	9092708	2015-07-28
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14680684	Continuation of	13592323	2012-08-22	9004361	2015-04-14
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13592323	Continuation of	13304663	2011-11-27	8573494	2013-11-05
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13304663	Continuation of	13114434	2011-05-24	8091786	2012-01-10
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13114434	Continuation of	12941410	2010-11-08	7954715	2011-06-07
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12941410	Continuation of	12539369	2009-08-11	7828214	2010-11-09
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12539369	Continuation of	11063291	2005-02-22	7581678	2009-09-01
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.					Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 — Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Tyfone, Inc.

Mailing Address Information For Applicant:

Address 1	6331 SW Macadam Ave		
Address 2	Suite 251		
City	Portland	**State/Province**	OR
Country	US	Postal Code	97239
Phone Number	503-226-3939	Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	Tyfone, Inc.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	5331 SW Macadam Avenue		
Address 2	Suite 251		
City	Portland	**State/Province**	OR
Country i	US	Postal Code	97239
Phone Number	503-226-3939	Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

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

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	115.001US9.10
	Application Number	
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	40563300
Application Number:	17021347
International Application Number:	
Confirmation Number:	2310
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Correspondence Address:	Tyfone, Inc. Patent Dept. 5331 SW Macadam Avenue Suite 251 Portland OR 97239 US 971-344-0038 dana.lemoine@tyfone.com
Filer:	Dana B. LeMoine/Theresa LeMoine
Filer Authorized By:	Dana B. LeMoine
Attorney Docket Number:	115.001US9.10
Receipt Date:	15-SEP-2020
Filing Date:	
Time Stamp:	15:20:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Other Reference-Patent/App/Search documents	115001TW1_10_20_09.pdf	679590 d4c44dd45308a4525b12fe285ea5a8f3050a3bac	no	6
Warnings:					
Information:					
2	Other Reference-Patent/App/Search documents	13592323_OA_09-30-2014.pdf	210127 22834beeccb23d169323b1dd82328b94dc81ab4d	no	6
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	14680684_OA_05-22-2015.pdf	183496 8821224830a3a6b26276da3a731fec4d05af34f9	no	5
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	14747770_OA_9-25-2015.pdf	252343 e25f78ea602aba2a0dcad781318c2356d7c0ccec	no	7
Warnings:					
Information:					
5	Other Reference-Patent/App/Search documents	14833113_OA_9-24-2015.pdf	338665 27a41bc805cca40b9aa9f1c9e4640239286172d1	no	9
Warnings:					
Information:					
6	Other Reference-Patent/App/Search documents	14866998_OA_11-5-2015.pdf	264194 f393f0fb171c42367775e5533fdb1634f91f9121	no	7
Warnings:					
Information:					
7	Other Reference-Patent/App/Search documents	14929297_OA_09-16-2016.pdf	293790 320bc841d3350c0c085650cf5a952213e1c4ab6d	no	8
Warnings:					
Information:					

8	Other Reference-Patent/App/Search documents	14948325_OA_09-20-2016.pdf	272152 91ef91cf4907027e549f924391fc67b370d7fb4e	no	7
Warnings:					
Information:					
9	Other Reference-Patent/App/Search documents	15658208_OA_04-19-2018.pdf	264339 e988c2050c59bd973b0abead9b6f45ac08d618e0	no	7
Warnings:					
Information:					
10	Other Reference-Patent/App/Search documents	16218733_OA_11-29-2019.pdf	215621 55f4fd7dfeeaf7dfe4d7df118f54b26f3515b85a	no	6
Warnings:					
Information:					
		Total Files Size (in bytes):	2974317		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT6299207

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
SIVA G NARENDRA	06/23/2015
THOMAS N SPITZER	06/23/2015
PRABHAKAR TADEPALLI	06/23/2015

RECEIVING PARTY DATA

Name:	TYFONE, INC.
Street Address:	5331 SW MACADAM AVE
Internal Address:	STE 251
City:	PORTLAND
State/Country:	OREGON
Postal Code:	97239

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	17021347

CORRESPONDENCE DATA

Fax Number:

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 971-344-0038
Email: eofficeaction@appcoll.com
Correspondent Name: TYFONE, INC. PATENT DEPT.
Address Line 1: 5331 SW MACADAM AVENUE
Address Line 2: SUITE 251
Address Line 4: PORTLAND, OREGON 97239

ATTORNEY DOCKET NUMBER:	115.001US9.10
NAME OF SUBMITTER:	DANA B. LEMOINE
SIGNATURE:	/Dana B. LeMoine/
DATE SIGNED:	09/15/2020
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 6

source=115_001US9_3_DEC_Assignment_Siva_Executed#page1.tif
source=115_001US9_3_DEC_Assignment_Siva_Executed#page2.tif
source=115_001US9_3_DEC_Assignment_Tom_Executed#page1.tif
source=115_001US9_3_DEC_Assignment_Tom_Executed#page2.tif
source=115_001US9_3_DEC_Assignment_Prabhakar-signed#page1.tif
source=115_001US9_3_DEC_Assignment_Prabhakar-signed#page2.tif

United States Patent Application

COMBINED DECLARATION AND ASSIGNMENT

Title of Invention: MOBILE DEVICE WITH TIME-VARYING MAGNETIC FIELD

As a below named inventor, I hereby declare that:

This declaration is directed to the attached application.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the application, including the claims.

I am aware of the duty to disclose to the Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, I,

Siva G. Narendra residing at 7180 SW 84th Ave. Portland OR US

made certain new and useful inventions and improvements for which I filed an application for Letters Patent of the United States as identified above;

AND WHEREAS, Tyfone, Inc, a corporation organized and existing under and by virtue of the laws of the State of Oregon, and having an office and place of business at 5331 SW Macadam Ave., Suite 251, Portland, OR 97239 (hereinafter "Assignee"), is desirous of acquiring the entire right, title and interest in and to said inventions, improvements and application and in and to the Letters Patent to be obtained therefore;

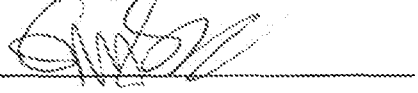
NOW, THEREFORE, to all whom it may concern, be it known that for good and valuable consideration, the receipt and sufficiency whereof is hereby acknowledged, I have sold, assigned, and transferred, and by these presents do sell, assign and transfer unto said Assignee, its successors or assigns, the entire right, title and interest for all countries in and to all inventions and improvements disclosed in the aforesaid application, and in and to the said application, all divisions, continuations, continuations-in-part, or renewals thereof, all Letters Patent which may be granted there from, and all reissues or extensions of such patents, and in and to any and all applications which have been or shall be filed in any foreign countries for Letters Patent on the said inventions and improvements, including an assignment of all rights under the provisions of the International Convention, and all Letters Patent of foreign countries which may be granted there from; and I do hereby authorize and request the Commissioner of Patents and Trademarks to issue any and all United States Letters Patent for the aforesaid inventions and improvements to the said Assignee as the assignee of the entire right, title and interest in and to the same, for the use of the said Assignee, its successors and assigns.

AND, for the consideration aforesaid, I do hereby agree that I and my executors

and legal representatives will make, execute and deliver any and all other instruments in writing including any and all further application papers, affidavits, assignments and other documents, and will communicate to said Assignee, its successors and representatives all facts known to me relating to said improvements and the history thereof and will testify in all legal proceedings and generally do all things which may be necessary or desirable more effectually to secure to and vest in said Assignee, its successors or assigns the entire right, title and interest in and to the said improvements, inventions, applications, Letters Patent, rights, titles, benefits, privileges and advantages hereby sold, assigned and conveyed, or intended so to be.

AND, furthermore, I covenant and agree with said Assignee, its successors and assigns, that no assignment, grant, mortgage, license or other agreement affecting the rights and property herein conveyed has been made to others by me and that full right to convey the same as herein expressed is possessed by me.

Legal name of inventor: Siva G. Narendra

Signature:  Date: June 23, 2015

United States Patent Application

COMBINED DECLARATION AND ASSIGNMENT

Title of Invention: MOBILE DEVICE WITH TIME-VARYING MAGNETIC FIELD

As a below named inventor, I hereby declare that:

This declaration is directed to the attached application.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the application, including the claims.

I am aware of the duty to disclose to the Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, I,

Thomas N. Spitzer residing at 2642 SW Bucharest Ct., Portland OR US

made certain new and useful inventions and improvements for which I filed an application for Letters Patent of the United States as identified above;

AND WHEREAS, Tyfone, Inc, a corporation organized and existing under and by virtue of the laws of the State of Oregon, and having an office and place of business at 5331 SW Macadam Ave., Suite 251, Portland, OR 97239 (hereinafter "Assignee"), is desirous of acquiring the entire right, title and interest in and to said inventions, improvements and application and in and to the Letters Patent to be obtained therefore;

NOW, THEREFORE, to all whom it may concern, be it known that for good and valuable consideration, the receipt and sufficiency whereof is hereby acknowledged, I have sold, assigned, and transferred, and by these presents do sell, assign and transfer unto said Assignee, its successors or assigns, the entire right, title and interest for all countries in and to all inventions and improvements disclosed in the aforesaid application, and in and to the said application, all divisions, continuations, continuations-in-part, or renewals thereof, all Letters Patent which may be granted there from, and all reissues or extensions of such patents, and in and to any and all applications which have been or shall be filed in any foreign countries for Letters Patent on the said inventions and improvements, including an assignment of all rights under the provisions of the International Convention, and all Letters Patent of foreign countries which may be granted there from; and I do hereby authorize and request the Commissioner of Patents and Trademarks to issue any and all United States Letters Patent for the aforesaid inventions and improvements to the said Assignee as the assignee of the entire right, title and interest in and to the same, for the use of the said Assignee, its successors and assigns.

AND, for the consideration aforesaid, I do hereby agree that I and my executors

and legal representatives will make, execute and deliver any and all other instruments in writing including any and all further application papers, affidavits, assignments and other documents, and will communicate to said Assignee, its successors and representatives all facts known to me relating to said improvements and the history thereof and will testify in all legal proceedings and generally do all things which may be necessary or desirable more effectually to secure to and vest in said Assignee, its successors or assigns the entire right, title and interest in and to the said improvements, inventions, applications, Letters Patent, rights, titles, benefits, privileges and advantages hereby sold, assigned and conveyed, or intended so to be.

AND, furthermore, I covenant and agree with said Assignee, its successors and assigns, that no assignment, grant, mortgage, license or other agreement affecting the rights and property herein conveyed has been made to others by me and that full right to convey the same as herein expressed is possessed by me.

Legal name of inventor: Thomas N. Spitzer

Signature: _____ Date: 6/23/15

United States Patent Application

COMBINED DECLARATION AND ASSIGNMENT

Title of Invention: MOBILE DEVICE WITH TIME-VARYING MAGNETIC FIELD

As a below named inventor, I hereby declare that:

This declaration is directed to the attached application.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the application, including the claims.

I am aware of the duty to disclose to the Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, I,

Prabhakar Tadepalli residing at E24 Chaithanya Smaran, Whitefield Hoskote Road, Bangalore, Kannamangala, IN

made certain new and useful inventions and improvements for which I filed an application for Letters Patent of the United States as identified above;

AND WHEREAS, Tyfone, Inc, a corporation organized and existing under and by virtue of the laws of the State of Oregon, and having an office and place of business at 5331 SW Macadam Ave., Suite 251, Portland, OR 97239 (hereinafter “Assignee"), is desirous of acquiring the entire right, title and interest in and to said inventions, improvements and application and in and to the Letters Patent to be obtained therefore;

NOW, THEREFORE, to all whom it may concern, be it known that for good and valuable consideration, the receipt and sufficiency whereof is hereby acknowledged, I have sold, assigned, and transferred, and by these presents do sell, assign and transfer unto said Assignee, its successors or assigns, the entire right, title and interest for all countries in and to all inventions and improvements disclosed in the aforesaid application, and in and to the said application, all divisions, continuations, continuations-in-part, or renewals thereof, all Letters Patent which may be granted there from, and all reissues or extensions of such patents, and in and to any and all applications which have been or shall be filed in any foreign countries for Letters Patent on the said inventions and improvements, including an assignment of all rights under the provisions of the International Convention, and all Letters Patent of foreign countries which may be granted there from; and I do hereby authorize and request the Commissioner of Patents and Trademarks to issue any and all United States Letters Patent for the aforesaid inventions and improvements to the said Assignee as the assignee of the entire right, title and interest in and to the same, for the use of the said Assignee, its successors and assigns.

AND, for the consideration aforesaid, I do hereby agree that I and my executors and legal representatives will make, execute and deliver any and all other instruments in writing including any and all further application papers, affidavits, assignments and other documents, and will communicate to said Assignee, its successors and representatives all facts known to me relating to said improvements and the history thereof and will testify in all legal proceedings and generally do all things which may be necessary or desirable more effectually to secure to and vest in said Assignee, its successors or assigns the entire right, title and interest in and to the said improvements, inventions, applications, Letters Patent, rights, titles, benefits, privileges and advantages hereby sold, assigned and conveyed, or intended so to be.

AND, furthermore, I covenant and agree with said Assignee, its successors and assigns, that no assignment, grant, mortgage, license or other agreement affecting the rights and property herein conveyed has been made to others by me and that full right to convey the same as herein expressed is possessed by me.

Legal name of inventor: Prabhakar Tadepalli

Signature: _____ Date: June 23, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/021,347	09/15/2020		1720	115.001US9.10	18	3

CONFIRMATION NO. 2310

FILING RECEIPT

35781
Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239

OC000000120349493

Date Mailed: 10/02/2020

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Siva G. Narendra, Portland, OR;
Thomas N. Spitzer, Portland, OR;
Prabhakar Tadepalli, Bangalore, INDIA;

Applicant(s)

Tyfone, Inc., Portland, OR;

Assignment For Published Patent Application

Tyfone, Inc., Portland, OR

Power of Attorney: The patent practitioners associated with Customer Number 35781

Domestic Priority data as claimed by applicant

This application is a CON of 16/218,733 12/13/2018 PAT 10803370
which is a CON of 15/658,208 07/24/2017 PAT 10185909
which is a CON of 14/948,325 11/22/2015 PAT 9715649
which is a CON of 14/747,770 06/23/2015 PAT 9202156
which is a CON of 14/680,684 04/07/2015 PAT 9092708
which is a CON of 13/592,323 08/22/2012 PAT 9004361
which is a CON of 13/304,663 11/27/2011 PAT 8573494
which is a CON of 13/114,434 05/24/2011 PAT 8091786
which is a CON of 12/941,410 11/08/2010 PAT 7954715
which is a CON of 12/539,369 08/11/2009 PAT 7828214
which is a CON of 11/063,291 02/22/2005 PAT 7581678

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 10/01/2020
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/021,347**
Projected Publication Date: 01/07/2021
Non-Publication Request: No
Early Publication Request: No
Title

MOBILE PHONE WITH MAGNETIC CARD EMULATION

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign

patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/021,347

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	660
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760
TOTAL CLAIMS (37 CFR 1.16(i))	18 minus 20 =	*			OR	x 100 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 460 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1720

APPLICATION AS AMENDED - PART II

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/021,347	09/15/2020	Siva G. Narendra	115.001US9.10

CONFIRMATION NO. 2310

PUBLICATION NOTICE

35781
Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239



Title:MOBILE PHONE WITH MAGNETIC CARD EMULATION

Publication No.US-2021-0004655-A1
Publication Date:01/07/2021

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/021,347	09/15/2020	Siva G. Narendra	115.001US9.10	2310

35781 7590 06/25/2021

Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239

EXAMINER	
HAUPT, KRISTY A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
06/25/2021	ELECTRONIC

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

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

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

docketing@ghmip.com

Office Action Summary	Application No. 17/021,347	Applicant(s) Narendra et al.	
	Examiner KRISTY A HAUPT	Art Unit 2876	AIA (FITF) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☑ Responsive to communication(s) filed on 9/15/20.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-18 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-18 is/are rejected.

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

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

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

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 9/15/20 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 9/15/20.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This office action is in response to application 17/021,347 filed 9/15/20. Claims 1-18 are pending with claims 1, 7 and 13 in independent form.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP § 2146 *et seq.* for applications not subject

to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

2. Claims 1-18 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-18 of U.S. Patent No. 9,715,649 in view of Daughty et al. US 2011/0240748 A1. Although the claims at issue are not identical, they are not patentably distinct from each other because all the currently claimed limitations are found recited within the narrower '649 claims. The '649 claims recite a cellular telephone with a memory to hold transaction data, a conductor that can produce a time-varying magnetic field to emulate a magnetic stripe of a card and circuitry such as a current driver to control the time-varying magnetic field.

The '649 patent fails to specifically teach a processor to control the driver along with the types of transactions (POS, access, credit card).

However, Daughty teaches a processor to control the driver along with the types of transactions the time-varying magnetic field represents (as shown in the 102 rejection below).

Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of the '649 patent to include the teachings of Daughty, as an obvious matter of design choice where it is well-known that a device to emulate a magnetic stripe would include a processor and where the reading

of magnetic stripes related to transactions and user accounts are commonly used in credit card transactions at POS devices or for access control (paragraph 0008).

Claim Rejections - 35 USC § 102

3. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

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

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claim(s) 1-18 is/are rejected under pre-AIA 35 U.S.C. 102(a) as being anticipated by Doughty et al. US 2011/0240748 A1.

Doughty teaches:

With respect to claim 1, A mobile phone comprising: a memory to hold transaction data for repeated use in a plurality of transactions (fig. 3, 312; paragraph 0009); a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions (fig. 3, 308; paragraph 0051); a driver to excite the current carrying conductor (fig. 5B, control circuit 554; paragraph 0051); and a processor coupled to control the driver (fig. 3, 314).

With respect to claim 2, The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction (paragraphs 0008, 0095-0097).

With respect to claim 3, The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction (paragraphs 0008, 0038).

With respect to claim 4, The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction (paragraphs 0008, 0038).

With respect to claim 5, The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card (paragraph 0051).

With respect to claim 6, The mobile phone of claim 1 wherein the driver comprises a current driver (paragraph 0051).

With respect to clam 7, A mobile phone comprising: a memory to hold transaction data for repeated use in a plurality of transactions (fig. 3, 312; paragraph 0009); a conductor that when excited by a reversing polarity current produces a time-varying magnetic field that represents the transaction data in the plurality of transactions (fig. 3, 308; paragraph 0051); a driver to excite the conductor (fig. 5B, control circuit 554; paragraph 0051); and a processor coupled to control the driver (fig. 3, 314).

With respect to claim 8, The mobile phone of claim 7 wherein the time-varying magnetic field represents a point-of-sale transaction (paragraphs 0008, 0095-0097).

With respect to claim 9, The mobile phone of claim 7 wherein the time-varying magnetic field represents an access transaction (paragraphs 0008, 0038).

With respect to claim 10, The mobile phone of claim 7 wherein the time-varying magnetic field represents a credit card transaction (paragraphs 0008, 0038).

With respect to claim 11, The mobile phone of claim 7 wherein the time-varying magnetic field emulates a swipe of a magnetic card (paragraph 0051).

With respect to claim 12, The mobile phone of claim 7 wherein the driver comprises a current driver (paragraph 0051).

With respect to claim 13, A mobile phone comprising: a memory to hold transaction data for repeated use in a plurality of transactions (fig. 3, 312; paragraph 0009); a conductor that when excited by a reversing polarity current that varies in amplitude produces a time-varying magnetic field that represents the transaction data in the plurality of transactions (fig. 3, 308; paragraph 0051); a driver to excite the conductor (fig. 5B, control circuit 554; paragraph 0051); and a processor coupled to control the driver (fig. 3, 314).

With respect to claim 14, The mobile phone of claim 13 wherein the time-varying magnetic field represents a point-of-sale transaction (paragraphs 0008, 0038, 0095-0097).

With respect to claim 15, The mobile phone of claim 13 wherein the time-varying magnetic field represents an access transaction (paragraphs 0008, 0038).

With respect to claim 16, The mobile phone of claim 13 wherein the time-varying magnetic field represents a credit card transaction (paragraphs 0008, 0038).

With respect to claim 17, The mobile phone of claim 13 wherein the time-varying magnetic field emulates a swipe of a magnetic card (paragraph 0051).

With respect to claim 18, The mobile phone of claim 13 wherein the driver comprises a current driver (paragraph 0051).

It is noted that "mobile phone" for purposes of claims 1-18 is a preamble limitation only, not brought to life within the body of the claims, however paragraph 0046 teaches the components are mounted on a substrate that can be integrated into different devices, such as a person communication device, a PDS, a telecommunications device, a computer, a watch, etc.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KRISTY A HAUPT whose telephone number is (571)272-8545 and email address is kristy.haupt@uspto.gov. The examiner can normally be reached on Mon-Sun 5:30 AM- 10PM; Flex during day.

If all attempts to reach the examiner ***by telephone and email*** are unsuccessful, the examiner's supervisor, Michael Lee can be reached on 5712722398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/KRISTY A HAUPT/
Primary Examiner, Art Unit 2876

KAH

Notice of References Cited	Application/Control No. 17/021,347	Applicant(s)/Patent Under Reexamination Narendra et al.	
	Examiner KRISTY A HAUPT	Art Unit 2876	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20110240748-A1	10-2011	Doughty; Ralph O.	G06Q20/40145	235/492
*	B	US-9715649-B2	07-2017	Narendra; Siva G.	G06K19/07741	1/1
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/021,347	Narendra et al.
	Examiner	Art Unit
	KRISTY A HAUPT	2876

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

CLAIMS

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

CLAIM		DATE								
Final	Original	06/21/2021								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/021,347	Narendra et al.
	Examiner	Art Unit
	KRISTY A HAUPT	2876

CPC - Searched*		
Symbol	Date	Examiner
G06K19/06187; G06K19/07; G06K19/0703; G06K19/0723; G06K19/0727; G06K19/073; G06K19/07741; G06K19/07758; G06K19/07762; G06Q20/204; G06Q20/327; G06Q20/341; G06Q20/353 (text search)	06/21/2021	KAH

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search	06/21/2021	KAH
East search	06/21/2021	KAH

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/KRISTY A HAUPT/ Primary Examiner, Art Unit 2876	

Bibliographic Data

Application No: 17/021,347

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /KRISTY A HAUPT/ KAH

Examiner's Signature Initials

Title: MOBILE PHONE WITH MAGNETIC CARD EMULATION

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/15/2020	235	2876	115.001US9.10
RULE			

APPLICANTS

Tyfone, Inc., Portland, OR,

INVENTORS

Siva G. Narendra, Portland, OR, UNITED STATES

Thomas N. Spitzer, Portland, OR, UNITED STATES

Prabhakar Tadepalli, Bangalore, INDIA

CONTINUING DATA

This application is a CON of 16218733 12/13/2018 PAT 10803370

16218733 is a CON of 15658208 07/24/2017 PAT 10185909

15658208 is a CON of 14948325 11/22/2015 PAT 9715649

14948325 is a CON of 14747770 06/23/2015 PAT 9202156

14747770 is a CON of 14680684 04/07/2015 PAT 9092708

14680684 is a CON of 13592323 08/22/2012 PAT 9004361

13592323 is a CON of 13304663 11/27/2011 PAT 8573494

13304663 is a CON of 13114434 05/24/2011 PAT 8091786

13114434 is a CON of 12941410 11/08/2010 PAT 7954715

12941410 is a CON of 12539369 08/11/2009 PAT 7828214

12539369 is a CON of 11063291 02/22/2005 PAT 7581678

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

10/01/2020

STATE OR COUNTRY

UNITED STATES

ADDRESS

Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239
UNITED STATES

FILING FEE RECEIVED

$1,720

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

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	/KRISTY A HAUPT/
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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	/KRISTY A HAUPT/
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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
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.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
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.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
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.		☒

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	T5
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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	/KRISTY A HAUPT/
	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	/KRISTY A HAUPT/	Date Considered	06/21/2021

*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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	153,403	G06K19/06206.cpc. or H04M1/72412.cpc. or G06K7/0008.cpc. or G06K19/06187.cpc. or G06K19/07.cpc. or G06K19/0703.cpc. or G06K19/0723.cpc. or G06K19/0727.cpc. or G06K19/073.cpc. or G06K19/07741.cpc. or G06K19/07758.cpc. or G06K19/07762.cpc. or G06Q20/204.cpc. or G06Q20/327.cpc. or G06Q20/341.cpc. or G06Q20/353.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 09:19
S2	720	(tyfone.in. near inc.in.) or (tyfone.as. near inc.as.) or (narendra.in. near siva.in.) or (spitzer.in. near thomas.in.) or (tadepalli.in. near prabhakar.in.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 09:43
S4	69	("6592044" | "6594759" | "6598031" | "6607127" | "6609654" | "6631849" | "6636833" | "6669487" | "6705520" | "6712277" | "6715679" | "6721196" | "6747547" | "6764005" | "6769607" | "6805288" | "6811082" | "6836843" | "6857566" | "6882900" | "6883718" | "6905072" | "6907123" | "6908030" | "6925568" | "6937526" | "6952788" | "6995651" | "7059520" | "7088246" | "7185146" | "7213766" | "7221473" | "7281101" | "7295790" | "7333062" | "7350717" | "7353993" | "7410102" | "7493484" | "7558107" | "7558110" | "7581678" | "7607580" | "7673080" | "7716082" | "7789303" | "7792516" | "7828214" | "7898994" | "7933571" | "7941197" | "7948356" | "7954715" | "7954716" | "7954717" | "7961101" | "7991158" | "8072331" | "8082575" | "8083145" | "8091786" | "8103881" | "9092708" | "9202156" | "9715649"	US-PGPUB; USPAT	OR	ON	2021/06/21 10:43

		| "RE41352" | "RE41471" | "RE42254").PN.				
S3	211	("20010002035" | "20010006902" | "20010013551" | "20010034246" | "20020007434" | "20020025796" | "20020043566" | "20020044043" | "20020095588" | "20020096570" | "20020099665" | "20020130187" | "20020138422" | "20020138735" | "20020139849" | "20020148892" | "20020153424" | "20020158747" | "20020178124" | "20020180584" | "20020186845" | "20030025939" | "20030028481" | "20030038177" | "20030052168" | "20030057278" | "20030061168" | "20030079096" | "20030080183" | "20030084220" | "20030085288" | "20030115126" | "20030128124" | "20030159050" | "20030200180" | "20030209604" | "20030218066" | "20030220876" | "20030231550" | "20040006654" | "20040027881" | "20040030660" | "20040035942" | "20040050930" | "20040058705" | "20040064612" | "20040065733" | "20040077372" | "20040087339" | "20040094624" | "20040122685" | "20040133787" | "20040162932" | "20040177045" | "20040188519" | "20040199469" | "20040227859" | "20040243785" | "20040243806" | "20040251303" | "20040255145" | "20050006462" | "20050017068" | "20050022002" | "20050029349" | "20050038736" | "20050039027" | "20050044044" | "20050050367" | "20050052924" | "20050060586" | "20050071282" | "20050077349" | "20050092830" | "20050108096" | "20050109838" | "20050116026" | "20050121512" | "20050122209" | "20050127164" | "20050127166" | "20050133606" | "20050136964" | "20050168339" | "20050177724" | "20050197859" | "20050204077" | "20050204092" | "20050212657" | "20050223143" | "20050224589" | "20050240778" | "20050246546" | "20050253687" | "20050258245" | "20050268058" | "20050268330" | "20060011731" | "20060027655" | "20060045555" |	US-PGPUB; USPAT	OR	ON	2021/06/21 10:43

"20060077039" | "20060097851" |
"20060124755" | "20060169778" |
"20060172606" | "20060186209" |
"20060219776" | "20060226217" |
"20060268764" | "20060279413" |
"20070033334" | "20070076877" |
"20070108280" | "20070110404" |
"20070145135" | "20070145152" |
"20070195458" | "20070205864" |
"20070257797" | "20070293202" |
"20080046649" | "20080065830" |
"20080068173" | "20080073436" |
"20080136619" | "20080147950" |
"20080148077" | "20080153416" |
"20080186174" | "20080214111" |
"20080244208" | "20080279381" |
"20080311849" | "20080318535" |
"20090065571" | "20090065572" |
"20090069049" | "20090069050" |
"20090069051" | "20090069052" |
"20090070272" | "20090070691" |
"20090070861" | "20090108063" |
"20090150610" | "20090152361" |
"20090199283" | "20090250521" |
"20090265552" | "20090270127" |
"20090290582" | "20090298540" |
"20090315667" | "20100033307" |
"20100033310" | "20100049878" |
"20100213265" | "20110000960" |
"20110053644" | "20110073663" |
"20110073665" | "20110077052" |
"20110110404" | "20110171996" |
"20110180610" | "20110220726" |
"20110223972" | "20110240748" |
"20110269438" | "20110271044" |
"20110272468" | "20110272469" |
"4701601" | "4786791" | "4791283" |
"4864109" | "5212478" | "5378887" |
"5386106" | "5537584" | "5574273" |
"5585787" | "5629981" | "5700037" |
"5710421" | "5834756" | "5909491" |
"5940510" | "5949880" | "5952641" |
"5955961" | "6016476" | "6021944" |
"6039260" | "6045043" | "6068184" |
"6105013" | "6182891" | "6189786" |
"6206293" | "6219439" | "6223954" |
"6223984" | "6237095" | "6250557" |
"6315195" | "6402029" | "6450407" |
"6481623" | "6568600" |
"6588660").PN.

S5	1	("9715649").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/06/21 11:09
S6	77	((phone device apparatus) with ((memory stor$3) with (transaction))) and ((phone device apparatus) with (time near3 (vary varying)) with ((magnetic$3 "EM" electromagnet$3) adj3 field))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:21
S9	57	S2 and S6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:22
S8	73	S1 and S6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:22
S7	47,538	S1 and "7"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:22
S10	1	("20110240748").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/06/21 11:34
S11	19,494	(time near3 (vary varying)) near5 (magnetic magnet ("em" near2 field))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:36
S12	3,546,237	((mobile portable cellular smart) adj2 (phone device apparatus))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:37

S13	3,342	S11 and S12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:38
S14	176	S1 and S13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:39
S15	66	S2 and S13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:40
S18	99	S1 and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:43
S17	182	S13 and S16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:43
S16	316,681	((memory stor$3) with (transaction))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:43
S19	1	("20050182710").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/06/21 11:50
S20	1	("6016476").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/06/21 11:53

S21	16	S3 and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:55
S23	79	S22 not S2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:58
S22	79	((mobile portable cellular smart) adj2 (phone device apparatus)) with (magnetic$4 adj1 stripe adj3 emulat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 11:58
S24	1	("20050168339").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/06/21 12:33
S25	22	((memory "sim") adj1 card) with (transaction with ((magnetic mag) adj2 stripe))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 12:37
L1	36	(memory and transaction and current and time and vary$3 and magnetic and field and driver and processor).dm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 14:19
L4	47	(memory and transaction and current and time and vary$3 and magnetic and field).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 14:20
L3	1	1 and 2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2021/06/21 14:20

			DERWENT; IBM_TDB			
L2	720	(tyfone.in. near inc.in.) or (tyfone.as. near inc.as.) or (narendra.in. near siva.in.) or (spitzer.in. near thomas.in.) or (tadepalli.in. near prabhakar.in.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 14:20
L5	9	2 and 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/06/21 14:21

6/21/2021 3:03:40 PM
C:\Users\khaupt\Documents\EAST\Workspaces\17 021 347.wsp

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17/021,347
	Filing Date	Sep 15, 2020
	First Named Inventor	Siva Narendra
	Art Unit	2887
	Examiner Name	
	Attorney Docket Number	115.001US9.10

U.S.PATENTS

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

U.S.PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	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]

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
		Final Office Action notified December 26, 2007 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Non-Final Office Action notified December 11, 2008 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Non-Final Office Action notified February 26, 2007 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Non-Final Office Action notified July 08, 2010 for U.S. Patent Application No. 12/539,369 (Docket No. 115.1US2).	

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17/021,347
	Filing Date	Sep 15, 2020
	First Named Inventor	Siva Narendra
	Art Unit	2887
	Examiner Name	
	Attorney Docket Number	115.001US9.10

		Non-Final Office Action notified July 23, 2008 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Notice of Allowance notified April 14, 2011 for U.S. Patent Application No. 12/941,410 (Docket No. 115.001US2.1).	
		Notice of Allowance notified July 10, 2009 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Notice of Allowance notified September 30, 2010 for U.S. Patent Application No. 12/539,369 (Docket No. 115.001US2).	
		Notice of Allowance notified September 30, 2010 for U.S. Patent Application No. 12/539,369 (Docket No. 115.1US2).	

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17/021,347
	Filing Date	Sep 15, 2020
	First Named Inventor	Siva Narendra
	Art Unit	2887
	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.

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

☐ None

SIGNATURE

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

Signature	/Usman Mughal/	Date (YYYY-MM-DD)	2021-06-29
Name/Print	Usman A. Mughal	Registration Number	62887

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.**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: **Siva Narendra**	Examiner: **Kristy A. Haupt**
Application No.: 17/021,347	Art Group: 2876
Filed: September 15, 2020	Confirmation No.: 2310
For: MOBILE PHONE WITH MAGNETIC CARD EMULATION	Docket No.: 115.001US9.10

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

INFORMATION DISCLOSURE STATEMENT

Applicants respectfully request that this Information Disclosure Statement be entered and the documents listed on the attached form be considered by the Examiner and made of record. Pursuant to the provisions of MPEP 609, Applicants request that a copy of the form, initialed as being considered by the Examiner, be returned to the Applicants with the next official communication.

Pursuant to 37 CFR § 1.97(b), it is believed that no fee or statement is required with the Information Disclosure Statement. However, if an Office Action on the merits has been mailed, the Commissioner is hereby authorized to charge the required fees to Deposit Account No. 50-6613 in order to have this Information Disclosure Statement considered.

Pursuant to 37 CFR § 1.98(d), copies of the listed documents are not provided as these references were previously cited by or submitted to the U.S. Patent Office in connection with Applicants' prior U.S. Application Nos.: 11/063,291, filed February 22, 2005, and 12/539,369, filed August 11, 2009, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

Examiner Haupt is invited to contact the Applicants' Representative at the below-listed telephone number if there are any questions regarding this communication.

Pursuant to 37 C.F.R. § 1.136(a)(3), Applicants request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 C.F.R. § 1.16 and § 1.17, to Deposit Account No. 50-6613.

Respectfully submitted,
GREEN, HOWARD, & MUGHAL, LLP

06/29/21
Date

/Usman Mughal/
Usman Mughal
Reg. No. 62887
Attorney for Applicants

5 Centerpointe Drive, Suite 400
Lake Oswego, OR 97035
(503) 968-8233
docketing@ghmip.com

Electronic Patent Application Fee Transmittal

Application Number:	17021347
Filing Date:	15-Sep-2020
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Filer:	Usman Mughal/Katherine Campbell
Attorney Docket Number:	115.001US9.10

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	130	130
		Total in USD ($)		**130**

Electronic Acknowledgement Receipt

EFS ID:	43119197
Application Number:	17021347
International Application Number:	
Confirmation Number:	2310
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Customer Number:	35781
Filer:	Usman Mughal/Katherine Campbell
Filer Authorized By:	Usman Mughal
Attorney Docket Number:	115.001US9.10
Receipt Date:	29-JUN-2021
Filing Date:	15-SEP-2020
Time Stamp:	19:46:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$130
RAM confirmation Number	E20216SJ47224963
Deposit Account	
Authorized User	

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	115-001US9-10_IDS.pdf	74094 b311e1327a224f67e266888426a12cccfe6b61b3	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Transmittal Letter	115-001US9-10_IDS_Transmittal.pdf	22876 080290d4b8f7efaf14bc9c469e0b0081ff23fac5	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30624 64f17afd4b4cc0ca069134d5e78f31934a071c23	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	127594		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: **Siva Narendra**	Examiner: **Kristy A. Haupt**
Application No.: 17/021,347	Art Group: 2876
Filed: September 15, 2020	Confirmation No.: 2310
For: MOBILE PHONE WITH MAGNETIC CARD EMULATION	Docket No.: 115.001US9.10

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

AMENDMENT UNDER 37 C.F.R. § 1.111

Dear Examiner:

This Amendment is in response to the Non-Final Office Action notified June 25, 2021. Applicants respectfully request the Examiner to enter this Amendment and consider the following remarks.

SPECIFICATION AMENDMENT

Please add the following paragraph before the first paragraph of the application:

CLAIM FOR PRIORITY

[0001] This application is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 16/218,733, filed December 13, 2018, now issued as U.S. Patent No. 10,803,370 on October 13, 2020, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 15/658,208, filed July 24, 2017, now issued as U.S. Patent No. 10,185,909 on January 22, 2019, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 14/948,325, filed November 22, 2015, now issued as U.S. Patent No. 9,715,649 on July 25, 2017, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 14/747,770, filed June 23, 2015, now issued as U.S. Patent No. 9,202,156 on December 01, 2015 which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 14/680,684, filed April 07, 2015, now issued as U.S. Patent No. 9,092,708 on July 28, 2015 which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 13/592,323, filed August 22, 2012, now issued as U.S. Patent No. 9,004,361 on April 14, 2015, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 13/304,663, filed November 27, 2011, now issued as U.S. Patent No. 8,573,494 on November 05, 2013, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 13/114,434, filed May 24, 2011, now issued as U.S. Patent No. 8,091,786, on January 10, 2012, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 12/941,410, filed November 08, 2010, now issued as U.S. Patent No. 7,954,715 on June 07, 2011, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 12/539,369, filed August 11, 2009, now issued as U.S. Patent No. 7,828,214 on November 09, 2010, which is a continuation of, and claims the benefit of priority to U.S. Patent Application No. 11/063,291, filed February 22, 2005, now issued as U.S. Patent No. 7,581,678 on September 01, 2009, and which is incorporated by reference in entirety.

LISTING OF CLAIMS

1. (**Currently Amended**) A mobile phone comprising:

a memory to hold transaction data for ~~repeated~~ use in a plurality of transactions;

a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;

a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;

a driver to excite the current carrying conductor; and

a processor coupled to control the driver.

2. (Original) The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.

3. (Original) The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.

4. (Original) The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.

5. (Original) The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.

6. (Original) The mobile phone of claim 1 wherein the driver comprises a current driver.

7. (**Currently Amended**) A mobile phone comprising:

a memory to hold transaction data for ~~repeated~~ use in a plurality of transactions;

a conductor that when excited by a reversing polarity current produces a time-varying magnetic field that represents the transaction data in the plurality of transactions;

a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;

a driver to excite the conductor; and

a processor coupled to control the driver.

8. (Original) The mobile phone of claim 7 wherein the time-varying magnetic field represents a point-of-sale transaction.

9. (Original) The mobile phone of claim 7 wherein the time-varying magnetic field represents an access transaction.

10. (Original) The mobile phone of claim 7 wherein the time-varying magnetic field represents a credit card transaction.

11. (Original) The mobile phone of claim 7 wherein the time-varying magnetic field emulates a swipe of a magnetic card.

12. (Original) The mobile phone of claim 7 wherein the driver comprises a current driver.

13. **(Currently Amended)** A mobile phone comprising:

a memory to hold transaction data for ~~repeated~~ use in a plurality of transactions;

a conductor that when excited by a reversing polarity current that varies in amplitude produces a time-varying magnetic field that represents the transaction data in the plurality of transactions;

a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;

a driver to excite the conductor; and

a processor coupled to control the driver.

14. (Original) The mobile phone of claim 13 wherein the time-varying magnetic field represents a point-of-sale transaction.

15. (Original) The mobile phone of claim 13 wherein the time-varying magnetic field represents an access transaction.

16. (Original) The mobile phone of claim 13 wherein the time-varying magnetic field represents a credit card transaction.

17. (Original) The mobile phone of claim 13 wherein the time-varying magnetic field emulates a swipe of a magnetic card.

18. (Original) The mobile phone of claim 13 wherein the driver comprises a current driver.

19. (**New**) The mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.

20. (**New**) The mobile phone of claim 1 wherein the downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.

21. (**New**) The mobile phone of claim 1, wherein the transaction data includes a transaction

number used for each transaction of the plurality of transactions

22. (**New**) The mobile phone of claim 7 wherein the network is one of a cellular network or a wireless local area network.

23. (**New**) The mobile phone of claim 7 wherein the downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.

24. (**New**) The mobile phone of claim 7, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions

25. (**New**) The mobile phone of claim 13 wherein the network is one of a cellular network or a wireless local area network.

26. (**New**) The mobile phone of claim 13 wherein the downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.

27. (**New**) The mobile phone of claim 13, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions

REMARKS

This listing of claims will replace all prior versions and listings of claims in the application. Claims 1, 7, and 13 are amended. Claims 19-27 are added. No claims are cancelled in this response. Hence, claims 1-27 are pending. Applicants respectfully request reconsideration of claims in view of the amendments and arguments.

SPECIFICATION AMENDMENT

Applicants add the claim of priority to the Specification. No new matter is added.

DOUBLE PATENTING REJECTION

Claims 1-18 stand provisionally rejected on the grounds of nonstatutory double patenting for allegedly being unpatentable over claims 1-18 of U.S. Patent No. 9,715,649, in view of U.S. Patent Publication No. 2011/0240748 of Doughty et al. (hereinafter "Doughty"). Office Action, p. 3, item 2.

"A rejection based on a nonstatutory type of double patenting can be avoided by filing a terminal disclaimer in the application or proceeding in which the rejection is made." M.P.E.P. § 804.02. Hence, Applicants submit the Terminal Disclaimer and authorize Customer Number 175023 (that includes Applicants' Attorney) to sign the Terminal Disclaimer.

Applicants wish to note that the filing of the enclosed Terminal Disclaimer in compliance with 37 C.F.R. § 1.321(c) is not an admission to the propriety of the rejection. *See M.P.E.P.* § 804.02 ("The filing of a terminal disclaimer to obviate a rejection based on nonstatutory double patenting is not an admission of the propriety of the rejection. *Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ 2d 1392 (Fed. Cir. 1991). The court indicated that the 'filing of a terminal disclaimer simply serves the statutory function of removing the rejection of double patenting, and raises neither a presumption nor estoppels on the merits of the rejection.'").

Accordingly, Applicants respectfully request Examiner to consider the Terminal Disclaimer and withdraw the double patenting rejection.

REJECTION UNDER 35 U.S.C. § 102

Claims 1-18 stand rejected under 35 U.S.C. § 102(a) as allegedly anticipated by Doughty. Office Action, p. 4, item 5.

The following arguments are presented with reference to independent claim 1. The same argument applies to other rejected independent claims.

MPEP § 2131 states that "'[a] claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.' *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)" (emphasis added). "'The identical invention must be shown in **as complete detail** as is contained in the ... claim.' *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)" (emphasis added). Moreover, "[e]very element of the claimed invention must be literally present, **arranged as in the claim**." *Id.* (emphasis added).

Applicants contend that Doughty does not disclose a mobile phone comprising: a memory to hold transaction data for use in a plurality of transactions; a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions; a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network; a driver to excite the current carrying conductor; and a processor coupled to control the driver. The amendment is supported by the Specification. See, for example, paragraphs, [0036, [0037], [0040]. See also, previously issued related applications with similar amendments.

Doughty "relates generally to the field of electronic devices and equipment used in the authentication and processing of commercial and security related transactions and, more particularly, to a system, method and apparatus for enabling transactions using biometrically enabled programmable magnetic stripes." Doughty, paragraph [0002]. However, Doughty does not disclose a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network. When the application is reviewed as a whole, the network interface of the mobile phone allows for downloading of one or more parts of the transaction data to the mobile phone while in active

usage, for example. Conversely, the alleged card of Doughty cannot connect to a network while in active use. The alleged network interface of Doughty is not part of a mobile phone. As such, the alleged transaction data of Doughty is not downloadable to a mobile phone via the network. Note, the preamble of the claim is tied to the various features of the claim, and thus cannot be discarded. As such, the term "mobile phone" is an integral part of the claim. Based on the amendment and arguments, claim 1 is not anticipated by Doughty. The same arguments apply to other independent claims.

Accordingly, Applicants respectfully request reconsideration of pending claims in view of the amendments.

Note that merely because Applicants do not specifically argue that certain limitations of a claim are not in the references is not a concession that a reference or combination of references includes the limitations. That Applicants do not contradict a particular statement made in the Office action is not a concession that Applicants agree with it. Further, merely because Applicants do not separately argue the patentability of every dependent claim is not a concession that there are not additional reasons for patentability of these dependent claims.

Applicants believe every assertion by the Office Action has been addressed. However, in the interest of clarity and brevity, Applicants may not have asserted every available argument for each assertion made in the Office Action. Applicants' silence regarding any such assertion does not constitute any admission or acquiescence. Applicants reserve all rights not exercised in connection with this response, such as the right to challenge or rebut any tacit or explicit characterization of any reference or of any of the present claims, the right to challenge or rebut any asserted factual or legal basis of any of the rejections, the right to swear behind any cited reference such as provided under 37 C.F.R. § 1.131 or otherwise, or the right to assert co-ownership of any cited reference.

Applicants do not admit that any of the cited references or any other references of record is relevant to the present claims, or that they constitute prior art. To the extent that any rejection or assertion is based upon the Examiner's personal knowledge, rather than any objection evidence of record as manifested by a cited prior art reference, Applicants timely object to such

reliance on Official Notice, and reserve all rights to request that the Examiner provide a reference or affidavit in support of such assertion, as required by M.P.E.P. § 2144.03. Applicants reserve all rights to pursue any cancelled claims in a subsequent patent application claiming the benefit of priority of the present patent application, and to request rejoinder of any withdrawn claim, as required by M.P.E.P. § 821.04.

New Claims:

Applicants add new claims 19-27. The new claims are supported by the Specification. See, for example, paragraphs [0039-40]. Applicants respectfully request Examiner to consider the new claims.

Based on the amendments and arguments, Applicants respectfully request the Examiner to allow all pending claims.

CONCLUSION

Applicants submit that they have overcome Examiner's objections to and rejections of the claims and that they have the right to claim the invention as listed in the listing of claims. Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Pursuant to 37 C.F.R. § 1.136(a)(3), Applicants request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 C.F.R. § 1.16 and § 1.17, to Deposit Account No. 60-4139.

Respectfully submitted,
MUGHAL IP P.C.

08/17/21
Date

/Usman Mughal/
Usman A. Mughal
Reg. No. 62,887
Attorney for Applicants

1500 NW Bethany Blvd. Suite. 200
Portland, OR 97006
docketing@impactpatents.com

Electronic Patent Application Fee Transmittal

Application Number:	17021347
Filing Date:	15-Sep-2020
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Filer:	Usman Mughal/Katherine Campbell
Attorney Docket Number:	115.001US9.10

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	7	50	350
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**350**

Electronic Acknowledgement Receipt

EFS ID:	43534187
Application Number:	17021347
International Application Number:	
Confirmation Number:	2310
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Customer Number:	35781
Filer:	Usman Mughal/Katherine Campbell
Filer Authorized By:	Usman Mughal
Attorney Docket Number:	115.001US9.10
Receipt Date:	17-AUG-2021
Filing Date:	15-SEP-2020
Time Stamp:	20:11:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$350
RAM confirmation Number	E20218GK17454386
Deposit Account	
Authorized User	

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		115-001US9-10_ROA1.pdf	63840 ba35c62133990cca2b5901203c08883f231b9d1c	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Specification	2	2
	Claims	3	6
	Applicant Arguments/Remarks Made in an Amendment	7	11

Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37994 f781d1e0b0b6a05f372bd751e2b10d4e11f44bf4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	101834		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	17021347
Filing Date	15-Sep-2020
First Named Inventor	Siva Narendra
Attorney Docket Number	115.001US9.10
Title of Invention	MOBILE PHONE WITH MAGNETIC CARD EMULATION

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
iCashe, Inc.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

9715649

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○	I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

- ◉ Small Entity
- ○ Micro Entity
- ○ Regular Undiscounted

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

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

- ◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

  Registration Number 62887

- ○ A sole inventor
- ○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application
- ○ A joint inventor; all of whom are signing this request

Signature	/Usman Mughal/
Name	Usman Mughal

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	17021347
Filing Date:	15-Sep-2020
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Filer:	Usman Mughal/Katherine Campbell
Attorney Docket Number:	115.001US9.10

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	170	170
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**170**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 17021347

Filing Date: 15-Sep-2020

Applicant/Patent under Reexamination: Narendra

Electronic Terminal Disclaimer filed on August 17, 2021

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	43534215
Application Number:	17021347
International Application Number:	
Confirmation Number:	2310
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Customer Number:	35781
Filer:	Usman Mughal/Katherine Campbell
Filer Authorized By:	Usman Mughal
Attorney Docket Number:	115.001US9.10
Receipt Date:	17-AUG-2021
Filing Date:	15-SEP-2020
Time Stamp:	20:24:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$170
RAM confirmation Number	E20218GK24094415
Deposit Account	
Authorized User	

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	41237 b501208729ff634e8cc922d33001fedfcd60310a	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38152 be4a7ccff46a995455c5d428402e9bfd336f2973	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	79389		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 17/021,347	Filing Date 09/15/2020	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $230 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	08/17/2021	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 27	Minus	** 20	= 7		x $50 =	350
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $240 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	350

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

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

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

35781 7590 11/10/2021

Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239

EXAMINER
HAUPT, KRISTY A

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 11/10/2021

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/021,347	09/15/2020	Siva G. Narendra	18.115.001US9.10	2310

TITLE OF INVENTION: MOBILE PHONE WITH MAGNETIC CARD EMULATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	02/10/2022

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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

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

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

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

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

35781 7590 11/10/2021

Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239

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

Certificate of Mailing or Transmission

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

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/021,347	09/15/2020	Siva G. Narendra	18.115.001US9.10	2310

TITLE OF INVENTION: MOBILE PHONE WITH MAGNETIC CARD EMULATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	02/10/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
HAUPT, KRISTY A	2876	235-492000

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

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

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

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

1 _____
2 _____
3 _____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

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

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

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

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

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/021,347	09/15/2020	Siva G. Narendra	18.115.001US9.10	2310

35781 7590 11/10/2021

Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239

EXAMINER	
HAUPT, KRISTY A	

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 11/10/2021

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

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 17/021,347	Applicant(s) Narendra et al.	
	Examiner KRISTY A HAUPT	Art Unit 2876	AIA (FITF) Status No

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

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

1. ☑ This communication is responsive to 8/17/21.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-27 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

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

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

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

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

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 6/29/21.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/KRISTY A HAUPT/
Primary Examiner, Art Unit 2876

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This office action is in response to applicant's amendments and remarks filed 8/17/21. Claims 1-27 are pending with claims 1, 7 and 13 in independent form.

Terminal Disclaimer

1. The terminal disclaimer filed on 8/17/21 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of US Pat. No. 9,715,649 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

2. Claims 1-27 are allowed.

The following is an examiner's statement of reasons for allowance: The prior art of record fails to teach or fairly suggest to one of ordinary skill in the art, in conjunction with all the other limitations of the claims: With respect to claim 1 and all its dependencies, A mobile phone comprising: a memory to hold transaction data for repeated use in a plurality of transactions; a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions; a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network; a driver to excite the current carrying conductor; and a processor coupled to control the driver. With respect to claim 7 and all its dependencies, A mobile phone comprising: a memory to hold transaction data for repeated use in a plurality of transactions; a conductor that when excited by a reversing polarity current

produces a time-varying magnetic field that represents the transaction data in the plurality of transactions; a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network; a driver to excite the conductor; and a processor coupled to control the driver. With respect to claim 13 and all its dependencies, A mobile phone comprising: a memory to hold transaction data for repeated use in a plurality of transactions; a conductor that when excited by a reversing polarity current that varies in amplitude produces a time-varying magnetic field that represents the transaction data in the plurality of transactions; a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network; a driver to excite the conductor; and a processor coupled to control the driver. The prior art of record fails to provide sufficient teaching or motivation to one of ordinary skill in the art to provide the additionally recited features of these claims in the combinations as claimed.

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

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KRISTY A HAUPT whose telephone number is (571)272-8545 and email address is kristy.haupt@uspto.gov. The examiner can normally be reached on Mon-Sun 5:30 AM- 10PM; Flex during day.

If all attempts to reach the examiner ***by telephone and email*** are unsuccessful, the examiner's supervisor, Michael Lee can be reached on 5712722398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/KRISTY A HAUPT/
Primary Examiner, Art Unit 2876

KAH

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/021,347	Narendra et al.
	Examiner	Art Unit
	KRISTY A HAUPT	2876

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06K19/06187; G06K19/07; G06K19/0703; G06K19/0723; G06K19/0727; G06K19/073; G06K19/07741; G06K19/07758; G06K19/07762; G06Q20/204; G06Q20/327; G06Q20/341; G06Q20/353 (text search)	06/21/2021	KAH
Updated	10/25/2021	KAH

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	06/21/2021	KAH
East search	06/21/2021	KAH
Updated	10/25/2021	KAH

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
SAME AS	ABOVE	10/25/2021	KAH

/KRISTY A HAUPT/ Primary Examiner, Art Unit 2876	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/021,347	Narendra et al.
	Examiner	**Art Unit**
	KRISTY A HAUPT	2876

CPC						
Symbol					**Type**	**Version**
G06K	/	19	/	06206	F	2013-01-01
G06K	/	7	/	0008	I	2013-01-01
G06Q	/	20	/	353	I	2013-01-01
G06K	/	19	/	06187	I	2013-01-01
G06K	/	19	/	07	I	2013-01-01
G06K	/	19	/	07741	I	2013-01-01
H04M	/	1	/	72412	I	2021-01-01
G06K	/	19	/	0723	I	2013-01-01
G06K	/	19	/	07758	I	2013-01-01
G06K	/	19	/	073	I	2013-01-01
G06K	/	19	/	07762	I	2013-01-01
G06Q	/	20	/	204	I	2013-01-01
G06Q	/	20	/	341	I	2013-01-01
G06K	/	19	/	0727	I	2013-01-01
G06Q	/	20	/	327	I	2013-01-01
G06K	/	19	/	0703	I	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	27	
/KRISTY A HAUPT/ Primary Examiner, Art Unit 2876	25 October 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

U.S. Patent and Trademark Office — Part of Paper No.: 20211025

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/021,347	Narendra et al.
	Examiner	**Art Unit**
	KRISTY A HAUPT	2876

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06K19/06	/	19	/	06
H04M1/72412	/	1	/	72412
G06K19/073	/	19	/	073
G06Q20/20	/	20	/	20
G06Q20/32	/	20	/	32

NON-CLAIMED				
G06K7/00	/	7	/	00
G06Q20/34	/	20	/	34
G06K19/07	/	19	/	07
G06K19/077	/	19	/	077

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	27	
/KRISTY A HAUPT/ Primary Examiner, Art Unit 2876	25 October 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

U.S. Patent and Trademark Office

Part of Paper No.: 20211025

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/021,347	Narendra et al.
	Examiner	**Art Unit**
	KRISTY A HAUPT	2876

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	13	10	7	19										
2	2	14	11	8	20										
3	3	15	12	9	21										
4	4	19	13	16	22										
5	5	20	14	17	23										
6	6	21	15	18	24										
10	7	22	16	25	25										
11	8	23	17	26	26										
12	9	24	18	27	27										

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	27	
/KRISTY A HAUPT/ Primary Examiner, Art Unit 2876	25 October 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

U.S. Patent and Trademark Office

Part of Paper No.: 20211025

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/021,347	Narendra et al.
	Examiner	Art Unit
	KRISTY A HAUPT	2876

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

CLAIMS

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

CLAIM		DATE								
Final	Original	06/21/2021	10/25/2021							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
10	7	✓	=							
11	8	✓	=							
12	9	✓	=							
13	10	✓	=							
14	11	✓	=							
15	12	✓	=							
19	13	✓	=							
20	14	✓	=							
21	15	✓	=							
22	16	✓	=							
23	17	✓	=							
24	18	✓	=							
7	19		=							
8	20		=							
9	21		=							
16	22		=							
17	23		=							
18	24		=							
25	25		=							
26	26		=							
27	27		=							

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17/021,347
	Filing Date	Sep 15, 2020
	First Named Inventor	Siva Narendra
	Art Unit	2887
	Examiner Name	/KRISTY A HAUPT/
	Attorney Docket Number	115.001US9.10

U.S.PATENTS

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

U.S.PATENT APPLICATION PUBLICATIONS

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	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]

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
		Final Office Action notified December 26, 2007 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Non-Final Office Action notified December 11, 2008 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Non-Final Office Action notified February 26, 2007 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Non-Final Office Action notified July 08, 2010 for U.S. Patent Application No. 12/539,369 (Docket No. 115.1US2).	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17/021,347
	Filing Date	Sep 15, 2020
	First Named Inventor	Siva Narendra
	Art Unit	2887
	Examiner Name	/KRISTY A HAUPT/
	Attorney Docket Number	115.001US9.10

		Non-Final Office Action notified July 23, 2008 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Notice of Allowance notified April 14, 2011 for U.S. Patent Application No. 12/941,410 (Docket No. 115.001US2.1).	
		Notice of Allowance notified July 10, 2009 for U.S. Patent Application No. 11/063,291 (Attorney Docket No. 115.001US1).	
		Notice of Allowance notified September 30, 2010 for U.S. Patent Application No. 12/539,369 (Docket No. 115.001US2).	
		Notice of Allowance notified September 30, 2010 for U.S. Patent Application No. 12/539,369 (Docket No. 115.1US2).	

EXAMINER SIGNATURE

Examiner Signature	/KRISTY A HAUPT/	Date Considered	10/25/2021

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17/021,347
	Filing Date	Sep 15, 2020
	First Named Inventor	Siva Narendra
	Art Unit	2887
	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.

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

☐ None

SIGNATURE

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

Signature	/Usman Mughal/	Date (YYYY-MM-DD)	2021-06-29
Name/Print	Usman A. Mughal	Registration Number	62887

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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.A.H/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S43	3,646,325	((mobile portable cellular smart) adj2 (phone device apparatus))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S62	3,373,568	@pd>"20210621"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:22
S47	326,041	((memory stor$3) with (transaction))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S32	157,698	G06K19/06206.cpc. or H04M1/72412.cpc. or G06K7/0008.cpc. or G06K19/06187.cpc. or G06K19/07.cpc. or G06K19/0703.cpc. or G06K19/0723.cpc. or G06K19/0727.cpc. or G06K19/073.cpc. or G06K19/07741.cpc. or G06K19/07758.cpc. or G06K19/07762.cpc. or G06Q20/204.cpc. or G06Q20/327.cpc. or G06Q20/341.cpc. or G06Q20/353.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S38	48,423	S32 and "7"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16

S42	19,853	(time near3 (vary varying)) near5 (magnetic magnet ("em" near2 field))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S64	6,045	((mobile smart cellular) and phone and transaction).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:23
S44	3,401	S42 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S63	2,496	S32 and S62	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:22
S33	724	(tyfone.in. near inc.in.) or (tyfone.as. near inc.as.) or (narendra.in. near siva.in.) or (spitzer.in. near thomas.in.) or (tadepalli.in. near prabhakar.in.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S58	724	(tyfone.in. near inc.in.) or (tyfone.as. near inc.as.) or (narendra.in. near siva.in.) or (spitzer.in. near thomas.in.) or (tadepalli.in. near prabhakar.in.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S34	211	("20010002035" | "20010006902" | "20010013551" | "20010034246" | "20020007434" | "20020025796" | "20020043566" | "20020044043" | "20020095588" | "20020096570" | "20020099665" | "20020130187" | "20020138422" | "20020138735" | "20020139849" | "20020148892" |	US-PGPUB; USPAT	OR	ON	2021/10/25 09:16

"20020153424" | "20020158747" |
"20020178124" | "20020180584" |
"20020186845" | "20030025939" |
"20030028481" | "20030038177" |
"20030052168" | "20030057278" |
"20030061168" | "20030079096" |
"20030080183" | "20030084220" |
"20030085288" | "20030115126" |
"20030128124" | "20030159050" |
"20030200180" | "20030209604" |
"20030218066" | "20030220876" |
"20030231550" | "20040006654" |
"20040027881" | "20040030660" |
"20040035942" | "20040050930" |
"20040058705" | "20040064612" |
"20040065733" | "20040077372" |
"20040087339" | "20040094624" |
"20040122685" | "20040133787" |
"20040162932" | "20040177045" |
"20040188519" | "20040199469" |
"20040227859" | "20040243785" |
"20040243806" | "20040251303" |
"20040255145" | "20050006462" |
"20050017068" | "20050022002" |
"20050029349" | "20050038736" |
"20050039027" | "20050044044" |
"20050050367" | "20050052924" |
"20050060586" | "20050071282" |
"20050077349" | "20050092830" |
"20050108096" | "20050109838" |
"20050116026" | "20050121512" |
"20050122209" | "20050127164" |
"20050127166" | "20050133606" |
"20050136964" | "20050168339" |
"20050177724" | "20050197859" |
"20050204077" | "20050204092" |
"20050212657" | "20050223143" |
"20050224589" | "20050240778" |
"20050246546" | "20050253687" |
"20050258245" | "20050268058" |
"20050268330" | "20060011731" |
"20060027655" | "20060045555" |
"20060077039" | "20060097851" |
"20060124755" | "20060169778" |
"20060172606" | "20060186209" |
"20060219776" | "20060226217" |
"20060268764" | "20060279413" |
"20070033334" | "20070076877" |
"20070108280" | "20070110404" |
"20070145135" | "20070145152" |
"20070195458" | "20070205864" |
"20070257797" | "20070293202" |
"20080046649" | "20080065830" |

		"20080068173" | "20080073436" | "20080136619" | "20080147950" | "20080148077" | "20080153416" | "20080186174" | "20080214111" | "20080244208" | "20080279381" | "20080311849" | "20080318535" | "20090065571" | "20090065572" | "20090069049" | "20090069050" | "20090069051" | "20090069052" | "20090070272" | "20090070691" | "20090070861" | "20090108063" | "20090150610" | "20090152361" | "20090199283" | "20090250521" | "20090265552" | "20090270127" | "20090290582" | "20090298540" | "20090315667" | "20100033307" | "20100033310" | "20100049878" | "20100213265" | "20110000960" | "20110053644" | "20110073663" | "20110073665" | "20110077052" | "20110110404" | "20110171996" | "20110180610" | "20110220726" | "20110223972" | "20110240748" | "20110269438" | "20110271044" | "20110272468" | "20110272469" | "4701601" | "4786791" | "4791283" | "4864109" | "5212478" | "5378887" | "5386106" | "5537584" | "5574273" | "5585787" | "5629981" | "5700037" | "5710421" | "5834756" | "5909491" | "5940510" | "5949880" | "5952641" | "5955961" | "6016476" | "6021944" | "6039260" | "6045043" | "6068184" | "6105013" | "6182891" | "6189786" | "6206293" | "6219439" | "6223954" | "6223984" | "6237095" | "6250557" | "6315195" | "6402029" | "6450407" | "6481623" | "6568600" | "6588660").PN.				
S66	195	((mobile smart cellular) and phone and transaction and magnetic and field).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:24
S48	188	S44 and S47	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2021/10/25 09:16

			DERWENT; IBM_TDB			
S45	181	S32 and S44	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S49	103	S32 and S48	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S68	91	((mobile smart cellular) and phone and transaction and magnetic and field and network).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:24
S53	80	((mobile portable cellular smart) adj2 (phone device apparatus)) with (magnetic$4 adj1 stripe adj3 emulat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S54	80	S53 not S33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S37	79	((phone device apparatus) with ((memory stor$3) with (transaction))) and ((phone device apparatus) with (time near3 (vary varying)) with ((magnetic$3 "EM" electromagnet$3) adj3 field))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S39	75	S32 and S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2021/10/25 09:16

			DERWENT; IBM_TDB			
S35	69	("6592044" | "6594759" | "6598031" | "6607127" | "6609654" | "6631849" | "6636833" | "6669487" | "6705520" | "6712277" | "6715679" | "6721196" | "6747547" | "6764005" | "6769607" | "6805288" | "6811082" | "6836843" | "6857566" | "6882900" | "6883718" | "6905072" | "6907123" | "6908030" | "6925568" | "6937526" | "6952788" | "6995651" | "7059520" | "7088246" | "7185146" | "7213766" | "7221473" | "7281101" | "7295790" | "7333062" | "7350717" | "7353993" | "7410102" | "7493484" | "7558107" | "7558110" | "7581678" | "7607580" | "7673080" | "7716082" | "7789303" | "7792516" | "7828214" | "7898994" | "7933571" | "7941197" | "7948356" | "7954715" | "7954716" | "7954717" | "7961101" | "7991158" | "8072331" | "8082575" | "8083145" | "8091786" | "8103881" | "9092708" | "9202156" | "9715649" | "RE41352" | "RE41471" | "RE42254").PN.	US-PGPUB; USPAT	OR	ON	2021/10/25 09:16
S46	67	S33 and S44	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S40	58	S33 and S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S60	48	(memory and transaction and current and time and vary$3 and magnetic and field).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S57	36	(memory and transaction and current and time and vary$3 and magnetic and field and driver and processor).dm.	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2021/10/25 09:16

			JPO; DERWENT; IBM_TDB			
S56	22	((memory "sim") adj1 card) with (transaction with ((magnetic mag) adj2 stripe))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S52	16	S34 and S48	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S65	14	S63 and S64	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:23
S61	9	S58 and S60	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16
S67	4	S62 and S66	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:24
L1	1	((mobile smart cellular) and phone and transaction and magnetic and field and network and polarity).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 10:28
S31	1	("9715649").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/10/25 09:05

S36	1	("9715649").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/10/25 09:16
S41	1	("20110240748").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/10/25 09:16
S50	1	("20050182710").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/10/25 09:16
S51	1	("6016476").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/10/25 09:16
S55	1	("20050168339").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/10/25 09:16
S59	1	S57 and S58	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/10/25 09:16

10/25/2021 10:30:27 AM
C:\Users\khaupt\Documents\EAST\Workspaces\17 021 347.wsp

Bibliographic Data

Application No: 17/021,347

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /KRISTY A HAUPT/ KAH

Examiner's Signature Initials

Title: MOBILE PHONE WITH MAGNETIC CARD EMULATION

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/15/2020	235	2876	18.115.001US9.10
RULE			

APPLICANTS

Tyfone, Inc., Portland, OR,

INVENTORS

Siva G. Narendra, Portland, OR, UNITED STATES

Thomas N. Spitzer, Portland, OR, UNITED STATES

Prabhakar Tadepalli, Bangalore, INDIA

CONTINUING DATA

This application is a CON of 16218733 12/13/2018 PAT 10803370

16218733 is a CON of 15658208 07/24/2017 PAT 10185909

15658208 is a CON of 14948325 11/22/2015 PAT 9715649

14948325 is a CON of 14747770 06/23/2015 PAT 9202156

14747770 is a CON of 14680684 04/07/2015 PAT 9092708

14680684 is a CON of 13592323 08/22/2012 PAT 9004361

13592323 is a CON of 13304663 11/27/2011 PAT 8573494

13304663 is a CON of 13114434 05/24/2011 PAT 8091786

13114434 is a CON of 12941410 11/08/2010 PAT 7954715

12941410 is a CON of 12539369 08/11/2009 PAT 7828214

12539369 is a CON of 11063291 02/22/2005 PAT 7581678

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

10/01/2020

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239
UNITED STATES

FILING FEE RECEIVED

$1,720

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	17021347
Filing Date	2020-09-15
First Named Inventor	Siva G. Narendra
Art Unit	2876
Examiner Name	Kristy A HAUPT
Attorney Docket Number	18.P115.001US9.10

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	10185909	B2	2019-01-22	Narendra et al.	Entire Document
	2	4701601	A	1987-10-20	Francini et al.	Entire Document
	3	4786791	A	1988-11-22	Hodama	Entire Document
	4	6811082	B2	2004-11-02	Wong	Entire Document

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					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	1	2001088659	WO	A3	2002-04-18	Wong et al.	Entire Document	

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.	T5
	1	Final Office Action notified September 30, 2014 for U.S. Patent Application No. 13/592,323 (Docket No. 115.001US9).	
	2	International Preliminary Report on Patentability notified August 28, 2007 for PCT Patent Application No. PCT/US2006/006361 (Attorney Docket No. 115.001WO1).	
	3	International Preliminary Report on Patentability notified August 30, 2011 for PCT Application No. PCT/US2010/025014 (Docket No. 115.024WO01).	
	4	International Preliminary Report on Patentability notified December 04, 2006 for PCT Application No. PCT/US2005/019988 (Docket No 115.004WO1).	
	5	International Preliminary Report on Patentability notified December 16, 2005 for PCT Application No. PCT/US2005/019988 (Docket No 115.004WO1).	
	6	International Preliminary Report on Patentability notified January 22, 2008 for PCT Patent Application No. PCT/US2006/027847 (Docket No. 115.012WO1).	
	7	International Preliminary Report on Patentability notified October 06, 2009 for PCT Patent Application No. PCT/US2008/057588 (Docket No. 115.019WO1).	
	8	International Preliminary Report on Patentability notified October 09, 2007 for PCT Application No. PCT/US2006/013603 (Docket No. 115.002WO01).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	9	International Preliminary Report on Patentability notified October 21, 2005 for PCT Application No. PCT/US2005/022993 (Docket No 115.003WO1).	
	10	International Search Report & Written Opinion notified October 09, 2008 for PCT Patent Application No. PCT/US2008/057588 (Docket No. 115.019WO1).	
	11	International Search Report & Written Opinion notified September 22, 2006 for PCT Patent Application No. PCT/US2006006361 (Docket No. 115.001WO1).	
	12	International Search Report notified September 22, 2006 for PCT Patent Application No. PCT/US2006/006361 (Attorney Docket No. 115.001WO1).	
	13	International Search Report notified September 22, 2016 for PCT Patent Application No. PCT/US2006/006361 (Attorney Docket No. 115.001WO1).	
	14	Non-Final Office Action notified August 04, 2011 for U.S. Patent Application No. 13/114,434 (Docket No. 18.P115.001US4.1).	
	15	Non-Final Office Action notified July 05, 2013 for U.S. Patent Application No. 13/592,323 (Docket No. 115.001US9).	
	16	Non-Final Office Action notified June 18, 2013 for U.S. Patent Application No. 13/304,663 (Docket No. 115.001US4.2).	
	17	Non-Final Office Action notified March 18, 2011 for U.S. Patent Application No. 12/941,410 (Docket No. 115.001US2.1).	
	18	Non-Final Office Action notified November 01, 2021 for U.S. Patent Application No. 17/243,58 (Docket No. 18.P115.001US9.11)	
	19	Non-Final Office Action notified November 29, 2019 for U.S. Patent Application No. 16/218,733 (Docket No. 115.001US9.9).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	20	Non-Final Office Action notified September 20, 2016 for U.S. Patent Application No. 14/948,325 (Docket No. 115.001US0.7).	
	21	Notice of Allowance notified February 18, 2015 for U.S. Patent Application No. 13/592,323 (Docket No. 115.001US9).	
	22	Notice of Allowance notified June 18, 2020 for U.S. Patent Application No. 16/218,733 (Docket No. 115.001US9.9).	
	23	Notice of Allowance notified June 19, 2015 for U.S. Patent Application No. 14/680,684 (Docket No. 115.001US9.2).	
	24	Notice of Allowance notified March 24, 2017 for U.S. Patent Application No. 14/948,325 (Docket No. 115.001US9.7).	
	25	Notice of Allowance notified November 14, 2011 for U.S. Patent Application No. 13/114,434 (Docket No. 18. P115.001US4.1).	
	26	Notice of Allowance notified October 26, 2015 for U.S. Patent Application No. 14/747,770 (Docket No. 115.001US9.3).	
	27	Notice of Allowance notified September 16, 2013 for U.S. Patent Application No. 13/304,663 (Docket No. 115.001US4.2).	
	28	Notice of Allowance notified September 19, 2018 for U.S. Patent Application No. 15/658,208 Docket No. 115.001US9.8).	
	29	Official Letter notified January 26, 2010 from Taiwan Patent Office for TW Patent Application No. 95105997 (Docket No. 115.001TW1).	
	30	Official Letter notified October 20, 2010 from Taiwan Patent Office for TW Patent Application No. 95105997 (Docket No. 115.001TW1).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

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	17021347
Filing Date	2020-09-15
First Named Inventor	Siva G. Narendra
Art Unit	2876
Examiner Name	Kristy A HAUPT
Attorney Docket Number	18.P115.001US9.10

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	/Usman Mughal/	Date (YYYY-MM-DD)	2021-12-06
Name/Print	Usman Mughal	Registration Number	62887

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: **Siva Narendra**	Examiner: **Kristy A. Haupt**
Application No.: 17/021,347	Art Group: 2876
Filed: September 15, 2020	Confirmation No.: 2310
For: MOBILE PHONE WITH MAGNETIC CARD EMULATION	Docket No.: 115.001US9.10

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

INFORMATION DISCLOSURE STATEMENT

Applicants respectfully request that this Information Disclosure Statement be entered and the documents listed on the attached form be considered by the Examiner and made of record. Pursuant to the provisions of MPEP 609, Applicants request that a copy of the form, initialed as being considered by the Examiner, be returned to the Applicants with the next official communication.

Pursuant to 37 CFR § 1.97(b), it is believed that no fee or statement is required with the Information Disclosure Statement. However, if an Office Action on the merits has been mailed, the Commissioner is hereby authorized to charge the required fees to Deposit Account No. 60-4139 in order to have this Information Disclosure Statement considered.

Pursuant to 37 CFR § 1.98(d), copies of the listed documents are not provided as these references were previously cited by or submitted to the U.S. Patent Office in connection with Applicants' prior U.S. Application Nos.: 16/218,733, filed December 13, 2018, 10,803,370 filed October 13, 2020, 15/658,208, filed July 24, 2017, 14/948,325, filed November 22, 2015, 14/747,770, filed June 23, 2015, 14/680,684, filed April 07, 2015, 13/592,323, filed August 22,

2012, 13/304,663, filed November 27, 2011, 13/114,434, filed May 24, 2011, 12/941,410, filed November 08, 2010, 12/539,369, filed August 11, 2009, 11/063,291, filed February 22, 2005, which are relied upon for an earlier filing date under 35 U.S.C. § 120.

Examiner Haupt is invited to contact the Applicants' Representative at the below-listed telephone number if there are any questions regarding this communication.

Pursuant to 37 C.F.R. § 1.136(a)(3), Applicants request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 C.F.R. § 1.16 and § 1.17, to Deposit Account No. 60-4139.

Respectfully submitted,
MUGHAL IP P.C

December 06, 2021
Date

/Usman Mughal/
Usman Mughal
Reg. No. 62887
Attorney for Applicants

1500 NW Bethany Blvd. Suite 200
Beaverton, OR 97006
docketing@impactpatents.com

Electronic Acknowledgement Receipt

EFS ID:	44445666
Application Number:	17021347
International Application Number:	
Confirmation Number:	2310
Title of Invention:	MOBILE PHONE WITH MAGNETIC CARD EMULATION
First Named Inventor/Applicant Name:	Siva G. Narendra
Customer Number:	35781
Filer:	Usman Mughal/Katherine Campbell
Filer Authorized By:	Usman Mughal
Attorney Docket Number:	18.115.001US9.10
Receipt Date:	06-DEC-2021
Filing Date:	15-SEP-2020
Time Stamp:	22:02:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	18P115001US910_IDS_120621.pdf	1054434 7a1337aa03fbe7e4bb90b7d4ae7e1d12ef51800d	no	7

Warnings:

Information:					
2	Transmittal Letter	115-001US9-10_IDS_Transmittal.pdf	22610 1610e8adcf9ac570981d69e5643d538323183554	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1077044	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/021,347	09/15/2020	Siva G. Narendra	18.115.001US9.10	2310

7590 12/13/2021

Tyfone, Inc.
Patent Dept.
5331 SW Macadam Avenue
Suite 251
Portland, OR 97239

EXAMINER	
HAUPT, KRISTY A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
12/13/2021	ELECTRONIC

NOTICE OF NON-COMPLIANT INFORMATION DISCLOSURE STATEMENT

An Information Disclosure Statement (IDS) filed *12/6/2021* in the above-identified application fails to meet the requirements of 37 CFR 1.97(d) for the reason(s) specified below. Accordingly, the IDS will be placed in the file, but the information referred to therein has not been considered.

The IDS is not compliant with 37 CFR 1.97(d) because:

☑ The IDS lacks a statement as specified in 37 CFR 1.97(e).

☐ The IDS lacks the fee set forth in 37 CFR 1.17(p).

☐ The IDS was filed after the issue fee was paid. Applicant may wish to consider filing a petition to withdraw the application from issue under 37 CFR 1.313(c) to have the IDS considered. See MPEP 1308.

N. Horne, for

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

FORM PTOM327-B (Rev. 02/08)

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	17021347
Filing Date	2020-09-15
First Named Inventor	Siva G. Narendra
Art Unit	2876
Examiner Name	Kristy A HAUPT
Attorney Docket Number	18.P115.001US9.10

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	1238055	A	1917-08-21	Thornton	Entire Document
	2	5294782	A	1994-03-15	Kumar	Entire Document
	3	5679945	A	1997-10-21	Renner et al.	Entire Document
	4	5748740	A	1998-05-05	Curry et al.	Entire Document
	5	5787154	A	1998-07-28	Hazra et al.	Entire Document
	6	5805702	A	1998-09-08	Curry et al.	Entire Document
	7	5834747	A	1998-11-10	Cooper	Entire Document
	8	5917913	A	1999-06-29	Wang	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	9	6061344	A	2000-05-09	Wood Jr.	Entire Document
	10	6129277	A	2000-10-10	Grant et al.	Entire Document
	11	6131811	A	2000-10-17	Gangi	Entire Document
	12	6219438	B1	2001-04-17	Giordano et al.	Entire Document
	13	6394343	B1	2002-05-28	Berg et al.	Entire Document
	14	6705529	B1	2004-03-16	Kettunen et al.	Entire Document
	15	6722570	B1	2004-04-20	Eisele	Entire Document
	16	6766952	B2	2004-07-27	Luu	Entire Document
	17	6816058	B2	2004-11-09	McGregor et al.	Entire Document
	18	6820177	B2	2004-11-16	Poisner	Entire Document
	19	6868460	B1	2005-03-15	Kou	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	20	6922770	B2	2005-07-26	Shanmugasundaram et al.	Entire Document
	21	6938821	B2	2005-09-06	Gangi	Entire Document
	22	6958706	B2	2005-10-25	Chaco et al.	Entire Document
	23	6959874	B2	2005-11-01	Bardwell	Entire Document
	24	6983882	B2	2006-01-10	Cassone	Entire Document
	25	7028897	B2	2006-04-18	Fernandes et al.	Entire Document
	26	7044394	B2	2006-05-16	Brown	Entire Document
	27	7051932	B2	2006-05-30	Fernandes et al.	Entire Document
	28	7080037	B2	2006-07-18	Burger et al.	Entire Document
	29	7155416	B2	2006-12-26	Shatford	Entire Document
	30	7195154	B2	2007-03-27	Routhenstein	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	31	7210014	B2	2007-04-24	Drasnin et al.	Entire Document
	32	7249112	B2	2007-07-24	Berardi et al.	Entire Document
	33	7267266	B2	2007-09-11	Rouille et al.	Entire Document
	34	7273168	B2	2007-09-25	Linlor	Entire Document
	35	7280984	B2	2007-10-09	Phelan et al.	Entire Document
	36	7308426	B1	2007-12-11	Pitroda	Entire Document
	37	7336973	B2	2008-02-26	Goldthwaite et al.	Entire Document
	38	7340439	B2	2008-03-04	Burger et al.	Entire Document
	39	7352413	B2	2008-04-01	Liang	Entire Document
	40	7360688	B1	2008-04-22	Harris	Entire Document
	41	7363505	B2	2008-04-22	Black	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	42	7461787	B2	2008-12-09	Chung	Entire Document
	43	7470244	B2	2008-12-30	Harrison Jr.	Entire Document
	44	7486172	B2	2009-02-03	Martinez et al.	Entire Document
	45	7502937	B2	2009-03-10	McKinley et al.	Entire Document
	46	7548491	B2	2009-06-16	MacFarlane	Entire Document
	47	7591426	B2	2009-09-22	Osterweil et al.	Entire Document
	48	7597250	B2	2009-10-06	Finn	Entire Document
	49	7604176	B2	2009-10-20	Bates et al.	Entire Document
	50	7907935	B2	2011-03-15	Saint et al.	Entire Document
	51	7966497	B2	2011-06-21	Gantman et al.	Entire Document
	52	8015592	B2	2011-09-06	Doughty et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	53	8918900	B2	2014-12-23	Saito	Entire Document

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	20020043566	A1	2002-04-18	Goodman et al.	Entire Document
	2	20030048174	A1	2003-03-13	Stevens et al.	Entire Document
	3	20040127256	A1	2004-07-01	Goldthwaite et al.	Entire Document
	4	20050027030	A1	2005-02-03	Park et al.	Entire Document
	5	20050269401	A1	2005-12-08	Spitzer et al.	Entire Document

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	399405T	AT		2008-07-15	Felt et al.	Entire Document	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	2	2002366416	AU	A1	2003-06-30	Amtmann et al.	Entire Document	
	3	4831500	AU	A	2000-11-21	Rienzo	Entire Document	
	4	5079498	AU	A	1998-05-15	Arakaki	Entire Document	
	5	6159601	AU	A	2001-11-26	Wong et al.	Entire Document	
	6	PP411098A0	AU		1998-07-09	NEWCOM TECHNOLOGIES Pty Ltd	Entire Document	
	7	2337672	CA	A1	2001-10-26	Husemann et al.	Entire Document	
	8	2388007	CA	A1	2001-04-05	Burger et al.	Entire Document	
	9	690048	CH		2000-03-31	Korshun	Entire Document	
	10	1218276C	CN	C	2005-09-07	Nishizawa et al.	Entire Document	
	11	1653751	CN	A	2005-08-10	Kaarle et al.	Entire Document	
	12	19928733	DE	A1	2001-01-04	Grasl	Entire Document	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	13	60026768T2	DE		2006-11-09	Christensen et al.	Entire Document	
	14	0541818	EP	B1	1997-12-03	Kobayashi	Entire Document	
	15	0720102	EP	A1	1996-07-03	Furuhashi et al.	Entire Document	
	16	100137	FI	B	1997-09-30	Vazvan	Entire Document	
	17	99071C	FI	C	1997-09-25	Terho et al.	Entire Document	
	18	2788646	FR	B1	2007-02-09	Carpier et al.	Entire Document	
	19	2801709	FR	B1	2002-02-15	Kayanakis	Entire Document	
	20	2868987	FR	A1	2005-10-21	Rancien et al.	Entire Document	
	21	2316908	GB	A	1998-03-11	Cowling	Entire Document	
	22	119943	IL		1997-03-18	ON TRACK INNOVATIONS LTD	Entire Document	
	23	MI981564	IT	A1	2000-01-09	Campardo	Entire Document	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	24	2001167187	JP	A	2001-06-22	Natsuno et al.	Entire Document	
	25	2005202914	JP	A	2005-07-28	Minemura et al.	Entire Document	
	26	2523960	JP		1997-01-29	Fukushima	Entire Document	
	27	3180086	JP	U	2012-12-06	NAGAOKA	Entire Document	
	28	3519491	JP	B2	2004-04-12	KOKUBU	Entire Document	
	29	3614157	JP	B2	2005-01-26	FUKUOKA SHINICHIRO	Entire Document	
	30	3641230	JP	B2	2005-04-20	Murakami	Entire Document	
	31	3839288	JP	B2	2006-11-01	Katayama et al.	Entire Document	
	32	4053704	JP	B2	2008-02-27	Ito et al.	Entire Document	
	33	4086584	JP	B2	2008-05-14	FURUKAWA HIDEYUKI	Entire Document	
	34	4322021	JP	B2	2009-08-26	MIZUSHIMA EIGA et al.	Entire Document	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	35	4412947	JP	B2	2010-02-10	NISHIZAWA HIROTAKA et al.	Entire Document	
	36	4515793	JP	B2	2010-08-04	MASUYAMA HIROSHI et al.	Entire Document	
	37	4624732	JP	B2	2011-02-02	TAKAGI YOSHIHIKO et al.	Entire Document	
	38	H1097599	JP	A	1998-04-14	Ito et al.	Entire Document	
	39	100604877	KR	B1	2006-07-31	LEE BYEONG HOON	Entire Document	
	40	101149887	KR	B1	2012-06-11	KANG SANG WOOK et al.	Entire Document	
	41	20030072203	KR	A	2003-09-13	Hutchison et al.	Entire Document	
	42	2007000546	MX	A	2007-03-30	Smets et al.	Entire Document	
	43	I457835	TW	B	2014-10-21	Arai et al.	Entire Document	
	44	1996026500	WO	A1	1996-08-29	Peek	Entire Document	
	45	2000014678	WO	A1	2000-03-16	Combaluzier	Entire Document	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17021347
	Filing Date	2020-09-15
	First Named Inventor	Siva G. Narendra
	Art Unit	2876
	Examiner Name	Kristy A HAUPT
	Attorney Docket Number	18.P115.001US9.10

	46	2001067355	WO	A2	2001-09-13	Breck et al.	Entire Document	
	47	2002071311	WO	A3	2002-11-21	Halpern	Entire Document	
	48	2003010939	WO	A1	2003-02-06	Bando	Entire Document	
	49	2003081519	WO	A2	2003-10-02	Thomas et al.	Entire Document	
	50	2005119607	WO	A3	2006-05-04	Spitzer et al.	Entire Document	

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

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

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	17021347
Filing Date	2020-09-15
First Named Inventor	Siva G. Narendra
Art Unit	2876
Examiner Name	Kristy A HAUPT
Attorney Docket Number	18.P115.001US9.10

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	/Usman Mughal/	Date (YYYY-MM-DD)	2022-01-10
Name/Print	Usman Mughal	Registration Number	62887

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 terminal with removable memory and SIM card function

Classifications

H04W8/183 Processing at user equipment or user record carrier

DE60026768T2
Summary

Download PDF Find Prior Art Similar

Other languages: German

Inventor: Per Hartmann Christensen, Digital Telecomm. Europe
Yutaka Yamagishi, Digital Telecommunications Europe
Tatsuji Ushino

Current Assignee : Sony Deutschland GmbH

Worldwide applications

2000 DE EP

Application DE2000626768 events

2000-09-19 Application filed by Sony Deutschland GmbH
2000-09-19 Priority to EP20000120475
2006-05-11 Application granted
2006-05-11 Publication of DE60026768D1
2006-11-09 Publication of DE60026768T2
2020-09-20 Anticipated expiration
Status Expired - Lifetime

Info: Patent citations (2), Cited by (15), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, DPMA, Discuss

Claims (6)

Hide Dependent

1. Mobile terminal (1) for a wireless telecommunication system with a terminal control device (2) for controlling the functions of the mobile terminal and with a removable memory module (5 , 12), which is a memory device (7) and a memory controller (6) for controlling the memory device (7), wherein the respective memory module (5 , 12) with the terminal control device (2) by means of an interface device (4), which has a plurality of connections for an exchange of information between the respective terminal control device (2) and the said memory control device (6), wherein the respective memory module (5 , 12) a subscriber identity or subscriber identification device (8th) for providing subscriber identity information for said terminal control module (2) via at least one of the various connections of the interface device (4), **characterized** in that said memory module (5 , 12) a switching device (9 , 13 , 14), that the switching device (9 , 13 , 14) the relevant subscriber identification device (8th) with said at least one compound of said different compounds of the interface device (4), the relevant switching device (9 , 13 , 14) a corresponding connection of said interface device (4) between the memory controller (6) and the subscriber identification device (8th) selectively switches

2. Mobile terminal according to claim 1, characterized in that the subscriber identification device (8th) has connection means for connecting a removable subscriber identification module card.

3. Mobile terminal according to claim 1, characterized in that the subscriber identification device (8th) comprises a subscriber memory device for storing subscriber identification information.

4. Mobile terminal according to claim 1, 2 or 3, characterized in that the at least one connection which is selectively connected to said subscriber identification device (8th) and the said memory control device (6) is a data input / output connection.

5. Mobile terminal according to one of claims 1 to 4, characterized in that said switching device (5) by the terminal control device (2) is controlled.

6. Mobile terminal according to one of claims 1 to 4, characterized in that the switching device in question (13 , 14) by the said memory control device (6) is controlled.

Description

[0001] The The present invention relates to a mobile terminal for a wireless Telecommunications system, such as the GSM or the UMTS system, with a removable

Memory module.

[0002] mobile terminals like portable phones, palmtops, personal digital assistants or the like of wireless telecommunication systems of the second Generation and the third generation are becoming increasingly more versatile and more powerful multimedia devices developed. Due to the higher transfer rates between the mobile device and the respective base stations of the wireless telecommunication system in the mobile devices to store and manage increasing amounts of data. That's the concept proposed by removable memory modules by the Applicant Service. These removable memory modules, the memory sticks or Sticks are essentially protected a memory device such as random access memory Access of any type and a memory controller that the data reading and writing from or to the memory device controls. Such a removable memory module extends the memory from modern mobile devices considerably. Furthermore, the removable memory module may be based on from standardized interface connections with several different ones electronic devices be used so that a user can get valuable information, like e-mail addresses, phone numbers etc. flexible in different Devices through easy replacement of the removable memory module can use. On the other hand, mobile terminals require wireless telecommunications systems generally the introduction a subscriber identity module card or SIM card before operation by a user. A subscriber identity module card contains a subscriber identity information, the a user or a subscriber for the wireless used Telecommunication system identified. This will be the respective User during the communication detected in the wireless telecommunication system, so that the respective contracted features are provided by the system and can be charged to the user.

[0003] in the EP 0 564 105 A2 a memory module adapter has been proposed which can be used in a wireless or mobile phone detachable or removable. The memory module adapter has the size and configuration, that is electrical contacts, to be compatible with a credit card size reader of a SIM card in the radiotelephone. Furthermore, the memory module adapter has a memory module reader, such as a plug for a small SIM card. Generally, the memory module adapter will be described as a data card or any other form of packaging that encloses or carries a storage device. However, the only disclosure regarding the exchange of information between the memory module adapter and the cellular phone is that there are contacts that are sized and configured to be compatible with a credit card size SIM card reader of the phone.

[0004] in FR-A-2,745,834 is a mobile terminal with a removable memory module according to the generic term of claim 1.

[0005] The object of the present invention is 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 which considerably extends the storage capacity of the mobile terminal. The above object is achieved by a mobile terminal for a wireless telecommunication system according to claim 1, comprising a terminal controller for controlling the function of the mobile terminal and a removable memory module having a memory means and a memory controller for controlling the memory means. The memory module is detachably connected to the terminal controller by means of an interface device having a plurality of connections for exchanging information between the terminal controller and the memory controller, the memory module further comprising subscriber identification means for providing subscriber identification information to the terminal control module has at least one of the various connections or connections of the interface device in question. The memory module has a switching device, and the relevant switching device connects said subscriber identification device to said at least one connection of said different ports of the interface device. The respective switching device selectively switches the corresponding connection of the interface device between the memory control device and the subscriber identification device. The subscriber identification device and the memory control device share at least one common connection of the interface device and the selective switching device ensures that the desired subscriber identification function or the memory function of the removable memory module is selected in a simple manner become.

[0006] The mobile terminal according to the present invention thus advantageously combines the functions a removable storage module and a removable SIM card in a single removable device in a simple and effective way. In particular, the integration of the subscriber identification function and the memory module function in a single removable device guaranteed a high level of integration. As the subscriber identification device and the memory controller at least one common connection for the Use exchange of information with the terminal controller, is achieved a high level of simplicity.

[0007] In Advantageously, the subscriber identification device a connection device for connecting a removable subscriber identification module card on. In this case, that carries removable memory module a connector or a connection device for the introduction a separate subscriber identification module card.

[0008] alternative includes the subscriber identification device in an advantageous manner Way a subscriber storage device for storing the subscriber identification information. In this case, the subscriber identification function is in the removable memory module integrated, and the subscriber storage device forms a permanent part of the memory module.

[0009] Especially can the switching devices by appropriate control signals easily be controlled, and they are easy to integrate, so that entire removable memory module on a highly integrated IC technology can be based Advantageously, the concerned at least a connection which selectively connects to the subscriber identification device and said memory controller is connected to a data input / output connection This data is stored in the memory device or subscriber information provided by the subscriber identification device is selectively connected to the same or the same connection or connecting device issued, which line the respective data with a corresponding data input / output connector and the line the terminal control device combines.

[0010] In Advantageously, the respective switching device by the Terminal control means controlled. In this case, the terminal control device sends a control signal to the respective switching device to the relevant line between the memory controller and the subscriber identification device to switch.

[0011] alternative is the respective switching device in an advantageous manner the memory controller controlled. At this time, the memory controller transfers a control signal to the respective switching device to this between the subscriber identification device and the respective line the memory controller to switch

[0012] The mobile terminal according to the present invention therefore integrates the subscriber identification function and an additional one Memory function in a separate removable device in a simple and effective way. In particular, the integration reduces these two functions in a single device the space requirement in the mobile terminal. By exploiting the same interface or interface connections for the subscriber identification device and the memory control device the removable memory module is also the number of necessary Compounds significantly reduced.

[0013] In The following description will be advantageous embodiments of the present invention with reference to the accompanying drawings explained in more detail. In the drawings show

[0014] 1 a mobile terminal and a first embodiment of the removable memory module according to the present invention and

[0015] 2 A second embodiment of a removable memory module according to the present invention for use with in FIG 1 represented mobile terminal.

[0016] 1 shows a mobile terminal 1 for a wireless telecommunication system, such as the GSM or UMTS system. The mobile device 1 includes all the necessary elements for operation in a wireless telecommunications system, such as input keys, a display, a speaker, a microphone, an antenna, and the like. For the sake of clarity, only the elements which are important and necessary for the present invention are shown.

[0017] The mobile device 1 has a terminal controller 2 for controlling the functions of the mobile terminal 1 on. The terminal control device 2 For example, it may be a microcontroller, a microchip, or the like. The terminal control device 2 is particularly for controlling the information exchange with a removable memory module 5 suitable as in the first embodiment in 1 shown is, or with a removable memory module 12 as in a second embodiment in 2 is shown. It will be appreciated that the removable memory modules 5 and 12 , in the 1 or in 2 are shown, are shown only schematically and that their actual sizes are considerably smaller compared to the size of the mobile terminal 1 according to the present invention.

[0018] The terminal control device 2 of the mobile terminal 1 has a group 3 from input / output connections or input / output pins connected to a corresponding connection or interface of an interface device 4 are connected. The removable memory module 5 or 12 is capable of interfacing with the interface device 4 to be releasably connected, for example by means of a Einschnappverbindung or the like.

[0019] The interface device or the interface 4 of the mobile terminal 1 includes, as in 1 a bus state port BS connected to a corresponding bus state pin of the terminal controller 2 for providing a bus state signal for a connected memory module 5 or 12 connected is. Furthermore, the interface device comprises 4 a data input / output connection, or a data input / output port, connected to a corresponding data input / output pin IO of the terminal controller 2 for an exchange of input / output data with a connected memory module 5 or 12 connected is. The interface device 4 also comprises a clock signal connection or a clock signal

connection SCLK, which is connected to a corresponding clock signal pin CLK of the terminal control device 2 to provide a clock signal to a connected removable memory module 5 or 12 connected is. Furthermore, the interface device comprises 4 a control voltage terminal VCC connected to a corresponding control voltage pin VCC of the terminal controller 2 for providing a control voltage for a removable memory module 5 or 12 connected is. The interface device 4 further comprises a permanent voltage terminal VSS connected to a corresponding permanent-voltage pin VSS of the terminal controller 2 to provide a steady state voltage to the attached removable memory module 5 or 12 connected is. Typically, the steady voltage terminal VSS is the terminal controller 2 connected to earth or ground. The interface device 4 may further comprise a spare terminal RES connected to a corresponding output pin OUT of the terminal controller 2 connected is. For example, the spare port RES represents a dedicated port for further use, which is designed to provide space for future enhancements of functionality.

[0020] In the case of in 1 shown first embodiment, the terminal control device 2 a control signal via the output / output pin OUT and the spare terminal RES of the interface device 4 to the attached removable memory module 5 starting to switch the switching devices 9 as explained in detail below. In the case of in 2 illustrated second embodiment of the removable memory module 12 becomes the reserve connection or reserve connection of the interface device 4 not needed to the removable memory module 12 to control.

[0021] This in 1 illustrated removable storage module 5 has a number of electrical connections or terminals connected to the terminals BS, DIO, SCLK, VCC, VSS and RES of the interface device 4 of the mobile terminal 1 to connect. The removable memory module 5 further comprises a memory controller 6 for controlling a storage device 7 on. The memory controller 6 For example, it may be a microprocessor, a microcontroller or the like. The memory control device 6 controlled storage device 7 is a storage device into which data can be written and read from the data.

[0022] Further, the removable storage module has 5 a subscriber identification device 8th for providing subscriber identification information. The subscriber identification device 8th is either a connection device for the connection of a removable subscriber identification module card or it comprises a subscriber memory device for storing a subscriber identification information. In the latter case, the subscriber identification device 8th a subscriber identification control device for controlling the reading and writing of subscriber data from or to the subscriber storage device.

[0023] The respective switching device 9 connects some of the connections or ports of the removable memory module 5 selectively with appropriate connections or connections of the subscriber identification device 8th and the memory controller 6 to control and make data exchange as required. A first switching device 9 is between the bus state signal terminal BS of the memory module 5 , a reset signal terminal RST of the subscriber identification device 8th and a bus state signal terminal of the memory controller 6 connected. A second switching device 9 is between the data input / output terminal DIO of the memory module 5 a subscriber data input / output port SIO of the subscriber identification device 8th and a data input / output port of the memory controller 6 connected. A third switching device 9 is between the clock signal terminal SCLK of the memory module 5 , a clock signal terminal CLK of the subscriber identification device 8th and a clock signal terminal of the memory controller 6 connected. The first, second and third switching devices 9 are connected to the reserve terminal RES of the memory module 5 connected to selectively and simultaneously between the respective terminals of the memory controller 6 and the subscriber identification device 8th to be switched.

[0024] The first, second and third switching devices 9 For example, they may be configured as shown in FIG 1 is shown enlarged. In the illustrated example, the first, second and third switching devices comprise 9 each a first diode 10 and a second diode 11 , A control signal CTL, which via the reserve terminal RES of the first diode 10 is supplied directly, is used as the inverted signal of the second diode 11 fed. In response to a supplied control signal CTL, an input signal ON, such as a signal supplied from one of the terminals BS, DIO or SCLK, is applied via either the first diode 10 to the corresponding terminal of the subscriber identification device 8th or via the second diode 11 to the memory controller 6 issued. The control device CTL is operated by the terminal control device 2 powered by the OFF pin depending on which of the functionalities of the memory module 5 needed.

[0025] Thus, the terminals BS, DIO and SCLK of the memory module become 5 selectively from the subscriber identification device 8th or from the memory controller 6 depending on which of the functionalities of the terminal control device 2 be requested or are. In the case that the first, second and third switching devices 9 to the subscriber identification device 8th are switched, which is the terminal control device 2 Bus state signal supplied via the corresponding bus state signal terminals BS in the subscriber identification module 8th used as reset signal. Likewise, one or more clock signals received from the terminal controller 2 be supplied via the corresponding clock signal terminals SCLK, as a clock signal in the subscriber identification device 8th used. The subscriber identification data may be sent to the subscriber identification device 8th via the corresponding data input / output terminals DIO delivered or from the subscriber identification device 8th for the terminal control device 2 to be read. In the case that the first, second and third switching devices 9 to the memory controller 6 , a bus state signal output via the bus state signal terminal BS and a clock signal output via the clock signal terminals SCLK are used in a corresponding manner. Data is transferred via the data input / output terminals DIO under the control of the memory controller 6 between the storage device 7 and the terminal controller 2 replaced.

[0026] It should be noted that the control voltage terminal VCC and the long-voltage terminal VSS are also connected with the memory controller, if necessary 6 and / or with the subscriber identification device 8th are connected. However, their functions are not important to the understanding of the present invention, which is why no connections or connections are shown. Furthermore, the interface device or the interface 4 as well as the removable memory module 5 have additional connections or connections, not shown, which are necessary for other required functions.

[0027] The same is true for the subscriber identification device 8th too, the more than the three in 1 or 2 may have shown connections, such as an additional terminal for delivering a variable supply voltage, such as a programming voltage or the like.

[0028] The subscriber identification device 8th and the memory controller 6 do not necessarily require the same number and type of clock signals, so the terminal controller 2 the respective required clock signals via the clock signal connections or connections SCLK can deliver depending on which of the two units is addressed. The same applies to the bus state signal supplied by the terminal controller 2 is output via the bus state signal connections which can be changed depending thereon, such as the setting of the switching devices 9 is. Regarding the removable memory module 5 according to the in 1 The first embodiment shown controls and changes the terminal controller 2 the settings of the first, second and third circuit devices 9 directly by a control signal, which is delivered via the re served connections RES. Here is the setting of the first, second and third switching devices 9 upon receiving a control signal from the terminal controller 2 here changed directly.

[0029] 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 those in relation to the in 1 illustrated removable storage module 5 are illustrated and explained. The main difference is that the reserve connection or reserve connection RES of the interface device 4 is not necessary to provide a control signal to change the settings of the switching devices 13 and 14 which indicate the respective connections of the interface devices 4 , the subscriber identification device 8th and the memory controller 6 connect. In the in 2 shown removable storage module 12 According to the second embodiment, the clock signal terminal SCLK of the memory module 12 directly and constantly with the clock signal terminal CLK of the subscriber identification device 8th and the clock signal terminal CLK of the memory controller 6 connected. The first switching device 13 is between the bus state signal terminal BS of the memory module 12 , the reset signal terminal RST of the subscriber identification device 8th and the bus state signal terminal of the memory controller 6 connected. The second switching device 14 is between the data input / output port of the memory module 12 , the data input / output port IO of the subscriber identification device 8th and the data input / output port of the memory controller 6 connected. The first switching device 13 and the second switching device 14 are each via a switching control signal terminal SWCTL of the memory controller 6 connected and controlled via this port. This provides the first switching device 13 a controlled three-state switching device as the first, second and third switching devices 9 of in 1 illustrated memory module 5 while the second switching device 15 of the memory module 12 is only a controlled two-state delivery switch. In other words, this means that the first switching device 13 selectively the bus state signal terminal BS between the respective connections or terminals of the subscriber identification device 8th and the memory controller 6 on. On the other hand, the data input / output terminal is DIO of the memory module 12 continuously and directly with the data input / output terminal IO of the memory controller 6 connected. The second

IPR2025-00645 Page 01592

switching device 15 selectively connects the data input / output port DIO of the memory module 12 and the data input / output terminal IO of the memory controller 6 with the data input / output port IO of the subscriber identification device 8th , Thus, even during the access of the terminal controller 2 to the subscriber identification device 8th the data exchange by the memory controller 6 supervised. When the terminal control device 2 of the mobile terminal 1 the removable memory module 12 the first time it sends a first command to the memory controller 6 , for example, via the bus state signal terminal BS. The first switching device 13 thus normally becomes the memory controller 6 switched and the second switching device 14 is open (switched off). In the case that the terminal control device 2 wishes, the memory controller 6 and the storage device 7 to address, the settings of the first switch remain 13 and the second switch 14 unchanged. In the case that the terminal control device 2 wishes to the subscriber identification device 8th to access, gives the memory controller 6 upon receiving a corresponding command, a control signal via its switching control terminal SWCTL from which at the same time the first switching device 13 and the second switching device 14 such that the participants identification device 8th can be addressed. While the terminal control device 2 to the subscriber identification device 8th accesses, the data exchange by the memory controller 6 supervised. When the memory controller 6 the end of data transfer between the terminal controller 2 and the subscriber identification device 8th detects, for example, after determining that a certain amount of time has passed without any data has been transmitted, the memory controller 6 automatically another or different control signal via the switching control terminal SWCTL from, whereby the first switching device 13 and the second switching device 14 be switched back in their initial position.

[0030] Thus brings the memory module 12 according to the second embodiment in comparison to the memory module 5 in the first embodiment, the advantage that a connection is less required to control the setting of the switches. On the other hand, the required processing is more complex.

[0031] As in 2 shown enlarged, the second switching device 14 a diode 15 exhibit. One of the switching control terminal SWCTL of the memory controller 6 output control signal CTL is called the inverted signal of the diode 15 supplied to the data input / output terminal IO of the subscriber identification device 8th selectively connect or disconnect. The configuration of the first switching device 13 of the memory module 12 can for example, the configuration or the structure of the switching device 9 match that in 1 is shown enlarged. The other functionalities and configurations of the subscriber identification device 8th , the memory controller 6 , the storage device 7 and the various connection points of the memory module 15 correspond identically to the functionalities or configurations, which in relation to the in 1 illustrated memory module 5 have been explained.

Patent Citations (2)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US5633484A *	1994-12-26	1997-05-27	Motorola, Inc.	Method and apparatus for personal attribute selection and management using a preference memory
FR2748883B1 *	1996-05-17	1999-02-12	Gemplus Card Int	COMMUNICATION SYSTEM ALLOWING SECURE AND INDEPENDENT MANAGEMENT OF A PLURALITY OF APPLICATIONS BY EACH USER CARD, USER CARD AND CORRESPONDING MANAGEMENT METHOD

* Cited by examiner, † Cited by third party

Cited By (15)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7058116982 *	2002-02-26	2006-05-23	Kyocera Wireless Corp.	Memory configuration for a wireless communications device
KR100486525B1 *	2002-07-05	2005-05-03	엘지전자 주식회사	Transport protocol data unit transmission method for mobile communication device
US20060098405A1 *	2004-11-08	2006-05-11	Bloebaum Leland S	Combined mass storage and subscriber identity module and apparatus for use therewith
US7856249B2	2004-11-08	2010-12-21	Sony Ericsson Mobile Communications Ab	Combined mass storage and subscriber identity module providing information security and apparatus for use therewith
US7588178B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060226217A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card
CN100446600C *	2005-09-22	2008-12-24	华为技术有限公司	Extending system and its method for mobile terminal storage space
WO2007107166A1 *	2006-03-21	2007-09-27	Anwar Reda Sedra Henein	Back-up device for a mobile telephone
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
DE102007006570A1 *	2007-02-09	2008-08-14	Giesecke & Devrient Gmbh	Method for backing up data of a mobile terminal
US8742287B2	2007-12-14	2014-06-03	Tyfone, Inc.	Memory card based contactless devices
DE102008012082A1 *	2008-02-29	2009-09-24	T-Mobile International Ag	Memory card with integrated SIM
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8485112B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
DE60026768T2	2006-11-09	Mobile terminal with removable memory and SIM card function
DE69938549T2	2009-07-23	IMPROVED CELLULAR GSM TERMINAL
DE19607509B4	2008-04-03	Dual card
DE602004007402T2	2008-03-13	EFFICIENT CONNECTION BETWEEN MODULES OF REPLACEABLE ELECTRONIC CIRCUITS
DE69626763T2	2004-02-05	Multichip IC card and usage system
DE102004015535B4	2009-01-29	Data transmission interface and method
DE69933863T2	2007-06-21	COMMUNICATION PROCESS AND DEVICE
EP1832093B1	2011-10-19	Testing apparatus used in a testing system for checking transmission processes in a mobile radio communication network
DE69400549T3	2006-12-21	IC card transmission system
EP0882274B1	1999-10-06	Device for processing and storage of data
EP0614302A1	1994-09-07	Telecommunication device comprising a terminal with interfaces for a chip card and a memory card
DE102013112314A1	2014-05-22	Mobile terminal
DE69921880T2	2005-11-24	Chip card with a memory content transfer control unit and data storage method in a chip card
DE69735118T2	2006-08-03	Expansion card, card interface and electronic device
DE10311966A1	2004-12-16	smart card
EP1800234B1	2010-06-09	Electronic module for programming chip cards comprising and/or without contacts
DE69334063T2	2007-04-05	Control system for a timer
DE10052619C1	2002-03-28	Modular electrotechnical system has contacts of multi-pin connector between base unit and plug-in unit divided into groups cooperating with fixed configuration and variable configuration lines respectively
DE102005036267B4	2007-06-21	Memory arrangement and method for addressing a memory arrangement
EP1826680B1	2008-08-20	Method for operating an expansion card
DE4136014A1	1992-05-14	Lap-top computer with modem control functions and extended unit - determines usage of modem addresses in extended unit and deactivates modem accordingly
EP1031599B1	2008-11-05	Multiprocessor system
WO2002099729A2	2002-12-12	Electronic circuit for chip card interfaces and method for communication with chip card interfaces
WO2009033688A2	2009-03-19	Mass memory card
WO2002067610A2	2002-08-29	Method, telecommunication device and computer programme for operating a mobile telecommunication device on at least two mobile radio standards

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
EP20000120475	2000-09-19	2000-09-19	Mobile terminal with removable memory having SIM card function

Legal Events

Date	Code	Title	Description
2007-04-12	8364	No opposition during term of opposition	

Data provided by IFI CLAIMS Patent Services

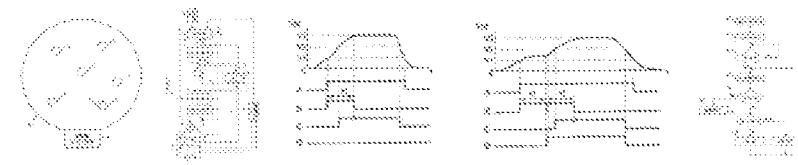
IPR2025-00645 Page 01595

Patents JP3614157

JP3614157B2 -- RFID tag and method for adjusting resonance frequency in RFID tag

RFID tag and method for adjusting resonance frequency in RFID tag

Images (10)



Classifications

G06K19/0726 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e.g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips the record carrier comprising an arrangement for non-contact communication, e.g. wireless communication circuits on transponder cards, non-contact smart cards or RFIDs the arrangement including a circuit for tuning the resonance frequency of an antenna on the record carrier

View 3 more classifications

JP3614157B2

Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: 裏…部 福岡

Worldwide applications

2002 JP 2002 ES DE AT US CN

Application JP2002221841A events

2002-07-30 Application filed by オムロン株式会社

2002-07-30 Priority to JP2002221841A

2004-02-26 Publication of JP2004062665A

2005-01-26 Application granted

2005-01-26 Publication of JP3614157B2

Status Expired - Fee Related

2022-07-30 Anticipated expiration

Info: Patent citations (8), Cited by (65), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (4) Hide Dependent

1. An RFID tag,
A switching circuit for turning on and off an inductance forming a resonance circuit and a plurality of resonance capacitors or at least one connection of the plurality of resonance capacitors;
A constant voltage circuit for smoothing a power signal supplied from the interrogator (reader / writer) through the resonance circuit and outputting a constant voltage;
Voltage detecting means for detecting the smoothed voltage;
Voltage monitoring means for monitoring the degree of rise of the smoothed voltage;
A resonance capacitance switching command means for commanding on / off of the switching circuit in response to an output of the voltage monitoring means when a predetermined increase cannot be obtained;
The voltage monitoring means is
A first voltage detection circuit that outputs a detection output when the output from the constant voltage circuit reaches a first voltage, and a timer circuit that receives the output of the first voltage detection circuit and outputs a timer signal for a predetermined period When,
A second voltage detection circuit for outputting a detection output when the output of the constant voltage circuit reaches a second voltage higher than the first voltage;
While the timer circuit outputs the timer signal, when the output from the second voltage detection circuit is not obtained, the switching circuit is driven to reduce the capacitance value of the resonance capacitor, while the timer signal the operation before Symbol switching circuit after the output has exceeded the predetermined time,
RFID tag, characterized in that to return the resonant circuit to an initial state.

2. The resonance capacitor has a fixed capacitor and at least one adjustment capacitor When the resonance frequency increases, the resonance capacitor is disconnected, and the capacitance value of the resonance capacitor is reduced. 2. The RFID tag according to claim 1, wherein the RFID tag is controlled so as to approach a resonance frequency defined by.

3. When there are a plurality of adjustment capacitors, the voltage monitoring unit sequentially disconnects the adjustment capacitors every predetermined period, all the adjustment capacitors are disconnected, and the second voltage higher than the first voltage. 2. The RFID tag according to claim 1, wherein when the voltage cannot be reached, the resonance circuit is returned to the initial state.

4. At least one on-off of the above connection of the inductance and a plurality of resonance capacity or the plurality of resonance capacities to form a resonant circuit carried out by the switching circuit,
The constant voltage circuit outputs a constant voltage by smoothing the power signal given from the interrogator (reader / writer) via the resonance circuit,
A voltage detection means detects the smoothed voltage,
The voltage monitoring means monitors the degree of increase in the smoothed voltage,
When the predetermined increase cannot be obtained, the switching of the switching circuit is commanded by the resonance capacitance switching command means in response to the output of the voltage monitoring means,

IPR2025-00645 Page 01596

In the voltage monitoring means, when the output from the constant voltage circuit reaches the first voltage, the first voltage detection circuit outputs a detection output, and the timer circuit receives the output of the first voltage detection circuit. A timer signal for a predetermined period is output, and when the output of the constant voltage circuit reaches a second voltage higher than the first voltage, the detection output is output by the second voltage detection circuit, and the timer circuit outputs the timer signal. When the output from the second voltage detection circuit is not obtained during the output, the switching circuit is driven to reduce the capacitance value of the resonance capacitor, while the output of the timer signal has passed a predetermined period the operation before Symbol switching circuit after adjustment method of the resonance frequency in the RFID tag, characterized in that to return the resonant circuit to an initial state.

Description

[0001]
BACKGROUND OF THE INVENTION
The present invention relates to an RFID tag andMethod for adjusting resonance frequency in RFID tagAbout.
[0002]
[Prior art]
FIG. 1 shows a system overview of an RFID tag and an RFID interrogator using the RFID tag. In FIG. 1, reference numeral 1 denotes an RFID tag. The interrogator 2 (reader / writer) has a detection area 3 having a predetermined spread. That is, in this system, there may be a plurality of tags 1, 1.
[0003]
[Problems to be solved by the invention]
RF for books, envelopes, casino chips, etc.IDWhen the tag 1 is mounted, if the tags 1 overlap each other, there is a problem that the communication performance is remarkably lowered and the interrogator (reader / writer) 2 cannot be accessed successfully. In these applications, RFIDTag 1 stacked, orRFIDWith tag 1RFIDThere is a case where the interval between the tags 1 is set very close.
[0004]
In that state, L (inductance of the resonance coil) of both tags 1 is mutually coupled, and the mutual inductorNTend to form, and the inherent inductance of the tag 1 tends to increase in conjunction with the mutual inductance.
[0005]
This meansRFIDSince the resonance capacitor existing in the tag 1 has a constant value, the resonance frequency is lower than the state where there is no mutual coupling (the expected resonance frequency and the frequency specified by the interrogator). Means.
[0006]
On the other hand, from the interrogator (reader / writer) 2 sideRFIDOscillation is performed at the same frequency as the resonance frequency of tag 1 (expected resonance frequency). This meansRFIDResonance point decreased due to overlap of tag 1 etc.RFIDFrom the viewpoint of the tag 1, this means that a magnetic field whose resonance has shifted is supplied from the interrogator (reader / writer) 2 side antenna, and the supplied energy is reduced accordingly As a result, the communication distance is reduced.
[0007]
RFIDin order to eliminate the decrease in communication distance due to the overlapping of the tags 1, JP 2000-151480 A discloses an identification method when a plurality of tags are superimposed. This is where the built-in tagNAlthough a configuration is described in which the resonance frequency can be changed by switching the switch, a method of adjusting the built-in capacitor for each tag among a plurality of superimposed tags to adjust to the desired frequency States. The resonance frequency of other tags is changed sequentially after the communication with one tag is completed.
[0008]
In the case of this method, it is possible to match the resonance frequency of one tag with the resonance frequency emitted by the interrogator, but the resonance frequency of the other tag deviates from the resonance frequency emitted by the interrogator. Therefore, a general collision prevention procedure (for example, JIS6323-3 ISO / IEC15693-3) is not used, and the interrogator and the tag perform one-to-one communication.
[0009]
In addition, there is no method for determining the order between multiple tags (from which tag the resonance frequency is adjusted), and it is difficult to ensure stable operation as a realistic system, and difficult to realize. There is a problem.
[0010]
The present invention has been made to solve such a problem, and an object of the present invention is to effectively use a collision prevention related function called anti-collision, which has a simple configuration and can realize a stable system operation.Method for adjusting resonance frequency in RFID tagIs to provide.
[0011]
[Means for Solving the Problems]
RFIDThe following is a brief description of the problems that occur with tag superposition. That is, RFIDThe coil inductance L of the tag causes mutual inductance due to overlapping with other tags, and the L value is increased accordingly. Therefore, by reducing the value of C for resonance corresponding to the increment of L, the resonance frequency is always kept constant, thereby solving problems such as insufficient rise in power supply voltage. In addition, the configuration consists of a plurality of resonance capacitors, and by separating this resonance capacitor configured under certain conditions, the capacitor value is reduced, and the decrease in resonance frequency caused by the increase in mutual inductance is corrected. To do.
[0012]
In order to solve the above problems, an RFID tag according to the present invention includes an inductance forming a resonance circuit and a plurality of resonance capacitors, or at least one of the plurality of resonance capacitors.ConnectedA switching circuit for performing on / off, a constant voltage circuit for smoothing a power signal supplied from an interrogator (reader / writer) via the resonance circuit and outputting a constant voltage, and for detecting the smoothed voltage Voltage detecting means, voltage monitoring means for monitoring the degree of rise of the smoothed voltage, and resonance for commanding on / off of the switching circuit in response to the output of the voltage monitoring means when a predetermined increase cannot be obtained. Capacity switching command means, and the voltage monitoring means outputs a detection output when the output from the constant voltage circuit reaches a first voltage, and the first voltage detection circuit. A timer circuit that receives the output of the circuit and outputs a timer signal for a predetermined period, and a second circuit that outputs a detection output when the output of the constant voltage circuit reaches a second voltage higher than the first voltage. And when the output from the second voltage detection circuit cannot be obtained while the timer circuit outputs the timer signal, the switching circuit is driven to set the capacitance value of the resonance capacitor. While the output of the timer signal has passed a predetermined periodPreviousThe resonance circuit is returned to the initial state by the operation of the switching circuit
[0013]
Further, the resonance capacitor according to the present invention has a fixed capacitor and at least one adjustment capacitor, and when the resonance frequency increases, the adjustment capacitor is disconnected and the capacitance value of the resonance capacitor is reduced. Control is performed so as to approach the resonance frequency defined by the interrogator.
[0014]
Further, the voltage monitoring means according to the present invention, when there are a plurality of adjustment capacitors, sequentially disconnect the adjustment

capacitors every predetermined period, all the adjustment capacitors are disconnected, andHigher than the first voltageThe resonance circuit is returned to the initial state when the second voltage cannot be reached.

[0015]

Furthermore, the method for adjusting the resonance frequency in the RFID tag according to the present invention includes an inductance forming a resonance circuit and a plurality of resonance capacitors, or at least one of the plurality of resonance capacitors.ConnectedON / OFF is performed by a switching circuit, the power signal supplied from the interrogator (reader / writer) through the resonance circuit is smoothed and the constant voltage circuit outputs a constant voltage, and the voltage detection means detects the smoothed voltage. Then, the voltage monitoring means monitors the degree of rise of the smoothed voltage, and when a predetermined increase cannot be obtained, the switching of the switching circuit is commanded by the resonance capacitance switching command means in response to the output of the voltage monitoring means. In the voltage monitoring means, when the output from the constant voltage circuit reaches the first voltage, the first voltage detection circuit outputs a detection output, and receives the output of the first voltage detection circuit to receive a timer. The circuit outputs a timer signal for a predetermined period, and when the output of the constant voltage circuit reaches a second voltage higher than the first voltage, the second voltage detection circuit outputs a detection output. While the timer circuit outputs the timer signal, when the output from the second voltage detection circuit cannot be obtained, the switching circuit is driven to reduce the capacitance value of the resonance capacitor, while the timer signal After the output has passed a predetermined periodPreviousThe resonance circuit is returned to the initial state by the operation of the switching circuit.

[0016]

ThisThe invention ofit is possible to switch the resonance capacity of the resonance circuit and stably update the data of the resonance frequency with the interrogator (reader / writer).

[0017]

DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the present invention will be described below with reference to the accompanying drawings. 2 is a block diagram of the main part of one embodiment of the RFID tag according to the present invention, FIG. 3 is a waveform diagram of the RFID tag according to the present invention, FIG. 4 is another waveform diagram of the RFID tag according to the present invention, FIG. FIG. 2 is an operation flowchart of one embodiment of an RFID tag according to the present invention. In FIG. 2, voltage detection means 8 and 11 are voltage monitoring means, latch circuit 15 is resonance capacitance switch command means, control circuit 12, UID storage means 16 and data modulator / demodulator 17 are anti-collision information output means, respectively. Constitute.

[0018]

The RFID tag 1 includes a parallel resonance circuit 4 including a coil L, a resonance capacitor C1, and an adjustment capacitor C2. Since the initial state of the switching circuit SW1 made of a semiconductor such as a CMOS-FET is ON, the adjustment capacitor C2 and the resonance capacitor C1 are connected in parallel and included in the resonance circuit 4 in the initial state. The resonance circuit 4 resonates when entering a high-frequency magnetic field (corresponding to the detection area 3 in FIG. 1) provided by the antenna of the interrogator (reader / writer) 2, and the resonance output is applied to the rectifier circuit 5.

[0019]

As a result, the rectifying circuit 5 outputs a direct current component (rectification result) corresponding to the degree of coupling between the RFID tag 1 and the interrogator (reader / writer) 2 antenna. This DC component is smoothed by the smoothing capacitor 6 and stabilized by the constant voltage circuit 7. However, the output of the constant voltage circuit 7 is stabilized after a predetermined time has elapsed since the RFID tag 1 entered the detection area 3, and the output Vcc of the constant voltage circuit 7 at the beginning of the entry is not stable. This is important for the present invention and will be described in detail below.

[0020]

On the other hand, various commands received from the interrogator (reader / writer) 2 via the coil L are demodulated by the data modulator / demodulator 17, and the demodulated commands are supplied to the control circuit 12 for processing. The control circuit 12 collates the UID included in the command with the UID of the UID storage means 16, and outputs the UID to the data modulator / demodulator 17 if they match, and the data modulator / demodulator 17 modulates the UID. The UID is transmitted to the interrogator (reader / writer) 2 through the coil L.

[0021]

When the control circuit 12 receives the data call request or data write request received from the interrogator (reader / writer) 2 via the coil L --- data modulator / demodulator 17, the control circuit 12 reads the requested data from the UID storage means 16. Output or write the requested data to the UID storage means 16.

[0022]

When receiving a command response prohibition request from the interrogator (reader / writer) 2, the control circuit 12 sets the prohibit mode and prohibits the response to the command as long as power is supplied thereafter.

[0023]

If it demonstrates using the waveform of FIG. 3, the constant voltage output Vcc will be 0 initially. As the RFID tag 1 enters the detection area 3, Vcc increases. When the voltage V1 is reached, the voltage V1 is detected by the first voltage detection circuit 8, and the voltage detection circuit 8 raises the detection output A.

[0024]

This output A is applied to the timer circuit 10 via an exclusive OR circuit 9. This timer circuit 10 is triggered by the rising or falling of its input. In this case, as shown by the signal waveform B in FIG. 3, the timer circuit 10 outputs a timed signal B for a predetermined timer time t1.

[0025]

When the constant voltage output Vcc reaches a higher voltage V2 during the timer time t1, the voltage V2 is detected by the second voltage detection circuit 11, and the detection output C rises. thisDetection outputC is applied to the reset terminal 13 of the control circuit 12. When the detection output C applied to the reset terminal 13 rises, the control circuit 12 can perform an original operation such as access to the interrogator (reader / writer) 2 or the like. In other words, thisDetection outputWhen C is at a low level, the control circuit 12 is held in a reset state, and at least its output section is immobilized so that no unnecessary signal is output. The above shows the case where the RFID tag 1 enters the detection area 3 of the interrogator (reader / writer) 2 and operates normally.

[0026]

Next, the case where it cannot be said that it is normal compared with FIG. 3 is demonstrated using the waveform of FIG. The power supply voltage Vcc in FIG. 4 does not rise smoothly compared to the waveform diagram 3. As described above, as described above, there are various cases where a plurality of RFID tags 1 are overlapped with each other and are located relatively far from the interrogator (reader / writer) 2.

[0027]

This unusual state is shown in FIG. 4, and in the operational flow diagram of FIG.Sit corresponds to 5 or later. That is, when the RFID tags 1 overlap each other, the power supply voltage Vcc cannot reach the voltage V2 even after the timer time t1 has elapsed after reaching the voltage V1. That is, the output C of the voltage detection circuit 11 that detects the voltage V2 remains at a low level.

[0028]

On the other hand, when the timer time t1 elapses in this state, the timer circuit 10fallsoutputSignal waveformB falls, and this fall is applied to the clock terminal CK of the latch circuit 15 via the OR circuit 14, and the output D of the latch circuit 15 is inverted. Thus, when the output of the latch circuit 15 is inverted, the output (inverted D) connected to the switching circuit SW1 is inverted from high to low, and the switching circuit SW1 is turned off.

[0029]

As a result, the adjustment capacitor C2 is disconnected from the resonance circuit 4, the resonance frequency of the resonance circuit 4 increases, and approaches the resonance frequency defined by the interrogator (reader / writer) 2. As a result, the power supply voltage Vcc rises as shown in FIG. When the power supply voltage Vcc reaches the operating voltage V2 of the circuit, the output C of the voltage detecting circuit 11 changes from low to high as described in the previous example, and the

IPR2025-00645 Page 01598

control circuit 12 enters the operating state. As a result, the corresponding RFID tag 1 can be accessed with the interrogator (reader / writer) 2.

[0030]

The above is an effective compensation operation in the case where the RFID tag 1 is superimposed and there is mutual interference. However, this compensation operation sometimes becomes a problem. That is, in the case of an application in which the RFID tag 1 moves and enters the communication area 3, even when the RFID tag 1 is alone, the operation is performed when the distance from the interrogator (reader / writer) 2 is long. It does not reach the level of the possible voltage V2, but reaches the voltage V1 that triggers the timer circuit 10.

[0031]

In this case, when the adjustment capacitor C2 is switched, the above-described compensation operation causes the resonance frequency of the RFID tag 1 to deviate from the desired resonance frequency, greatly reducing the communication distance of the corresponding single RFID tag 1. It will be.

[0032]

To improve this, the operation when the timer circuit 10 times up again is shown in the signal B of the waveform in FIG. That is, when the power supply voltage Vcc does not reach the voltage V2 at the second timer time t1, the timer circuit 10Butoutput Signal waveformWhile B falls, the voltage detection circuit 11Detection The output C is at a low level unlike the previous example. For this reason, the output of the OR circuit 14 falls. As a result, the state of the latch circuit 15 in which the output of the OR circuit 14 is applied to the clock terminal CK is reversed again, the switching circuit SW1 is turned on, the adjustment capacitor C2 is connected, and the resonance circuit 4 Return to state.

[0033]

As a result, since the distance from the interrogator (reader / writer) 2 is initially far, the power supply voltage Vcc is changed to the operating voltage V2.InThe RFID tag 1 that could not be reached also moves the interrogator (reader / writer) 2inAs the distance approaches, the power supply voltage Vcc increases. When the power supply voltage Vcc rises and reaches the voltage V2, the voltage V2 is detected by the voltage detection circuit 11, and the control circuit 12 is set to an accessible state in which communication with the interrogator (reader / writer) 2 is possible.

[0034]

Thus, for example, as shown in a part of FIG. 1, even when the RFID tags 1 and 1 are overlapped and superimposed, each resonance frequency is defined by the interrogator (reader / writer) 2. The access state can be set close to the frequency, the power supply voltage Vcc is secured, and signals can be transmitted and received between each RFID tag 1 and the interrogator (reader / writer) 2 relatively easily. Can do.

[0035]

Next, an anti-collision (multiple responder recognition) technique for distinguishing each RFID tag will be described. Here, an embodiment will be described based on Japanese Industrial Standard (JIS) X6323-3 (ISO / IEC 15693-3) "IC Card without External Terminal—Nearby Type—Part 3: Collision Prevention and Transmission Protocol". Therefore, in order to further understand this embodiment, the above-mentioned standard published by the Japanese Standards Association is helpful.

[0036]

In the anti-collision algorithm adopted here, an inventory of a plurality of responders (RFID tags 1, 1, 1,...) Existing in the communication area 3 of the interrogator (reader / writer) 2 is used as a UID. It is extracted based on (unique number of tag).

[0037]

The interrogator (reader / writer) 2 can detect the presence of a plurality of responders (RFID tags) (the RFID tag itself as a responder)Interrogator (Reader / Writer)The existence of another responder can be known only from the information from 2), and the subject of the algorithm execution is the reader / writer 2.

[0038]

FIG. 6 shows a UID (tag unique number) that is information for identifying each RFID tag. In this embodiment, the UID is composed of 64 bits as shown in FIG. 6, and the binary display character length of the number of time slots is set as an area. Here, since the number of time slots is 16, the area is divided in units of 4 bits, and the UID is divided into 16 areas. This UID uniquely sets each RFID tag by 14 areas and 56 bits of the IC manufacturer code 4 area and the serial number 10 area in areas A, B, C, and D. The UID of the control circuit 12 of the RFID tag 1 Written and kept inside.

[0039]

Next, the anti-collision sequence will be described with reference to the operation flowchart shown in FIG. The operation flowchart shown in FIG. 7 shows the contents of a program stored and executed in the interrogator (reader / writer) 2. Here, a typical anti-collision sequence when the number of time slots is 16 will be described.

[0040]

First, in step S11, an area (mask data area) that stores interrogator mask-related data is initialized. In this initialization, the mask length data is set to 0, the mask value data is set to a predetermined value, and the area position data indicating the position where the UID (unique data) stored in the RFID tag is operated is also set to 0.

[0041]

When you are ready to issue a command,SAt 12, the reader / writer 2 sends an inventory command. As a result, an inventory command is transmitted to the plurality of RFID tags 1. Since each RFID tag 1 has a mask length of 0, UIA response is independently returned to the interrogator (reader / writer) 2 at its own time slot timing determined in the area 0 of D. Therefore, in many cases, each UID returns a response alone to the interrogator (reader / writer) 2 due to the access between the two, but the response may collide with some of the RFID tags 1.

[0042]

Correspondingly, the stepsS13NA signal on the RFID tag 1 side in response to the Bentley command is detected to detect the time slot position where the collision occurred. The detected time slot position is stored in the collision slot buffer 18 shown in FIG. This is to distinguish the RFID tag 1 that has collided, as will be described later. The collision slot buffer 18 is formed in the interrogator (reader / writer) 2.

[0043]

If there is no collision, the next stepSWhen the presence of the tag is detected normally at 14, the UID data of the corresponding RFID tag 1 is stored and held in the detection UID buffer 19 shown in FIG. This detection UID buffer 19 is also formed in the interrogator (reader / writer) 2. In this way, the time slot data and the UID data that have collided are accumulated in the buffers 18 and 19 of the interrogator (reader / writer) 2.

[0044]

Next, if there is a tag that was successfully detected, this is the stepSThe next control is executed in step S16. StepSIn 16, the interrogator (reader / writer) 2 refers to the contents of the detection UID buffer 19 described above, specifies the corresponding (having UID) tag by specifying its UID, and accesses the tag. That is, necessary data / information exchange is completed.

[0045]

After this access is complete,SIn 17, a command for setting a state in which no response is returned to the inventory command called STAY QUIET command is transmitted to the corresponding RFID tag 1, and the operation as a tag is stopped. (However, when the power is reset, the state returns to the response state.) As a result, the access to the corresponding RFID tag 1 at this timing is terminated, which is equivalent to the fact that the corresponding RFID tag 1 does not exist (is not in stock). Transition to the state.

[0046]

Then stepS18 to search for any other RFID tag 1 detected,S15, if another RFID tag 1 is detected, the above stepsSThe process corresponding to each RFID tag 1 is repeated by repeating steps 16 and thereafter. When processing of the RFID tag 1 detected normally is completed, the stepSThe determination result at 15 is No, and the control is stepSMoved to 20.

[0047]

StepSAt 20, it is determined whether or not there is a collided RFID tag 1 by looking at the contents of the collision slot buffer 18. When it is detected that there is a

IPR2025-00645 Page 01599

collision.SThe determination of 20 is Yes and the step.SAfter 21, a process for distinguishing the collided tags using the UID is executed.

[0048]

le first step.SIn 21, the first time slot position data among the time slots in which the collision has occurred is taken in as mask related data. In this embodiment, as described above, there are 16 time slots. Now, it is assumed that a collision has occurred at two locations of time slot 1 and time slot 4. In this example, "1", that is, binary data (0001) is stored as the first time slot position data. In addition, (0001) is stored / stored as mask value data.

[0049]

Next steps.S22, the initial value is 0 (step.S11 is added to the mask length. As a result, the mask length is set to 4 bits. Also, +1 is added to the area position, and as a result, UID area 1 (see FIG. 6) is selected as position data for designating the next time slot.

[0050]

In this way, when the condition to execute the next inventory command is met, control.S12 is moved to. The inventory command to be executed next is different from the previous contents, and is updated with "mask length is 4", "mask value is 0001", and "UID area position is 1". In this way, the updated inventory command is executed. In this case where there is a tag that has collided, a value (0001) that has once collided is entered as a mask, so there are always a plurality of RFID tags. However, since the "UID area position" that specifies the timing at which the RFID tag 1 returns a response is different from the previous time, the possibility of collision again becomes low. However, it cannot be said that there is nothing in principle.

[0051]

Anyway, when the inventory command is performed again like this, the same step as the previous step is performed accordingly.SRepeat steps 15, 16, 17, and 18. As a result, access to the interrogator (reader / writer) 2 is completed for the RFID tag 1 detected normally, and the collision state is.stateAs a result, the number of RFID tags 1 that cannot be accessed decreases gradually. However, in principle, it is not completely eliminated. Therefore, if the collision tag remains after this second inventory command execution, again step.SControl is transferred to 20, and the determination result is Yes. And then step.SThe process of updating the inventory commands 21 and 22 is executed again, and the third inventory command is stepped accordingly.S12 is executed.

[0052]

Thereafter, when this process of updating such a mask position is repeated and there is no colliding slot, it is a step.SThe determination result determined at 20 is No, and the control is now a step.S23. As a result, this time, the control to return the area position is a step.S24, 25, and steps.SThe process of repeating 19 is performed. This is to cover a dropout when a collision occurs in a plurality of slots at the same area position. A series of processing is performed, and when the area position returns to 0, the anti-collision sequence is completed. By repeating the process in this manner, it is possible to substantially eliminate the remaining RFID tag 1 that cannot be accessed due to a collision.

[0053]

Next, the simple collision handling algorithm shown in FIG. 10 will be described. The operation flow diagram shown in FIG. 10 is a simplified version of the anti-collision algorithm shown in FIG.SAt 31, a read command with a simple collision prevention function is executed. In this case, a command having a code indicating the order of the unique ID of the tag to start the collision prevention slot and a code indicating the location of data to be read from the tag is issued as the command. As a result, step.SAs indicated by 12 and 13, the collided time slot, the normally detected UID, and the desired read data are stored and held.

[0054]

Step if there is a collision.SThe determination result of 35 is Yes, and step again.SA read command 31 with a simple collision prevention function is executed. In this case, this step.SIn 31, instead of executing the fine algorithm shown in the flowchart of FIG. 7, the next command is executed with a simple algorithm. That is, the next command is executed by simply moving the slot start position to the next position.

[0055]

In this way, when the slot start position is simply moved, it is not possible to completely eliminate the occurrence of a collision with the same RFID tag 1 again. However, as described above, the RFID tag 1 is given a unique UID at least with 56 bits of the IC manufacturer code and serial number, and the slot start position is simply and easily moved as described above. Even if the executed command is executed, each RFID tag 1 can be almost identified by repeating it several times from the second time, and there is no problem or malfunction in a normal application.

[0056]

This has been confirmed by experiments and experiences of the inventors. The merit of adopting such a simple collision prevention algorithm is that the system configuration is simplified and maintenance is facilitated, and the access speed between the RFID tag 1 and the interrogator (reader / writer) 2 is increased. As a result, in an application in which the RFID tag 1 and the interrogator (reader / writer) 2 move relative to each other, the reliability of signal exchange is improved, which is advantageous in ensuring the reliability of the system. . In such a case, the simplified collision prevention algorithm can be positively adopted by selecting application conditions.

[0057]

In the above-described embodiment, as shown in the circuit diagram of FIG. 2, there is one adjustment capacitor C2. By providing a plurality of adjustment capacitors C2, finer adjustment is possible. However, as a result of various experiments conducted by the inventors, a single adjustment capacitor is almost sufficient when the anti-collision function is used.

[0058]

【The invention's effect】

As described above, according to the present invention, an anti-collision function is mounted on the RFID tag, and a switching circuit for switching on and off the resonance capacitor is provided. For this reason, if a certain level of power supply voltage / operating voltage on the RFID tag side is obtained, identification of each RFID tag can be surely performed by the anti-collision function. For this reason, even if the change in the resonance frequency is set relatively rough, a stable operation can be secured, and the practicality that the reliability of the entire system can be easily improved is extremely high.

[Brief description of the drawings]

FIG. 1 is a system overview of an RFID tag and an RFID interrogator using the RFID tag.

FIG. 2 is a block diagram of a main part of an embodiment of an RFID tag according to the present invention.

FIG. 3 is a waveform diagram of an RFID tag according to the present invention.

FIG. 4 is another waveform diagram of the RFID tag according to the present invention.

FIG. 5 is an operation flowchart of one embodiment of an RFID tag according to the present invention.

6 is a UID (tag unique number) information diagram for identifying an RFID tag according to the present invention. FIG.

FIG. 7 is an operation flowchart of the anti-collision sequence according to the present invention.

FIG. 8 is an area storage diagram of a collision slot buffer according to the present invention.

FIG. 9 is a UID data storage diagram of a detection UID buffer according to the present invention.

FIG. 10 is an operation flowchart of the simple collision handling algorithm according to the present invention.

[Explanation of symbols]

1 RFID tag

2 Interrogator (reader / writer)

3 Detection area

4 Resonant circuit

5 Rectifier circuit

IPR2025-00645 Page 01600

6 Smoothing capacitor
7 Constant voltage circuit
8,11 Voltage detection circuit
9 Exclusive OR (Exclusive OR) circuit
10 Timer circuit
12 Control circuit
13 Reset terminal
14 OR circuit
15 Latch circuit
16 UID storage means
17 Data modulator / demodulator
18 Collision slot buffer
19 Detection UID buffer
C1 Capacitor for resonance
C2 Adjustment capacitor
SW1 switching circuit

Patent Citations (8)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US5111186A *	1990-11-29	1992-05-05	Sensormatic Electronics Corporation	LC-type electronic article surveillance tag with voltage dependent capacitor
US5446447A *	1994-02-16	1995-08-29	Motorola, Inc.	RF tagging system including RF tags with variable frequency resonant circuits
US5602538A *	1994-07-27	1997-02-11	Texas Instruments Incorporated	Apparatus and method for identifying multiple transponders
GB9813371DD *	1998-06-22	1998-08-19	Powell George L	Anti-collision tag apparatus and system
JP2000151480A *	1998-11-11	2000-05-30	Mitsubishi Materials Corp	Identification system for superposed tags
US6354493B1 *	1999-12-23	2002-03-12	Sensormatic Electronics Corporation	System and method for finding a specific RFID tagged article located in a plurality of RFID tagged articles
US6377203B1 *	2000-02-01	2002-04-23	3M Innovative Properties Company	Collision arbitration method and apparatus for reading multiple radio frequency identification tags
AT393437T *	2000-08-15	2008-05-15	Omron Tateisi Electronics Co	CONTACTLESS COMMUNICATION MEDIUM AND SYSTEM

* Cited by examiner, † Cited by third party

Cited By (65)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US6841981B2 *	2002-04-09	2005-01-11	Mstar Semiconductor, Inc.	Radio frequency data communication device in CMOS process
JP3874007B2 *	2004-01-27	2007-01-31	オムロン株式会社	Read / write processing apparatus and read / write processing method for RFID tag
US7132946B2 *	2004-04-08	2006-11-07	3M Innovative Properties Company	Variable frequency radio frequency identification (RFID) tags
JP4191088B2 *	2004-05-14	2008-12-03	株式会社デンソー	Electronic equipment
WO2006011207A1 *	2004-07-29	2006-02-02	Mitsubishi Denki Kabushiki Kaisha	Radio tag read system, radio tag read device, and radio tag
KR100624688B1 *	2004-08-09	2006-09-19	삼성전자주식회사	Apparatus and method for wireless communication in image forming system
PT1794665E *	2004-09-29	2008-06-18	Swisscom Ag	Method and system for inputting user instructions of a user controllable telecommunications device
US7385499B2	2004-10-12	2008-04-15	Aristocrat Technologies, Inc.	Method and apparatus for synchronization of proximate RFID readers in a gaming environment
US7316352B1	2004-12-23	2008-01-08	Storage Technology Corporation	System and method for locked code on a radio frequency identification tag
CN100373392C *	2005-01-11	2008-03-05	盛群半导体股份有限公司	Power supply processing interface in passive radio frequency identification system

IPR2025-00645 Page 01601

JP4873868B2 *	2005-02-09	2012-02-08	ルネサスエレクトロニクス株式会社	Passive RFID semiconductor device, IC tag, IC tag control method, and communication method
DE102005005812A1	2005-02-09	2006-08-17	Atmel Germany Gmbh	Circuit arrangement and method for supplying power to a transponder
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
KR101111722B1 *	2005-04-25	2012-03-19	엘지전자 주식회사	Reader control system
DE102005020101A1 *	2005-04-29	2007-01-25	Giesecke & Devrient Gmbh	Portable data carrier and method for operating a portable data carrier
JP2008543156A *	2005-05-23	2008-11-27	エヌエックスピー ビー ヴィ	Electronic communication system, in particular authentication control system and corresponding method
US8295851B2	2005-08-03	2012-10-23	Michael Edward Finnegan	Realtime, interactive and geographically defined computerized personal matching systems and methods
US8880047B2 *	2005-08-03	2014-11-04	Jeffrey C. Konicek	Realtime, location-based cell phone enhancements, uses, and applications
CN101248440B *	2005-08-25	2010-06-23	Nxp股份有限公司	Method and RFID reader for evaluating a data stream signal in respect of data and/or collision
JP2007064765A *	2005-08-30	2007-03-15	Fujitsu Ltd	Rfid tag device, rfid reader writer device and distance measuring system
US20070115098A1 *	2005-11-18	2007-05-24	Wj Communications, Inc.	Rfid system including tags having low rf scattering mode
US7933577B2 *	2005-11-29	2011-04-26	Electronics And Telecommunications Research Institute	Method and apparatus for sharing portable terminal in CDMA system and mobile RFID system
US7417496B2	2005-12-06	2008-08-26	Electronics And Telecommunications Research Institute	Demodulator circuit of RFID system
CN101346728B *	2005-12-21	2012-04-11	皇家飞利浦电子股份有限公司	Collaborating RFID devices
KR100680501B1	2006-03-08	2007-02-08	엘지이노텍 주식회사	Radio frequency identification system of dual phase locked loop type
US7439860B2 *	2006-03-22	2008-10-21	Assa Abloy Ab	Auto-tuned RFID reader antenna
KR101338815B1 *	2006-06-09	2014-04-23	가부시키가이샤 한도오따이 에네루기 켄큐쇼	Semiconductor device
KR100728306B1	2006-06-19	2007-06-13	학교법인 포항공과대학교	A anti-collision method of tag in rfid
US20090280753A1 *	2006-06-21	2009-11-12	Nxp B.V.	Method of Checking the Integrity of an Antenna Arrangement, Transmitter, Receiver and Transceiver
CN101246538A *	2007-02-14	2008-08-20	日电（中国）有限公司	Radio frequency recognition system and method
AU2008215173B2 *	2007-02-16	2013-05-02	Orica Explosives Technology Pty Ltd	Method of communication at a blast site, and corresponding blasting apparatus
US8354917B2 *	2007-02-21	2013-01-15	Impinj, Inc.	RFID tag chips and tags complying with only a limited number of remaining commands and methods
WO2008105477A1	2007-02-27	2008-09-04	Kyocera Corporation	Portable electronic device and magnetic antenna circuit
EP1973069B1	2007-03-22	2013-01-02	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
DE102007027610A1	2007-06-12	2008-12-24	Atmel Germany Gmbh	Transponder, method for operating a transponder
US7796039B2 *	2007-06-28	2010-09-14	International Business Machines Corporation	Quick and accurate detection and reporting of component failures using RFID
JP4488040B2	2007-07-26	2010-06-23	Ｔｄｋ株式会社	Radio communication transmitter / receiver, RFID system, and radio communication transmitter / receiver reception method
CN101098348B *	2007-07-27	2010-06-09	北京华大恒泰科技有限责任公司	Method for reading data of reader-writer in radio frequency recognition system, and method for sending data of label
JP5019381B2 *	2007-10-09	2012-09-05	東芝テック株式会社	Wireless tag reader and method
JP4974171B2 *	2007-12-07	2012-07-11	ソニーモバイルコミュニケーションズ株式会社	Non-contact wireless communication device, method for adjusting resonance frequency of non-contact wireless communication antenna, and portable terminal device
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices

IPR2025-00645 Page 01602

US7793237B2 *	2007-12-17	2010-09-07	International Business Machines Corporation	System, structure and method of providing dynamic optimization of integrated circuits using a non-contact method of selection, and a design structure
JP5364270B2 *	2008-01-22	2013-12-11	株式会社東芝	Charger
US8391817B2	2008-06-27	2013-03-05	Nxp B.V.	Method of and system for tuning an antenna
CN101338892B *	2008-07-29	2011-12-14	宁波瑞奥光电技术有限公司	Safety processing method of RFID system for door lock
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
WO2010032573A1 *	2008-09-17	2010-03-25	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
CN102282574B *	2008-12-15	2015-06-03	卡德赫博私人有限公司	An RFID tag
US10402710B1	2009-02-03	2019-09-03	Impinj, Inc.	RFID tags with public and private inventory states
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
DE102009013962A1	2009-03-20	2010-10-14	Texas Instruments Deutschland Gmbh	Power level indicator
CN101630374B *	2009-08-26	2012-05-23	北京商约纳电子有限公司	SIM card with radio frequency identification function and power-saving method thereof
US20110084814A1 *	2009-10-08	2011-04-14	Checkpoint Systems, Inc.	Security tag utilizing rfid reflectivity mode power rationing
US10049317B1	2010-02-01	2018-08-14	Impinj, Inc.	RFID tags with public and private inventory states
US8917160B2 *	2011-03-21	2014-12-23	Sony Corporation	RFID module
FR2987904B1 *	2012-03-07	2014-03-21	Commissariat Energie Atomique	DEVICE FOR EVALUATING THE DISTANCE BETWEEN AN RFID LABEL AND AN INTERFACE
GB2508380A *	2012-11-29	2014-06-04	Ibm	Remote control of electrical appliances
CN103884873A *	2014-03-20	2014-06-25	上海华力微电子有限公司	Structure for preventing occurrence of resonance in reliability test
US9275529B1	2014-06-09	2016-03-01	Tyco Fire And Security Gmbh	Enhanced signal amplitude in acoustic-magnetomechanical EAS marker
CN106203543B *	2015-02-11	2019-03-29	天地融科技股份有限公司	A kind of switching device
US10134252B1	2017-05-22	2018-11-20	Tyco Fire & Security Gmbh	Dual-sided security marker
CN107895131B *	2017-11-06	2021-08-13	厦门印天电子科技有限公司	RFID label checking method in accordance with ISO15693 protocol
US10637444B1 *	2018-12-21	2020-04-28	Northrop Grumman Systems Corporation	Near field RFID probe with tunning

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP3614157B2	2005-01-26	RFID tag and method for adjusting resonance frequency in RFID tag
EP2667328B1	2019-07-31	Multi-mode RFID tag architecture
CN100501758C	2009-06-17	Communication method for reader and tag in RFID system
US7274284B2	2007-09-25	Method for RF card detection in a contactless system
JP4983017B2	2012-07-25	Information access system and method for accessing information in a contactless information storage device
JP4685926B2	2011-05-18	Improved transponder
EP2537121B1	2016-04-13	Multiple antenna reading system suitable for use with contactless transaction devices
WO2010014435A1	2010-02-04	Self tuning rfid

IPR2025-00645 Page 01603

JP2004248310A	2004-09-02	Data processing method for rfid tag and interrogator (reader/writer)
US20070257775A1	2007-11-08	Identification system and identification method
JP4466678B2	2010-05-26	RFID tag and method for adjusting resonance frequency in RFID tag
JP3607585B2	2005-01-05	Non-contact response device
EP1892645B1	2013-09-04	Smart card
TW201701195A	2017-01-01	Dual frequency HF-UHF identification device, in particular of the passive type
JP4426820B2	2010-03-03	Non-contact IC card
KR101633240B1	2016-06-23	Method of configuring two wireless devices for mutual communication
JP2002525932A	2002-08-13	Electrostatic radio frequency identification system with contactless programming function
JP2007094885A	2007-04-12	Radio tag reader/writer, and radio tag read/write method
JP2011048600A	2011-03-10	Reader/writer device
JP2004252602A	2004-09-09	Non-contact data carrier
KR100662050B1	2006-12-27	Anti-collision method for rfid readers
KR101500188B1	2015-03-09	Method and apparatus for sensing collision tag in rfid system
JP4135278B2	2008-08-20	ID tag
JP2007049527A	2007-02-22	Radio ic tag reader and moving-body reading system
JP2011107894A	2011-06-02	Rfid system and anti-collision processing method

Priority And Related Applications

Child Applications (1)

Application	Priority date	Filing date	Relation	Title
JP2004083655A	2004-03-22	2004-03-22	Division	Data processing method for rfid tag and interrogator (reader/writer)

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2002221841A	2002-07-30	2002-07-30	RFID tag and method for adjusting resonance frequency in RFID tag

Applications Claiming Priority (6)

Application	Filing date	Title
JP2002221841A	2002-07-30	RFID tag and method for adjusting resonance frequency in RFID tag
AT03254399T	2003-07-11	RFID TAG WITH TIMER SWITCHING
EP03254399A	2003-07-11	RFID-tag with tuning means
DE60308113T	2003-07-11	RFID tag with tuning circuit
US10/627,872	2003-07-28	RFID tag and method for processing RFID data
CNB031331467A	2003-07-29	RFID -tag, RFID-tag and interrogator (reader/writer) data processing method

Legal Events

Date	Code	Title	Description
2004-01-09	A975	Report on accelerated examination	**Free format text:** JAPANESE INTERMEDIATE CODE: A971005 **Effective date:** 20040108
2004-01-21	A131	Notification of reasons for refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A131

IPR2025-00645 Page 01604

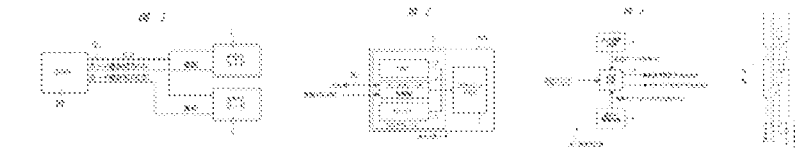
			Effective date: 20040120
2004-03-23	A521	Written amendment	Free format text: JAPANESE INTERMEDIATE CODE: A523 Effective date: 20040322
2004-05-07	A131	Notification of reasons for refusal	Free format text: JAPANESE INTERMEDIATE CODE: A131 Effective date: 20040506
2004-06-22	A521	Written amendment	Free format text: JAPANESE INTERMEDIATE CODE: A523 Effective date: 20040621
2004-10-05	TRDD	Decision of grant or rejection written	
2004-10-13	A01	Written decision to grant a patent or to grant a registration (utility model)	Free format text: JAPANESE INTERMEDIATE CODE: A01 Effective date: 20041012
2004-11-11	A61	First payment of annual fees (during grant procedure)	Free format text: JAPANESE INTERMEDIATE CODE: A61 Effective date: 20041025
2004-11-12	R150	Certificate of patent or registration of utility model	Free format text: JAPANESE INTERMEDIATE CODE: R150
2007-10-18	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20071112 Year of fee payment: 3
2007-10-23	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20081112 Year of fee payment: 4
2008-10-23	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20081112 Year of fee payment: 4
2008-10-28	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20091112 Year of fee payment: 5
2009-10-27	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20101112 Year of fee payment: 6
2010-10-21	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20101112 Year of fee payment: 6
2010-10-26	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20111112 Year of fee payment: 7
2011-10-18	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20121112 Year of fee payment: 8
2012-10-16	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20121112 Year of fee payment: 8
2012-10-23	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20131112 Year of fee payment: 9
2014-11-12	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

Patents JP3839288

Memory card

Images (9)



Classifications

G06K19/07 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e.g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips

View 1 more classification

JP3839288B2
Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: 国弘 片山 晶樹 金森 深史 四方 英史 大園 敦 白石

Worldwide applications

2001 JP 2002 US 2006 US

Application JP2001276002A events

2001-09-12 Application filed by 株式会社ルネサステクノロジ
2001-09-12 Priority to JP2001276002A
2003-03-20 Publication of JP2003085505A
2006-11-01 Application granted
2006-11-01 Publication of JP3839288B2
2021-09-12 Anticipated expiration
Status Expired - Fee Related

Info: Patent citations (4), Cited by (16), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (7) Hide Dependent

1. A memory card having a plurality of nonvolatile memory cells and capable of storing predetermined information and a controller for instructing operation of the nonvolatile semiconductor memory based on a command issued from a host And
The controller is
A processing determination means for outputting a transfer interruption signal when a card selection signal for selecting the memory card transits from assert to negate while data is being transferred from the host;
A memory card characterized in that when the process determining means outputs a transfer interruption signal, all data being transferred is invalidated and the transfer process is interrupted.

2. The memory card according to claim 1,
The processing determination means includes
A transfer control unit for detecting that data is being transferred from the host and outputting a transfer flag signal;
A transfer flag signal output from the transfer control unit and a card selection signal for selecting the memory card are input, and the card selection signal transits from assert to negate while the transfer flag signal is input. And a process determination unit for outputting the transfer interruption signal.

3. A memory card having a plurality of nonvolatile memory cells and capable of storing predetermined information and a controller for instructing operation of the nonvolatile semiconductor memory based on a command issued from a host. And
The controller is
Processing execution means for outputting a suspend signal when a card selection signal for selecting the memory card transits from assert to negate when executing a command transferred from the host;
The memory card according to claim 1, wherein when the processing determination unit outputs a suspend signal, the command is executed and the apparatus waits in a state before data transfer regardless of the state of the card selection signal.

4. The memory card according to claim 3,
The processing determination means is
A command control unit that outputs an operation signal when the command is executed;
When an operation signal output from the command control unit and a card selection signal for selecting the memory card are input, and the card selection signal transits from assert to negate while the operation signal is input, A memory card comprising a process determination unit for outputting a suspend signal.

5. The memory card according to claim 4,
A memory card characterized in that a command when the command control unit outputs an operation signal is at least one of a read command, a write command, and an erase command.

IPR2025-00645 Page 01606

6. A memory card having a plurality of nonvolatile memory cells and capable of storing predetermined information and a controller for instructing operation of the nonvolatile semiconductor memory based on a command issued from a host. And
The controller is
A transfer control unit for detecting that data is being transferred from the host and outputting a transfer flag signal;
A command control unit that outputs an operation signal when executing a command transferred from the host;
A transfer flag signal output from the transfer control unit and a card selection signal for selecting the memory card are input, and the card selection signal transits from assert to negate while the transfer flag signal is input. When the operation signal output from the command controller and the card selection signal are input and the operation signal is input, the card selection signal transits from assert to negate. And a process determination unit that outputs a suspend signal when
When the process determining unit outputs an interruption signal, all the data being transferred is invalidated and the transfer process is interrupted. When the process determining unit outputs the suspend signal, the state of the card selection signal is set. Regardless, after executing the command, the memory card stands by in a state before data transfer.

7. 7. The memory card according to claim 6, wherein the command when the command control unit outputs an operation signal is at least one of a read command, a write command, and an erase command.

Description

[0001]
BACKGROUND OF THE INVENTION
The present invention relates to a memory card, and more particularly to a technique that is effective when applied to a change in the standard of a multimedia card and an additional flexible response.
[0002]
[Prior art]
Multimedia cards are widely known as one of external storage media such as personal computers and multi-function terminals. The multimedia card is used for all kinds of digital information such as still image recording of a digital video camera, data recording of a mobile phone, music recording of a portable music player, and the like.
[0003]
The compatibility of the multimedia card is maintained by a multimedia card standard standardized by a standard organization MMCA (MultiMedia Card Association).
[0004]
The multimedia card is a product with a short history that was born with the expansion of the Internet and the spread of mobile phones, etc., and the multimedia card standard stipulates responses to operations such as unexpected host side violations. There may not be.
[0005]
According to the inventor's study, in the operation mode in which the multimedia card selected by the card selection signal (CS) issued by the host accepts the command and executes the processing, the access by the host command is being executed. In some cases, the card selection signal is negated.
[0006]
As processing in the multimedia card in such a case, it is conceivable to mask data input and data output and continue the processing inside the multimedia card as long as a clock signal is input.
[0007]
Examples of this type of IC card that have been described in detail include December 1, 1990, published by Industrial Research Co., Ltd., Masashi Oshima (ed.), "Electronic Materials" P22 to P26. Technical trends in various IC cards are described.
[0008]
[Problems to be solved by the invention]
However, the present inventors have found that the memory card operation process when the card selection signal as described above is negated has the following problems.
[0009]
That is, if the card selection signal is negated and then asserted again, the multimedia card continues processing even if the card selection signal is negated.
[0010]
On the other hand, since it is difficult for the host to grasp the card operation at the time of non-selection, when the card selection signal is asserted again, the processing of the host and the multimedia card cannot be synchronized, and the You may lose control of your media card.
[0011]
An object of the present invention is to provide a memory card capable of selecting and executing an optimum processing operation from an internal processing state even when a signal is transferred from a host at a timing not permitted by the standard.
[0012]
The above and other objects and novel features of the present invention will be apparent from the description of this specification and the accompanying drawings.
[0013]
[Means for Solving the Problems]
Of the inventions disclosed in this application, the outline of typical ones will be briefly described as follows.
1. In other words, the memory card of the present invention provides an interrupt signal when the card selection signal transits from assert to negate while data is being transferred from the host to the controller that instructs the operation of the nonvolatile semiconductor memory based on the command issued from the host. When the process determining unit outputs an interruption signal, all the data being transferred is invalidated and the transfer process is interrupted.
2. In the first item, the processing determination unit detects that data is being transferred and outputs a transfer flag signal, and a transfer flag signal output from the transfer control unit. When the card selection signal is input and the card selection signal transits from assertion to negation while the transfer flag signal is being input, the processing determination unit outputs a suspension signal.
[0014]
Moreover, the outline | summary of the other invention of this application is divided into items, and is shown simply.
1. Processing determination means for outputting a suspend signal when a card selection signal transits from assert to negate during execution of a transferred command to a controller that instructs operation of a nonvolatile semiconductor memory based on a command issued from a host When the processing determination means outputs a suspend signal, the command is executed regardless of the state of the card selection signal and then waits in a state before data transfer.
2. In the memory card of the first item, the processing determination unit receives a command control unit that outputs an operation signal when a command is executed. an operation signal output from the command control unit, and a card selection signal. When the card selection signal transits from assert to negate during the input of, the process determination unit outputs a suspend signal.
3. In the memory card of the second item, a command when the command control unit outputs an operation signal is composed of at least one of a read command, a

IPR2025-00645 Page 01607

write command, and an erase command.

4) A controller that instructs the operation of the nonvolatile semiconductor memory based on a command issued from the host, detects that data is being transferred from the host, and outputs a transfer flag signal, and is transferred from the host. A command control unit that outputs an operation signal when the command is executed, a transfer flag signal and a card selection signal output from the transfer control unit, and the card selection signal is asserted while the transfer flag signal is being input. When transitioning to negate, an interrupt signal is output, and the operation signal and card selection signal output from the command control unit are input, and when the card selection signal transitions from assert to negate while the operation signal is being input. And a processing determination unit that outputs a suspend signal. When the processing determination unit outputs an interruption signal, all the data being transferred interrupts the transfer process as effective, when the determination unit has output the suspend signal after executing the command regardless of the state of the card selection signal, and wait in the pre-data transfer state.

5). In the memory card of the fourth item, the command when the command control unit outputs an operation signal is composed of at least one of a read command, a write command, and an erase command.

[0015]

DETAILED DESCRIPTION OF THE INVENTION

Hereinafter, embodiments of the present invention will be described in detail with reference to the drawings.

[0016]

1 is a block diagram of a memory card connected to a host according to an embodiment of the present invention, FIG. 2 is a block diagram of the memory card of FIG. 1, and FIG. 3 is a process provided in the memory card of FIG. 4 to 7 are timing charts and diagrams showing examples of signal timings in the memory card when the host outputs a non-standard card selection signal according to an embodiment of the present invention. 8 is a state transition diagram of the memory card at the timings of FIGS. 4 to 7, and FIG. 9 is a timing chart showing an example of the operation timing in the memory card of FIG

[0017]

in the present embodiment, as shown in FIG. 1, memory cards 1 and 2 are connected as external storage media to a host HT in a digital video camera, a mobile phone, a portable music player, a personal computer, or the like. The memory cards 1 and 2 are multimedia cards.

[0018]

These memory cards 1 and 2 are connected to the host HT via a common bus BL. Various signals such as commands, data, and clocks are transferred via the bus BL.

[0019]

Further, the memory cards 1 and 2 are connected so that card selection signals CS1 and CS2 output when the host HT accesses them are respectively input. For example, when the host HT accesses the memory card 1, the card selection signal CS1 is input to the memory card 1, and when the host HT accesses the memory card 2, the card selection signal CS2 is input to the memory card 2. Is done.

[0020]

Furthermore, the memory card 1 (, 2) includes a controller 3 and a flash memory 4 as shown in FIG. The controller 3 controls the flash memory 4 based on commands received from the host HT, reads out programs and data stored in the flash memory 4, performs predetermined processing, and instructs data write operation. Do. The flash memory 4 is a nonvolatile semiconductor memory that can electrically rewrite and erase data.

[0021]

The controller 3 includes a CPU 5, an interface control unit 6, a buffer 7, and the like. The CPU 5 performs predetermined processing based on a control program stored in a nonvolatile memory such as a ROM (Read Only Memory) provided in the CPU 5 or an EEPROM (Electrically Erasable and Programmable ROM). To control.

[0022]

The interface control unit 6 receives commands or the like for instructing operations such as writing / reading / erasing input / output from the host HT, and inputs / outputs data necessary for these operations.

[0023]

The buffer 7 temporarily stores data input / output from the host HT and the flash memory 4.

[0024]

Further, as shown in FIG. 3, the interface control unit 6 is provided with a processing determination unit (processing determination means) 6a. The process determination unit 6 a includes a transfer control circuit (transfer control unit) 8, a write control circuit (command control unit) 9, and a determination circuit (process determination unit) 10.

[0025]

The transfer control circuit 8 controls the data transfer in the memory card 1 (, 2), and outputs the in-transfer flag signal TS to the determination circuit 10 during the data transfer. The write control circuit 9 generates an internal busy signal (operation signal) BUSY 1 (, BUSY 2) while the memory card 1 (, 2) is writing data, and outputs it to the determination circuit 10.

[0026]

The determination circuit 10 transfers the transfer interruption signal SS1 (, SS2) based on the respective states of the card selection signal CS1 (, CS2), the transfer flag signal TS, and the internal busy signal BUSY1 (, BUSY2) input from the host HT.), The suspend signal SUS1 (, SUS2) is output to the CPU 5.

[0027]

Next, in the memory card 1 of the present embodiment, the operation of the interface control unit 6 associated with the transition of the card selection signal CS1 not defined in the memory card standard will be described with reference to the timing charts of FIGS. This will be described with reference to FIG.

[0028]

Here, the timing charts of FIGS. 4 to 7 show the card selection signal CS1 transferred from the host HT, the command CMD transferred from the host HT, the data D transferred from the host HT, the memory card 1 from the upper side to the lower side. The timing of signals in the busy signal BY output from the memory card 1 to the host HT, the transfer interruption signal SS1 output from the memory card 1, and the suspend signal SUS1 output from the memory card 1 are shown. Although the memory card 1 is described here, the memory card 2 performs the same operation.

[0029]

FIG. 4 shows a case where the card selection signal CS1 of the host HT is negated during the data D write operation in multi-transfer. Also, the dotted line in the busy signal BY in FIG. 4 indicates the actual write operation of the memory card 1

[0030]

First, when the card selection signal CS1 is transferred from the host HT to the memory card 1 (state 1), a data write command CMD is subsequently transferred, and the memory card 1 waits for data transfer (state 2). Thereafter, the first write data D (first block) is transferred from the host HT (state 3).

[0031]

When receiving the data D from the host HT, the memory card 1 outputs a busy signal BY (Hi) indicating that data is being written to the host HT, and writes the data D (state 4).

[0032]

If the card selection signal CS1 transferred from the host HT is negated for some reason during the writing of the data D (state 5), the memory card 1 sends an intermediate level busy signal BY (high impedance state). is output to the host HT.

[0033]

At this time, the determination circuit 10 outputs the suspend signal SUS1 to the CPU 5 when the card selection signal CS1 is negated and the memory card 1 is writing

IPR2025-00645 Page 01608

data D (busy). The CPU 5 that has detected the suspend signal SUS1 performs the writing operation until the writing of the data D is completed even if the card selection signal CS1 is negated (state 6).

[0034]

Here, since the card selection signal CS1 of the host HT is asserted during the data D write operation, the determination circuit 10 receives the asserted card selection signal CS1 and stops outputting the suspend signal SUS1. Card 1 is in normal operation.

[0035]

When the writing of the first data D is completed and the busy signal BY is canceled and becomes a ready signal, the second (second block) data is transferred from the host HT.

[0036]

FIG. 5 shows a case where the card selection signal CS1 is negated during the transfer of data D from the host HT in multi-transfer.

[0037]

In this case, a card selection signal CS1 is transferred from the host HT to the memory card 1, a data write command CMD is transferred (state 1), and then the first data D is input (states 2 and 3). .

[0038]

When the transfer of data D from the host HT is completed, the memory card 1 outputs a busy signal BY (Hi) indicating that data is being written to the host HT, and writes the data D (state 4).

[0039]

When the writing of the data D is completed, the busy signal BY is canceled to become a ready signal, and when waiting for the data D transfer again (state 2), the second data is transferred from the host HT (state 3). If the card selection signal CS1 of the host HT is negated for some reason during the transfer of the data D (state 7), the determination circuit 10 outputs a transfer interruption signal SS1 to the CPU 5.

[0040]

Accordingly, the determination circuit 10 outputs the transfer interruption signal SS1 when both the card selection signal CS1 and the transfer flag signal TS of the transfer control circuit 8 are negated.

[0041]

The CPU 5 detecting this transfer interruption signal SS1 invalidates all data D being transferred and interrupts the internal processing. Thus, it is possible to prevent the data D from being received again when the card selection signal CS1 is asserted again.

[0042]

Further, FIG. 6 shows a case where the data D writing operation is completed while the card selection signal CS1 is negated. In FIG. 6, as in FIG. 4, the dotted line in the busy signal BY indicates the actual write operation of the memory card 1.

[0043]

The selection signal CS1 is transferred from the host HT to the memory card 1, and the data write command CMD is transferred (state 1) Thereafter, the first data D is input (states 2 and 3). When the memory card 1 receives the data D, the memory card 1 outputs a busy signal BY indicating that data is being written to the host HT, and writes the data D (state 4).

[0044]

If the card selection signal CS1 of the host HT is negated during the writing of the data D (state 5), an intermediate level busy signal BY is output from the memory card 1 to the host HT.

[0045]

At the same time, the determination circuit 10 outputs a suspend signal SUS1 to the CPU 5. The CPU 5 that has detected the suspend signal SUS1 performs the writing operation until the writing of the data D is completed even if the selection signal CS1 is negated (state 6).

[0046]

Here again, the determination circuit 10 outputs the suspend signal SUS1 when the card selection signal CS1 is negated and the memory card 1 is writing data D (busy).

[0047]

When the data D writing operation is completed, the determination circuit 10 stops outputting the suspend signal SUS1 even if the card selection signal CS1 is negated. After completion of the data writing operation, the memory card 1 is in a suspended state until the card selection signal CS1 is asserted.

[0048]

When the selection signal CS1 of the host HT is asserted again, the memory card 1 returns to the normal operation, and the data write command CMD and data D are input respectively.

[0049]

Further, FIG. 7 shows a case where the first data D write operation is completed and the card selection signal CS1 is negated when the second data D is transferred from the host HT

[0050]

The asserted card selection signal CS1 and the data write command are transferred from the host HT to the memory card 1, and then the first (first block) write data D is input.

[0051]

When the data D is received from the host HT, the memory card 1 outputs a busy signal BY indicating that data is being written to the host HT, and writes the data D.

[0052]

When the writing of the data D is completed, the busy signal BY is canceled and becomes a ready signal. Thereafter, when the card selection signal CS1 is negated, the memory card 1 outputs an intermediate level busy signal BY to the host HT.

[0053]

Here, since the memory card 1 has finished the data write operation, the determination circuit 10 does not output either the suspend signal SUS1 or the transfer interruption signal SS1 even if the card selection signal CS1 is negated.

[0054]

Thereafter, when the selection signal CS1 of the host HT is asserted again, the memory card 1 returns to the normal operation, and the data write command CMD and the data D are input.

[0055]

Next, an example of an effective operation using the memory cards 1 and 2 performing the operation shown in FIGS. 4 to 7 will be described with reference to FIG.

[0056]

In FIG. 9, from top to bottom, a card selection signal CS1 for selecting the memory card 1, a card selection signal CS2 for selecting the memory card 2, a command CMD transferred from the host HT, and data D transferred from the host HT. The internal busy signal BUSY1 output from the write control circuit 9 of the memory card 1, the internal busy signal BUSY2 output from the write control circuit 9 of the memory card 2, and the transfer interruption signal SS1 output from the determination circuit 10 of the memory card 1 , A suspend signal SUS1 output from the determination circuit 10 of the memory card 1, a transfer interruption signal SS2 output from the determination circuit 10 of the memory card 2, and a suspend signal SUS2 output from the determination circuit 10 of the memory card 2, respectively. ing.

[0057]

IPR2025-00645 Page 01609

First, the host HT outputs a card selection signal CS1 to select the memory card 1. Then, a data write command CMD1 is transferred to the memory card 1.

[0058]

Thereafter, the host HT transfers the first block of data D1-1 to be written to the memory card 1. When the transfer of the data D1-1 is completed, the memory card 1 starts a write operation of the data D1-1. While the data D1-1 is being written, the internal busy signal BUSY1 (Hi) is output from the write control circuit 9.

[0059]

At this time, the determination circuit 10 of the memory card 1 is supplied with the asserted card selection signal CS1 and the busy signal BUSY1 indicating that data is being written and is output from the write control circuit 9

[0060]

Thereafter, the host HT negates the card selection signal CS1, asserts the card selection signal CS2 for selecting the memory card 2, and transfers the command CMD2 for writing the data D2-1 to the memory card 2.

[0061]

The determination circuit 10 of the memory card 1 outputs a suspend signal SUS1 to the CPU 5 when the card selection signal CS1 transits from assertion to negation. In response to the suspend signal SUS1, the CPU 5 performs the writing operation until the writing of the data D is completed even if the selection signal CS1 is negated.

[0062]

When the writing operation of the data D1-1 is completed, the internal busy signal BUSY1 becomes a Lo level signal. Upon receiving this signal, the determination circuit 10 stops outputting the suspend signal SUS1.

[0063]

On the other hand, a data write command CMD2 is transferred from the host HT to the memory card 2 to which the asserted card selection signal CS2 is input, and then the first block data D2-1 to be written to the memory card 2 is transferred.

[0064]

When the transfer of the data D2-1 is completed, the memory card 2 starts a write operation of the data D2-1. Then, the host HT asserts the card selection signal CS1 again, negates the card selection signal CS1, and transfers the data D1-2 to the memory card 1.

[0065]

The determination circuit 10 of the memory card 2 outputs the suspend signal SUS2 to the CPU 5 when the card selection signal CS2 transits from assertion to negation. The CPU 5 receives the suspend signal SUS2 and performs the write operation until the data D is completely written even if the selection signal CS2 is negated.

[0066]

By repeating these operations, the memory card 1 is instructed to perform a write operation to transfer the data D1-1, and the memory card 1 is deselected while the data is being written inside the memory card 1. At the same time, the memory card 2 is selected, the write operation is similarly instructed, the data D2-1 is transferred, and the memory card 2 accesses the memory card 1 again during the data writing, so-called interleave processing is enabled. be able to.

[0067]

Thus, according to the present embodiment, even if the card selection signals CS1 and CS2 for selecting the memory cards 1 and 2 are negated during data transfer or data writing, the host HT and the memory cards 1 and 2 Thus, it is possible to reliably avoid problems such as processing discrepancies and timing mismatch.

[0068]

Further, by using the memory cards 1 and 2 as the host HT capable of processing a plurality of memory cards, interleaving processing and the like can be performed, and data processing can be performed efficiently and in a short time.

[0069]

Furthermore, although the data read operation is described in this embodiment, the present invention can be applied to other than data read operations such as a data read operation or an erase operation.

[0070]

As mentioned above, the invention made by the present inventor has been specifically described based on the embodiments of the invention. However, the present invention is not limited to the above-described embodiments, and various modifications can be made without departing from the scope of the invention. Needless to say, there is.

[0071]

For example, in the above embodiment, commands are input to each memory card at different timings. However, by simultaneously inputting commands to these memory cards, data processing can be further accelerated. Further, when a device signal is negated during data transfer, access may be returned to the beginning of the sector being transferred.

[0072]

【The invention's effect】

Of the inventions disclosed in the present application, effects obtained by typical ones will be briefly described as follows.

[0073]

(1) Even if the card selection signal is negated during command processing such as during data transfer or data write operation, the memory card executes the optimum process and the host violates the standard. In such a case, it is possible to reliably avoid problems such as inability to synchronize processing with the memory card.

[0074]

(2) Further, since a plurality of memory cards can be used effectively by the card selection signal, the data processing performance can be improved.

[Brief description of the drawings]

FIG. 1 is a block diagram of a memory card connected to a host according to an embodiment of the present invention.

FIG. 2 is a block diagram of the memory card of FIG.

FIG. 3 is a block diagram of a process determination unit provided in the memory card of FIG.

FIG. 4 is a timing chart showing an example of signal timing in a memory card when a host according to an embodiment of the present invention outputs a non-standard card selection signal.

FIG. 5 is a timing chart showing another example of signal timing in the memory card when the host according to the embodiment of the present invention outputs a non-standard card selection signal.

FIG. 6 is a timing chart showing an example of signal timing in a memory card when a host according to an embodiment of the present invention outputs a non-standard card selection signal.

FIG. 7 is a timing chart showing another example of signal timing in the memory card when the host according to the embodiment of the present invention outputs a non-standard card selection signal.

FIG. 8 is a state transition diagram of the memory card at the signal timings of FIGS.

9 is a timing chart showing an example of operation timing in the memory card of FIG. 1. FIG.

[Explanation of symbols]

1, 2 Memory card 3 Controller 4 Flash memory 5 CPU

6 Interface control unit 6a Process determination unit (process determination means)

7 Buffer 8 Transfer control circuit (transfer control unit)

9 Write control circuit (command control unit)

IPR2025-00645 Page 01610

1G Judgment circuit (Processing judgment unit)
HT Host BL Bus CS1, CS2 Card selection signal TS Transfer flag signal BUSY1, BUSY2 Internal busy signal (operation signal)
SUS1, SUS2 Suspend signal SS1, SS2 Transfer interruption signal BY Busy signal CMD Command D Data

Patent Citations (4)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US5740404A *	1993-09-27	1998-04-14	Hitachi America Limited	Digital signal processor with on-chip select decoder and wait state generator
US6278654B1 *	2000-06-30	2001-08-21	Micron Technology, Inc.	Active terminate command in synchronous flash memory
US20030028806A1 *	2001-08-06	2003-02-06	Rangaprasad Govindarajan	Dynamic allocation of ports at firewall
US20030172229A1 *	2002-03-08	2003-09-11	Takasugi Robin Alexis	Systems and methods for detecting and compensating for runt block data transfers

* Cited by examiner, † Cited by third party

Cited By (16)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US6499090B1 *	1999-12-28	2002-12-24	Intel Corporation	Prioritized bus request scheduling mechanism for processing devices
US7565469B2 *	2004-11-17	2009-07-21	Nokia Corporation	Multimedia card interface method, computer program product and apparatus
US7588178B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7930589B2 *	2005-06-17	2011-04-19	Analog Devices, Inc.	Interrupt-responsive non-volatile memory system and method
US7487287B2 *	2006-02-08	2009-02-03	Atmel Corporation	Time efficient embedded EEPROM/processor control method
DE102006028943B4 *	2006-06-23	2008-07-24	Infineon Technologies Ag	Method for operating a volatile random access memory as detector and circuit arrangement
KR100784869B1 *	2006-06-26	2007-12-14	삼성전자주식회사	Memory sysytem capable of reducing standby curret
KR100843136B1 *	2006-11-14	2008-07-02	삼성전자주식회사	Apparatus and method for controlling operation processing in non volatile memory
KR100866625B1 *	2007-02-26	2008-11-03	삼성전자주식회사	Method and system for interfacing a plurality of memory devices using MMC or SD protocol
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US20140013031A1 *	2012-07-09	2014-01-09	Yoko Masuo	Data storage apparatus, memory control method, and electronic apparatus having a data storage apparatus
KR20190033920A	2017-09-22	2019-04-01	삼성전자주식회사	Storage device and method of operating the same

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP3839288B2	2006-11-01	Memory card
EP2973572B1	2018-05-30	System and method of reading data from memory concurrently with sending write data to the memory
JP4593575B2	2010-12-08	A common interface for each component of an embedded computer system
JP5090819B2	2012-12-05	Memory card and data storage method

IPR2025-00645 Page 01611

KR100725271B1	2007-06-04	USB-SD Memory with multiple DMA channels, and data storing method thereof
US20080256352A1	2008-10-16	Methods and systems of booting of an intelligent non-volatile memory microcontroller from various sources
JP2004355476A	2004-12-16	Computer controller, computer device, card medium controlling method, and program
US8266371B2	2012-09-11	Non-volatile storage device, host device, non-volatile storage system, data recording method, and program
JP5832901B2	2015-12-16	Improved addressability for serial non-volatile memory
MX2012005183A	2012-06-08	Command queue for peripheral component.
JP4294894B2	2009-07-15	Memory card
JP2006236105A	2006-09-07	Access control unit and control method therefor
EP2214103A1	2010-08-04	I/O controller and descriptor transfer method
JP2004192051A	2004-07-08	Shared terminal controller
JP5188134B2	2013-04-24	Memory access control device and memory access control method
TWI230859B	2005-04-11	Method and related system for accessing LPC memory or firmware memory in a computer system
US10566062B2	2020-02-18	Memory device and method for operating the same
US7844754B2	2010-11-30	Data transfer apparatus and data transfer method
TWI667567B	2019-08-01	Memory device and method for operating the same
JP2002366509A	2002-12-20	Direct memory access controller and its access control method
US20180336147A1	2018-11-22	Application processor including command controller and integrated circuit including the same
US20110125481A1	2011-05-26	Apparatus and method for simulating function of multimedia device
JPH11317068A	1999-11-16	Memory card
KR20020058419A	2002-07-12	Smart media controller optimized on writing stream data
JP2002312307A	2002-10-25	Memory access control circuit

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2001276002A	2001-09-12	2001-09-12	Memory card

Applications Claiming Priority (3)

Application	Filing date	Title
JP2001276002A	2001-09-12	Memory card
US10/195,400	2002-07-16	Non-volatile memory card and transfer interruption means
US11/541,543	2006-10-03	Non-volatile memory card and transfer interruption means

Legal Events

Date	Code	Title	Description
2004-10-07	A621	Written request for application examination	**Free format text**: JAPANESE INTERMEDIATE CODE: A621 **Effective date**: 20041006
2005-03-16	A711	Notification of change in applicant	**Free format text**: JAPANESE INTERMEDIATE CODE: A711 **Effective date**: 20050315
2006-06-22	A977	Report on retrieval	**Free format text**: JAPANESE INTERMEDIATE CODE: A971007 **Effective date**: 20060622

IPR2025-00645 Page 01612

2006-06-27	TRDD	Decision of grant or rejection written	
2006-07-05	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text**: JAPANESE INTERMEDIATE CODE: A01 **Effective date**: 20060704
2006-08-10	A61	First payment of annual fees (during grant procedure)	**Free format text**: JAPANESE INTERMEDIATE CODE: A61 **Effective date**: 20060802
2006-08-11	R150	Certificate of patent or registration of utility model	**Free format text**: JAPANESE INTERMEDIATE CODE: R150
2009-07-30	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20090811 **Year of fee payment**: 3
2009-09-01	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20100811 **Year of fee payment**: 4
2010-04-06	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20110811 **Year of fee payment**: 5
2010-10-04	S111	Request for change of ownership or part of ownership	**Free format text**: JAPANESE INTERMEDIATE CODE: R313111
2010-10-04	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20110811 **Year of fee payment**: 5
2010-10-13	R350	Written notification of registration of transfer	**Free format text**: JAPANESE INTERMEDIATE CODE: R350
2010-10-13	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20110811 **Year of fee payment**: 5
2011-07-12	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20120811 **Year of fee payment**: 6
2012-06-14	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20120811 **Year of fee payment**: 6
2012-06-19	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20130811 **Year of fee payment**: 7
2015-09-11	S531	Written request for registration of change of domicile	**Free format text**: JAPANESE INTERMEDIATE CODE: R313531
2015-09-24	R350	Written notification of registration of transfer	**Free format text**: JAPANESE INTERMEDIATE CODE: R350
2016-08-11	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

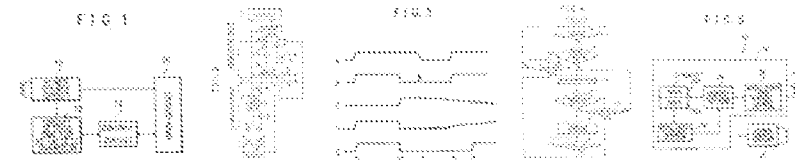
Patents EP0541818

Non-contact type ic card

Abstract

A non-contact type IC card, in which is incorporated a reaccess inhibition time setting circuit (12) which sets, after the operation of a main circuit (16), a reaccess inhibition time during which any reaccess is inhibited for a fixed time, and thereby, a double hysteresis can be prevented from being written in the IC card due to the reaccess in a short time. Also, in the IC card, two areas (321, 322) are provided in a memory (32), and data are recorded in these areas alternately. When the data is read, in case data in one area is destroyed, the other normal data is read out. When both the data are normal, the data recorded later is read out. Thereby, read impossibility due to defect data can be prevented.

Images (10)



Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 3 more classifications

EP0541818B1

European Patent Office

Download PDF Find Prior Art Similar

Other languages: German, French

Inventor: Yoshinori Kyodo Printing Co. Ltd. Kobayashi

Current Assignee : Kyodo Printing Co Ltd

Worldwide applications

1992 EP DE EP DA WO US DE

Application EP19920910459 events

1991-05-22 Priority to JP3146760A

1992-05-21 Application filed by Kyodo Printing Co Ltd

1993-05-19 Publication of EP0541818A1

1994-08-24 Publication of EP0541818A4

1997-12-03 Application granted

1997-12-03 Publication of EP0541818B1

2012-05-21 Anticipated expiration

Status Expired - Lifetime

Show all events

Info: Patent citations (24), Cited by (27), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, EPO GPI, EP Register, Global Dossier, Discuss

Claims (7)

Hide Dependent

1. A non-contact type IC card achieving communications of signals with an external device in a noncontact manner, comprising:
main circuit means (16) for conducting various operations based on functions of the IC card;
characterized by further comprising:

operation inhibition signal generating means (12) for creating an operation inhibition signal to inhibit the operation of the main circuit means for a predetermined period of time; and

control means (14) for controlling the main circuit means and the operation inhibition signal generating means, wherein

the control means (14) operates the operation inhibition signal generating means (12) when the operation of the main circuit means (16) is finished and inhibits the operation of the main circuit means (16) for a predetermined period of time according to the operation inhibition signal from the operation inhibition signal generating means (12).

2. A non-contact type IC card in accordance with claim 1, further including power source circuit means (10) for receiving power supplied from an external device and supplying the power to each section of the card, wherein
the main circuit means (16) and the operation inhibition signal generating means (12) operate by receiving the power from the power source circuit means (10).

3. A non-contact type IC card in accordance with claim 2, wherein the operation inhibition signal generating means (12) includes accumulating means (C3) for accumulating the power supplied from the power source circuit means (10) and discharging the power according to a predetermined time constant, voltage inverting means (24) for inverting an output from the power accumulating means (C3) to obtain a gradually increasing voltage, and Schmitt trigger circuit means (22) for outputting the operation inhibition signal when the voltage obtained from the voltage inverting means (24) exceeds a predetermined value.

4. A non-contact type IC card in accordance with claim 3, wherein the operation inhibition signal generating means further includes a switching transistor (Q) which is operated by a control signal from the control means to control accumulation of the power supplied from the power source circuit means in the power accumulating means.

IPR2025-00645 Page 01614

5. A non-contact type IC card, according to claim 1, further comprising:

communicating means (40) for communicating signals with an external device in a noncontact manner;

a memory (32) for storing therein data sent from the external device;

second control means (36) for controlling operations of the communicating means (40) and the memory (32),

said operation inhibition signal generating means (12) being capable of generating an operation inhibition signal for inhibiting the operations of the communicating means, the memory, and said first control means (12); wherein

the memory (32) has an area subdivided into a plurality of areas (321,322) for storing therein data sent from the external device;

said second control means (36) reads, when the data is to be read from the memory (32), the data from one of the plural areas in which the data is normally stored; and

said first control means (14) operates the operation inhibition signal generating means (12) when the operations of the communicating means (40), the memory (32), and said second control means (36) are finished and inhibits for a predetermined period of time the operations of the communicating means (40), the memory (32), and the second control means (36) according to the operation inhibition signal from the operation inhibition signal generating means (12).

6. A non-contact type IC card in accordance with claim 5, characterized in that number data indicating a recording sequence number of the data is recorded in each of the plural areas (321,322) of the memory (32).

7. A non-contact type IC card in accordance with claim 5, or 6, characterized by further including a power source circuit (10) for receiving power from an external device and supplying the power to each section of the card.

Description

Technical Field

[0001] The present invention relates to a non-contact type integrated circuit (IC) card not having contact terminals for a power source and for inputting and outputting signals.

Background Art

[0002] There has been known an IC card which has no contact terminals for receiving signals from an external device or for outputting signals thereto via a magnetic or capacitive coupling therewith. When using the non-contact type IC card, as compared with the card achieving communications of signals via contact terminals, the read operation is facilitated since, for example, when a person having the card in his or her hand approaches the external device, data stored in the card can be read therefrom into the external device. Moreover, there can be prevented such problems associated with the card achieving input and output operations of data via contact terminals as a contact failure due to dirt, erosion, etc. of terminal contact points and wrong operations due to a leakage current.

[0003] For the read operation of the non-contact type IC card, the card bearer having the card with him or her need only approach the reader and there is unnecessitated a read operation to insert the card into the reader. Consequently, the card is suitable for a check of sequential passage of many persons, for example, the card is suitably used as a commuter pass or a key for checking entrance an exit for a particular room.

[0004] In a case where the non-contact type IC card is adopted as a commuter pass or a key for checking entrance and exit for a room, ID data is read from a memory of the IC card for a collation thereof such that when the collation results in a coincidence, the passage of the gate or the entrance for the room is admitted. At the same time, historical data of uses of the IC card is written in the memory thereof.

[0005] When a non-contact type IC card is brought into an area accessible to the reader-writer, the collation and the write operation of the history are accomplished. Since the accessible area has a range of a certain magnitude, when the card is employed as, for example, a commuter pass, there may occur depending on actions of the card holder a case where an identical card enters two or more times the area accessible to the reader-writer installed at the gate. Namely, it may possible occur, the user puts the card into the area, removes the card from the area, and then puts again the card into the area. In such a case, it is necessary to avoid the write operation of history in the second access.

[0006] Conventionally, in the case above, the second access of an identical card is detected by the reader-writer to inhibit the write operation of new data on the card. However, since passage of many cards is required to be checked in a short period of time at the gate, it is necessary for the reader-writer, after an access of a card, to wait for passage of a subsequent card. Consequently, there does not exist any marginal time enough to check the second access.

[0007] In consequence, it is the object of the invention that the operation of a card is inhibited for a fixed period of time after a passage thereof.

[0008] However, in a card not having a power source therein, namely, a card of an external power supply type, an electromagnetic energy supplied from an external device is rectified to obtain a direct-current (dc) voltage necessary for an internal circuit thereof. Consequently, after the external energy supply is interrupted, it is difficult to control the operation inhibition for a fixed period of time. For example, after the external energy supply is stopped, the circuit in the card may be operated by energy resultant from discharge of electric charges accumulated in a smoothing capacitor of the power source circuit. However, since the operation of the circuit is determined by a value of a current consumed by the circuit and the energy accumulated in the smoothing capacitor, it is difficult to set the period for inhibiting the operation.

[0009] Moreover, in such a non-contact type IC card, since the contact (approaching) state between the card and the reader-writer cannot be fixedly established, communications of data and power source become to be unstable in some cases. For example, in a card of the external power supply type which receives supply of power via energy such as an electromagnetic field from an external power source, the card is supplied with power only when the card is in the proximity of the reader-writer. When the card is apart from the reader-writer, the power is not supplied thereto. In consequence, in a case where the bearer of the card puts the card close to the reader-writer to write data received from the reader-writer in the memory of the card, when the contact state is changed because the distance between the card and the reader-writer is increased due to movement or the like of the bearer, the power supply from the reader-writer to the card is interrupted. Consequently, the write operation of data in the memory of the card is stopped at an intermediate point and hence data is stored in the memory in an incomplete state.

[0010] Since such incomplete data is directly stored in the memory, when the data is read therefrom by the reader-writer, it is impossible to accomplish a predetermined check operation. For example, when the card is adopted as a commuter pass, the states of the pass such as a period thereof, a valid period thereof, a station name where the bearer took the train, and time when the bearer took the train are required to be accurate in any case. Otherwise, there arises a problem that the essential object of the card cannot be achieved.

[0011] It is therefore another object of the present invention to provide a non-contact type IC card guaranteeing the normal operation even when an abnormality occurs in an access operation between the card and the external device, thereby solving the problems of the non-contact type IC card.

IPR2025-00645 Page 01615

[0012] Namely, the present invention aims at providing a non-contact type IC card capable of preventing inappropriate data from being written therein even when the card enters an area accessible to the external device for a plurality of times at a short interval of time.

[0013] Moreover, another object of the present invention is to provide a non-contact type IC card guaranteeing the normal operation even when an abnormality occurs in the contact state during a write operation of data from the external device.

Disclosure of the Invention

[0014] A non-contact type IC card according to the present invention is defined in claim 1. The dependent claims 2 to 7 disclose particular embodiments thereof.

[0015] In accordance with the present invention, a non-contact type IC card achieving communications of signals with an external device in a noncontact manner includes main circuit means for conducting various operations based on functions of the IC card, operation inhibition signal generating means for creating an operation inhibition signal to inhibit the operation of the main circuit means for a predetermined period of time, and control means for controlling the main circuit means and the operation inhibition signal generating means. The control means operates the operation inhibition signal generating means when the operation of the main circuit means is finished and inhibits the operation of the main circuit means for a predetermined period of time according to the operation inhibition signal from the operation inhibition signal generating means

[0016] In accordance with the present invention, when an operation of the main circuit means is finished, the operation inhibition signal generating means operates to create an operation inhibition signal, thereby inhibiting the operation of the main circuit means for a predetermined period of time. In consequence, in a case where the card enters an area accessible to the external device a plurality of times during a short period of time, the second and subsequent accesses can be inhibited and hence the improper operation due to the plural accesses can be avoided. Moreover, since the inhibition of such accesses need not be monitored by the external device, the load imposed on the external device can be minimized.

[0017] In accordance with an embodiment of the present invention, a non-contact type IC card includes communicating means for communicating signals with an external device in a noncontact manner, a memory for storing therein data sent from the external device, and control means for controlling operations of the communicating means and the memory. The memory has an area subdivided into a plurality of areas for storing therein data sent from the external device, and the control means reads, when the data is to be read from the memory, the data from one of the plural areas in which the data is normally stored.

[0018] In accordance with the non-contact type IC card of an embodiment of the present invention, an area of a memory for storing therein data sent from the external device is subdivided into a plurality of areas such that when reading data from the memory, the data is read from an area of the plural areas in which the data is normally stored. In consequence, even when the data recorded in one of the areas is wrong, the data can be read from the other area. Consequently, even when an abnormality occurs in a write operation of data, the data can be read therefrom.

[0019] In consequence, a write operation of wrong data or absence of record data which occurs when the card holder moves therewith at a high speed can be coped with by executing a predetermined processing with the normal data read from the memory.

Brief Description of the Drawings

[0020] Fig. 1 is a functional block diagram showing an embodiment of a non-contact type IC card in accordance with the present invention;
Fig. 2 a circuit diagram showing a specific example of the card of Fig. 1;
Fig. 3 is a timing chart showing the operation of the circuit of Fig. 2;
Fig. 4 is a timing chart showing the operation of the control circuit of Fig. 2;
Fig. 5 is a block diagram showing another embodiment of a non-contact type IC card in accordance with the present invention;
Fig. 6 shows a write operation of data in a memory of the card of Fig. 5;
Fig. 7 shows a write operation of data in a memory of the card of Fig. 5;
Fig. 8 shows a write operation of data in a memory of the card of Fig. 5;
Fig. 9 shows a write operation of data in a memory of the card of Fig. 5;
Fig. 10 is a flowchart showing the operation of the card of Fig. 5;
Fig. 11 is a flowchart showing the operation of the card of Fig. 5;
Fig. 12 is a flowchart showing the operation of the card of Fig. 5; and
Fig. 13 is a flowchart showing the operation of the card of Fig. 5

Best Mode for Carrying Out the Invention

[0021] Referring next to the accompanying drawings, description will be given in detail of a non-contact type IC card in accordance with the present invention.

[0022] Fig. 1 shows an embodiment of a non-contact type IC card in accordance with the present invention. This IC card is an IC card of an external power supply type receiving power supply from an external device. In this connection, portions not directly related to the present invention are not shown in this embodiment.

[0023] The card has a power source circuit 10. The power source circuit 10 is a power supply circuit for transmitting power supplied from a reader-writer to the respective components of the card. The power source circuit 10 is coupled with the reader-writer via a magnetic coupling shown in the diagram or a capacitive coupling not shown therein to receive power supplied from the reader-writer.

[0024] The power source circuit 10 is connected to a main circuit 16. The main circuit 16 is a circuit accomplishing operations according to various functions of the card and is constituted with a central processing unit (CPU), a memory, etc. For example, as shown in Fig. 5, there are included a memory 32 and a memory control section 36.

[0025] The main circuit 16 has a function to read, when the card is put by the bearer into an area accessible to the reader-writer, ID data from the memory 16 to output the data to the reader-writer and/or a function to collate ID data sent from the reader-writer with data stored in the memory 32. Moreover, the main circuit 16 writes in the memory 32, after the passage of the bearer is admitted by the reader-writer as a result of such a collation of the ID data, an indication that the passage is admitted by the data sent from the reader-writer.

[0026] The card in addition has a re-access inhibition time setting circuit 12. The circuit 12 is connected to the power source circuit 10 to set a period of time for inhibiting a reaccess based on a voltage supplied from the power source circuit 10 and a control signal sent from the control circuit 14 and then outputs a re-access inhibition time setting signal to the control circuit 14.

[0027] The control circuit 14 is connected to the circuit 12 and the main circuit 16 to inhibit the operation of the main circuit 16 for a predetermined period of time according to the re-access inhibition time setting signal outputted from the circuit 12. Furthermore, the control circuit 14 controls, in accordance with an access operation terminating signal transmitted from the main circuit 16, the setting operation of the circuit 12.

[0028] Fig. 2 shows a more specific construction of the circuit of Fig. 1. Four diodes D1, D2, D3, and D4, two capacitors C1 and C2, and a regulator 20 are disposed as elements corresponding to the power source circuit 10 of Fig. 10. Electric energy supplied from the reader-writer via a coil L is rectified by the diodes D1 to D4 and the regulator 20. Alternating-current components are removed therefrom by the capacitors C1 and C2 such that the resultant signal is sent to the main circuit 1 and the re-access inhibition time setting circuit 12.

[0029] The circuit 12 possesses a transistor Q. The transistor Q has an emitter region connected to an output of the power source circuit 10 and a base region which is connected via a resistor R2 to the output from the power source 10 and which is connected via a resistor R4 to an output of the control circuit 14. The transistor Q has a collector region linked with an anode of the diode D5 having a cathode connected to a resistor R1 and a capacitor C3. Other terminals respectively of the resistor R1 and the capacitor C3 are grounded. The cathode of the diode D5 is further connected to a gate region of an field-effect transistor (FET) of an n-type channel 24. The FET 24 has a drain region which is linked via a resistor R3 to an output of the power source circuit 10 and which is linked to a Schmitt trigger circuit 22, whereas the FET 24 has a source region grounded. The Schmitt trigger circuit 22 has an output connected to an input of the control circuit 14.

[0030] Referring to the timing chart of Fig. 3, the operation of the circuit 12 will be described. In a case where the card is used as a commuter pass and is put into an accessible area of the reader-writer at a gate twice in a short period of time, the circuit 12 sets an inhibition time for inhibiting the second access.

IPR2025-00645 Page 01616

[0031] At a point A of Fig. 2, power as indicated by A in Fig. 3 is supplied as an output from the power source circuit 10. Namely, when the card enters the accessible area of the reader-writer twice (at points of time t1 and t4), energy is supplied at each point of time from the reader-writer via the power supply circuit 10. When power is supplied at the point A, the power is fed to the main circuit 16, thereby enabling the main circuit 16 to operate. During the operation of the main circuit 16, as indicated by B in Fig. 3, the main circuit 16 is powered and a signal B denoting that the main circuit 16 is operable is delivered via the resistor R4 to the base region of the transistor Q (time t1). Consequently, the transistor Q is in a non-conductive state and the power supplied to the point A is not fed to a point C. The potential of the point C is hence at a ground level as designated by C in Fig. 3. In consequence, since any signal is not inputted to the gate region of the FET 24, the FET 24 is in a non-conductive state and a point D of the drain region of the FET 24 is supplied with the output from the power source circuit 10 as indicated by D in Fig. 3. As a result, the output from the Schmitt trigger circuit 22 is also as denoted by E in Fig. 3 and the output E is transmitted to the control circuit 14. The control circuit 14 outputs, according to the output E, a signal allowing the operation of the main circuit 16 to the main circuit 16.

[0032] When the operation of the main circuit 16 is finished (time t2), the output of the signal B from the control circuit 14 is stopped. This sets the base region of the transistor Q to a low level and hence the transistor Q becomes to be conductive, which increases the potential at the point C as denoted by C in Fig. 3. At the time t3 when the power supply A from the power source circuit 10 is interrupted, the power from the power source circuit 10 is not supplied to the point C. However, according to a discharging operation of electric charge accumulated in the capacitor C3 during the power supply period, the potential of the point C is gradually decreased in accordance with the time constant of the capacitor and the resistor as indicated by C in Fig. 3.

[0033] At a point of time T4, when the card is again put into the accessible area of the reader-writer and the second power is supplied from the power source circuit 10, a signal B indicating that power can be supplied to the main circuit 16 is sent from the control circuit 14 to the transistor Q, which sets the transistor Q to a non-conductive state. In consequence, the point C is kept remained in a state where power is not supplied from the power source circuit 10 and hence the potential of the point C continues lowering as shown in Fig. 3. As a result, since the potential inputted to the gate region of the FET 24 continues decreasing and the current flowing from the drain region to the source region of the FET 24 is minimized, the potential of the point D is gradually increased. In consequence, the voltage D inputted to the Schmitt trigger circuit 22 is gradually increased, at a point of time t5 where the voltage D exceeds the predetermined value, a signal E is outputted from the Schmitt trigger circuit 22. According to this output E, the control circuit 14 outputs a signal allowing the operation of the main circuit 16 to the main circuit 16.

[0034] As above, after the output E from the Schmitt trigger circuit 22 is set to a high level, the operation of the main circuit 16 is allowed. Consequently, after the first operation (access to the reader-writer) of the main circuit 16 at the point of time t2 is finished, the operation of the main circuit 16 is not allowed until a point of time t5. In consequence, even in a case where the card is put to the accessible area at the time t4 to supply power from the power source circuit 10, the main circuit 16 does not achieve any operation. As above, after the first access is terminated, the access to the reader-writer can be inhibited for a fixed period of time.

[0035] Subsequently, the operation of the control circuit 14 will be described by reference to the flowchart of Fig. 4. Whether or not power is being supplied is judged (step 102). If this is not the case, a wait operation is effected until the power-on state occurs. If the power is being supplied, it is assumed that the card has entered the accessible area of the reader-writer and a check is made to determine whether or not the point of time is during the re-access inhibition period (step 104). If this is the case, whether or not the power is off is judged (step 106). If the power is not off, a wait operation is achieved until the power is turned off. When the power is turned off, it is assumed that the card is removed from the accessible area of the reader-writer and control is returned to the first step 102.

[0036] In the step 104, if the current point is not in the re-access inhibition period, it is assumed that the access to the reader-writer becomes to be possible and then a predetermined data communication is achieved with the reader-writer (step 108). Whether or not the data communication has been completed is judged (step 110). If this is the case, the re-access inhibition period is set (step 112). Thereafter, whether or not the power is turned off is checked (step 114). If the power is not turned off, a wait operation is executed until the power is turned off. When the power is turned off, it is assumed that the card is removed from the accessible area of the reader-writer and then control is returned to the first step 102.

[0037] Also in the case where the data communication is not completed in the step 110, whether or not the power is turned off is judged (step 116) such that if this is the case, control is passed to the step 102.

[0038] As above, in accordance with the card of the present embodiment, after an access is finished, the re-access can be inhibited for a fixed period of time. In consequence, in a case where the card enters the accessible area of the reader-writer two or more times in a short period of time, the second and subsequent accesses to the reader-writer can be inhibited and hence the inappropriate operation due to a plurality of accesses can be prevented. Moreover, since the card has the function to inhibit the access, the operation to inhibit the re-access of the card need not be achieved by the reader-writer, thereby minimizing the load imposed on the reader-writer.

[0039] In accordance with the card, in a case where, for example, it is necessary at a gate to check passages of many cards in a short period of time, the reader-writer is not required to check the re-access. Consequently, after an access of a card, the reader-writer can immediately await a passage of the next card, which enables the accesses to many cards in a smooth manner.

[0040] In accordance with the present invention as described above, when the operation of the main circuit means is terminated, the operation inhibition signal generating means operates to create an operation inhibition signal, thereby inhibiting the operation of the main circuit means for a predetermined period of time. Consequently, in a case where the card enters an area accessible to the external device a plurality of times in a short period of time, the second and subsequent accesses can be inhibited, thereby preventing the inappropriate operation due to the plural accesses. Furthermore, since the access inhibition above need not be monitored by the external device, the load on the external device can be reduced.

[0041] Fig. 5 shows another embodiment of a non-contact type IC card in accordance with the present invention. This card 30 includes a memory 32 of an electrically erasable programmable ROM (EEPROM) or the like. The memory 32 has two areas 321 and 322 in this embodiment. As will be described later, in the IC card of the embodiment, data items are recorded in these two areas 321 and 322 together with numbers indicating sequence numbers of the data item write operation. In a data read operation, the data items are read by referencing the numbers in the areas so that data is read from one of the areas last undergone a recording operation. Moreover, in a case where data recorded in either one of the two areas 321 and 322 is in a destroyed state due to, for example, an interruption of a data write operation, data recorded in the remaining one thereof is read. With the provision of two areas, even when an abnormality occurs during a data write operation in one of the areas of the card, data can be read from the remaining area for use thereof, which thereby prevents an operation failure. In this connection, the number of areas disposed in the memory 32 is not limited to two, namely, the number may be three or more.

[0042] The card 30 further include a read area deciding section 34 connected to the memory 32. The read area deciding section 34 judges to determine from which one of the two areas 321 and 322 of the memory data is to be read. The memory 32 and the section 34 are connected to a memory control section 36. The section 36 controls according to commands an operation to write in the memory 32 data sent from a reader-writer, not shown, via a noncontact terminal 40 and a modulating and demodulating section 38 and an operation to read data stored in the memory 32 so as to feed the data to the reader-writer. The memory control section 36 achieves a control operation to record data sent from the reader-writer alternately in the two areas 321 and 322 together with the numbers indicating the recording order. Moreover, particularly, the section 36 controls a data read operation to read data from an area determined by the section 34.

[0043] The modulating and demodulating section 38 modulates data outputted from the memory control section 36 to the reader-writer and demodulates data inputted from the reader-writer via the noncontact terminal 40. The terminal 40 is used to communicate data with the reader-writer, not shown, in a noncontact manner.

[0044] The power source circuit 10 is, like in the embodiment described above, a circuit to send power supplied from the reader-writer to the respective sections of the card 30. The power source circuit 10 is coupled with the reader-writer via a magnetic coupling shown in the diagram or a capacitive coupling, not shown, to receive power supplied from the reader-writer.

[0045] Referring to the changes in the recording state of the memory 32 shown in Figs. 6 to 9, description will be given of the operation to write data in the memory 32. In each of the areas 321 and 322, there are disposed the areas including a data area D in which data is recorded, a number area N in which a number of a write sequence of data is recorded, and a check code area in which a check code is recorded.

IPR2025-00645 Page 01617

[0046] immediately after the card 30 is issued, as shown in Fig. 6, there are recorded data 1, "0" as the number denoting the write sequence, and a predetermine code C such as a CRC code in the data areas D, N, and C respectively. The data recorded in the data area D is one of various kinds of data items such as an ID number communicated between the IC card and the reader-writer. The number indicating the write sequence recorded in the number area N indicates a write sequential number of data recorded in the data area D of each of two areas. As shown in Fig. 6, immediately after the issuance of the card 30, "0" is recorded as an initial value.

[0047] The check code recorded in the check code area C is used to determine whether or not the data is normal, and one of the known various codes is employed.

[0048] For the data to be recorded in the data area D, data inputted from the reader-writer via the noncontact terminal 40 is demodulated by the modulating and demodulating section 38 and is then sent from the memory control section 36 to the memory 32 so as to be stored therein. Moreover, the data to be recorded in the data area D and the code to be recorded in the check code area C are generated by the memory control section 36 and is then sent to the memory 32 to be stored therein.

[0049] Immediately after the issuance of the card 30, any data is not recorded in the area 322. Consequently, in a data read operation, the data in the area 322 is assumed to be in a destroyed state by the read area deciding section 34 such that data recorded in the area 321 is read by the memory control section 36.

[0050] Next, as shown in Fig. 7, a first data write operation is accomplished in the area 322. As shown in this diagram, data 2 is recorded in the data area D and a number "1" is recorded as a data record sequential number in the number area N. In the check code area C, there is recorded a predetermined check code. In a state in which the first data write operation has been conducted, the section 34 compares the number recorded in the number area N of the area 321 with that recorded in the number area N of the area 322 to determine that the data recorded in the area 322 is the latest data. Consequently, in the data read operation, the data 2 recorded in the area 322 is read.

[0051] In addition, as shown in Fig. 8, a second data write operation is achieved in the area 321. The data write operations are conducted as above in the two areas 321 and 322 in an alternating manner.

[0052] As a result of the second data write operation of Fig. 8, in the area 321, data 3 is recorded in the data area D, a number "2" is recorded as a data record sequential number in the number area N, and a predetermined check code is recorded in the check code area C. In a state where the second data write operation is achieved as above, the data recorded in the area 321 is the latest data and hence the data 3 recorded in the area 321 is read in the data read operation.

[0053] Subsequently, in a similar manner, data write operations are conducted in the two areas 321 and 322 in an alternating fashion. For example, as shown in Fig. 9, in a case where after the n-th data is correctly written in the area 322, if the (n + 1)-th data write operation in the area 321 results in a failure, the data in the area 321 is in the destroyed state. Consequently, in this case, the read area deciding section 34 assumes, without achieving the comparison between the numbers stored in the number areas N of the two areas, that the data recorded in the area 322 is the latest data such that the data is read by the memory control unit 36.

[0054] Subsequently, the operation of the IC card 30 will be described according to the flowcharts shown in Figs. 10 to 13.

[0055] First, in a step 202 of Fig. 10, normality or abnormality of the data in the two areas 321 and 322 of the memory 32 is judged by checking the check code by the read area deciding section 34. Whether or not the data of each of the areas 321 and 322 is wrong (NG) is judged (step 204). If this is the case, the section 34 outputs a signal of the condition to the section 36, which then proceeds to the processing of Fig. 11.

[0056] In a step 230 of Fig. 11, the section 36 judges to determine whether or not a read operation is to be executed. If this is the case, a signal indicating that the memory 32 is in the destroyed state is outputted from the section 36 to the reader-writer (step 232). Otherwise, whether or not a write operation is to be executed is judged (step 234). If this is the case, data is written in the data area D of the area 321 and a number "0" is recorded in the number area N (Step 236). If the write operation is not assumed in the step 234, control is returned to the step 230 to repeatedly achieve the same operation.

[0057] In the step 204 of Fig. 10, if data of both of the two areas 321 and 322 are not wrong (NG), control is passed to a step 206 such that the section 34 checks to determine whether or not the data in the area 321 is NG. If this is the case, control is transferred to the processing of Fig. 12.

[0058] In a step 240 of Fig. 12, the section 36 judges to decide whether or not a read operation is to be executed. If this is the case, data recorded in the area 322 is read to be transmitted to the reader-writer (step 242). Otherwise, whether or not a write operation is to be achieved is judged (step 244). If this is the case, data is written is the data area D of the area 321 and the number to be written in the number area N is updated (step 246). In the step 244, if the write operation is not assumed, control is returned to the step 240 to repeatedly accomplish the same operation.

[0059] In the step 206 of Fig. 10, when the data in the area 321 is not NG, control proceeds to a step 208 in which the section 34 judges to determine whether or not the data in the area 322 is NG. If this is the case, control is passed to the processing of Fig. 13. In a step 250 of Fig. 13, the section 36 judges to decide whether or not a read operation is to be executed. If this is the case, data recorded in the area 321 is read to be transmitted to the reader-writer (step 252). In the case of a write operation, data is written in the data area D of the area 322 and a number to be written in the number area N is updated (step 256). In the step 254, when the write operation is not assumed, control is returned to the step 250 to repeatedly accomplish the same operation.

[0060] In the step 208 of Fig. 10, when the data in the area 322 is not NG, control proceeds to a step 210 such that the section 34 judges to determine whether or not the number recorded in the number area N of each of the areas is successive. If this is not the case, data of each of the areas is assumed to have been destroyed and control is transferred to the processing of Fig. 11. If the number is consecutive, the number of the area 321 is compared with that of the area 322 (step 212). If the number of the area 321 is larger than that of the area 322, the section 34 assumes that the data recorded in the area 321 is the latest data and then passes control to the processing of Fig. 13 to read data from the area 321. In the step 212, if the number of the area 321 is smaller than that of the area 322, the section 34 assumes that the data recorded in the area 322 is the latest data and then transfers control to the processing of Fig. 12 to read data from the area 322.

[0061] As above, according to the IC card of the present embodiment, the memory 32 is subdivided into two areas 321 and 322 to record data alternately in these areas with a number indicating a write sequential number assigned to each of the recorded data. In consequence, even when data recorded in one of these areas is wrong, data can be read from the other area and hence the data read operation is not prevented even when an abnormality occurs in the data write operation.

[0062] For example, when the card is adopted as a commuter pass or a key for entrance and exit for a place, in a case where the holder moves at a high speed while putting the card in the proximity of the reader-writer, the power supply from the reader-writer is interrupted at an intermediate point of the data write operation and hence the data thus written is wrong. However, also in such a case, data such as the gate check state is kept in the other area; consequently, the disabled state of the data read operation can be avoided by reading the recorded data.

[0063] In addition, when the data recorded in each of the areas is normal, the numbers recorded in the number areas N of the two areas are compared with each other to select and to read the last recorded data. Consequently, although data items are recorded in two areas, it will not occur that the old data is read by mistake.

[0064] In accordance with the non-contact type IC card of the present invention, the memory has an area subdivided into a plurality of areas for storing therein data sent from an external device. In a case of an operation to read data from the memory, the data is read from one of the areas in which the data is normally recorded. Consequence, also in a case where data recorded in an area is wrong, data can be read from another area and hence the data read operation is not disabled even when an abnormality takes place in the data write operation.

[0065] Consequently, a write operation of wrong data and absence of record data caused, for example, when the card holder moves at a high speed with the card can be coped with by reading the normal data so as to conduct a predetermined processing.

[0066] Fig. 14 shows further another embodiment of a non-contact type IC card in accordance with the present invention. This card includes both configurations of the cards shown in Figs. 1 and 5. According to this card, as can be appreciated from the explanation above, after an access is finished, a reaccess can be inhibited for a fixed period of time. In consequence, when the card enters an accessible area of the reader-writer two or more times in a short period of time, the second and subsequent accesses to the reader-writer can be inhibited and hence an inappropriate operation due to the plural access can be prevented. Moreover, since the card has a function to inhibit the access, the operation to inhibit the re-access of the card need not be accomplished by the reader-writer and hence the load imposed on the reader-writer can be mitigated.

IPR2025-00645 Page 01618

[0067] Furthermore, a memory 32 is subdivided into two areas 321 and 322 such that data is recorded alternately in these areas with a number indicating a write sequence number assigned to the recorded data. Consequently, even when data recorded in one of the areas is wrong, data can be read from the other area and hence the data read operation is not disabled even when an abnormality occurs in the data write operation.

[0068] Moreover, in a case where data written in each of the areas is normal, the numbers recorded in the number areas N of the two areas are compared with each other so as to select and to read the latest record data. Consequently, although data items are recorded in two areas, the old data cannot be read by mistake.

[0069] In this regard, the respective embodiments have been described in conjunction with non-contact type IC card of an external power supply type to which power is supplied from an external device. However, the present invention is not restricted by the IC card of the external power supply type and is also applicable to an IC card of an integrated power supply type. In a case of the IC card of the integrated power supply type, there is disposed an integrated power source in addition to the power source circuit 10 above.

Patent Citations (24)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
IT1063465B *	1976-11-03	1985-02-11	Mesdan Spa	AUTOMATIC KNOTTER FOR THE FORMATION OF THE FISHER'S KNOT PARTICULARLY FOR LARGE TITLE YARNS
JPS5737228Y2 *	1976-12-23	1982-08-17		
JPS61686B1A *	1984-09-12	1986-04-09	Toshiba Corp	Portable medium
JPH0473196B2 *	1985-05-29	1992-11-20	Toppan Moore Kk	
GB8522418D0 *	1985-09-10	1985-10-16	Shorrock Security Systems Ltd	Non-contact personal identification system
JP2557838B2 *	1986-02-18	1996-11-27	株式会社東芝	IC card
JPS62234459A *	1986-04-04	1987-10-14	Casio Comput Co Ltd	Electronic blackboard device
JPS62287389A *	1986-06-05	1987-12-14	Omron Tateisi Electronics Co	id card
JPS63226752A *	1987-03-16	1988-09-21	Omron Tateisi Electronics Co	Data writing system for id system
JPS63273979A *	1987-05-06	1988-11-11	Mitsubishi Electric Corp	Non-contact card system
JPS6482194A *	1987-09-24	1989-03-28	Fuji Electric Co Ltd	Non-contact communication device for contact identification card
JPH01128269U *	1988-02-16	1989-08-22		
JPH02226390A *	1989-02-27	1990-09-07	Omron Tateisi Electron Co	Transponding card
JP2645163B2 *	1990-03-13	1997-08-25	三菱電機株式会社	Non-contact IC card
JP2822624B2 *	1990-07-03	1998-11-11	三菱電機株式会社	Non-contact IC card
JP2549189B2 *	1990-07-17	1996-10-30	三菱電機株式会社	IC card
JPH04113489A *	1990-09-04	1992-04-14	Mitsubishi Electric Corp	Non-contact ic card
US5191192A *	1990-09-10	1993-03-02	Mitsubishi Denki Kabushiki Kaisha	Non-contact type information card and communication system
JP2549192B2 *	1990-09-19	1996-10-30	三菱電機株式会社	Non-contact IC card and method of using the same
JP2872793B2 *	1990-10-01	1999-03-24	株式会社日立製作所	IC card
JPH04171592A *	1990-11-06	1992-06-18	Mitsubishi Electric Corp	Non-contact type information card
JP2543440B2 *	1990-12-17	1996-10-16	三菱電機株式会社	IC card and IC card system
EP0492482B1 *	1990-12-28	1996-10-23	Mitsubishi Denki Kabushiki Kaisha	Non contact type IC-card
JP3027019B2 *	1991-03-26	2000-03-27	東京エレクトロン株式会社	Heat treatment equipment

* Cited by examiner, † Cited by third party

Cited By (27)

Publication number	Priority date	Publication date	Assignee	Title

IPR2025-00645 Page 01619

Family To Family Citations

JP3442076B2 †	1991-12-04	2003-09-02	シチズン時計株式会社	Data carrier
JP2891136B2 *	1994-07-19	1999-05-17	株式会社デンソー	In-vehicle equipment with automatic toll collection system
JP2907048B2 *	1995-02-17	1999-06-21	株式会社デンソー	Mobile communication roadside unit, mobile communication mobile unit, and mobile communication system
US5847447A *	1996-07-09	1998-12-08	Ambient Corporation	Capcitively coupled bi-directional data and power transmission system
US5812942A *	1996-09-24	1998-09-22	Motorola, Inc.	Balanced differential radio receiver and method of operation
US5815020A *	1996-09-24	1998-09-29	Motorola, Inc.	Balance differential receiver
JPH10135882A *	1996-10-24	1998-05-22	Toshiba Corp	Contactless information recording medium and its data transmission system
US6164532A *	1997-05-15	2000-12-26	Hitachi, Ltd.	Power transmission system, power transmission/communication system and reader and/or writer
US5963144A *	1997-05-30	1999-10-05	Single Chip Systems Corp.	Cloaking circuit for use in a radiofrequency identification and method of cloaking RFID tags to increase interrogation reliability
JP3721725B2 *	1997-07-09	2005-11-30	ソニー株式会社	Information processing method and information processing apparatus
US6074312A *	1997-07-28	2000-06-13	Dynamic Solutions International	Golf handicap system and methods
US6079619A *	1997-08-05	2000-06-27	Denso Corporation	Identification tag for wireless communication with remote controller
JP3824481B2 *	1999-07-29	2006-09-20	富士通株式会社	Non-contact IC card presence / absence detection circuit
US6612852B1	2000-04-13	2003-09-02	Molex Incorporated	Contactless interconnection system
US6638297B1	2000-04-13	2003-10-28	Molex Incorporated	Contactless interconnection system
JP4208557B2 *	2002-11-28	2009-01-14	キヤノン株式会社	Contactless communication method card
JP3988995B2 *	2003-03-14	2007-10-10	ソニー・エリクソン・モバイルコミュニケーションズ株式会社	Information processing apparatus and method, recording medium, and program
JP4717381B2 *	2004-06-11	2011-07-06	株式会社エヌ・ティ・ティ・ドコモ	Mobile device and access control method
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
EP1959377A4 *	2005-11-16	2009-12-02	Kyodo Printing Co Ltd	Noncontact ic card
JP4228936B2 *	2006-09-12	2009-03-11	東芝テック株式会社	Wireless communication device
CA2636304C *	2007-06-27	2014-12-30	Research In Motion Limited	System and method for improving smart card reader reconnections
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
EP0541818B1	1997-12-03	Non-contact type ic card
US6462647B1	2002-10-08	Rechargeable active transponder
US4795898A	1989-01-03	Personal memory card having a contactless interface using differential data transfer
US4798322A	1989-01-17	Card reader/writer station for use with a personal memory card using differential data transfer
KR100593272B1	2006-06-26	Minimum voltage radio frequency identification

IPR2025-00645 Page 01620

EP0475716B1	1995-06-14	Non-contact type information card and communication system
US5736728A	1998-04-07	Non contact IC card and a non contact IC card system
KR100275167B1	2000-12-15	Chip card with field strength detector
US5382778A	1995-01-17	Non-contact IC card
EP1012784B1	2003-04-23	Data transaction device having contact and contactless modes of operation
EP1042731B1	2001-10-04	Contact/contactless smart card having customizable antenna interface
US5286955A	1994-02-15	Method for wireless transmission of data to a data carrier
EP0838694B1	2001-07-11	Non-contact information storage medium and data transmission method for the medium
US7000835B2	2006-02-21	Noncontact type IC card and system thereof
US5999713A	1999-12-07	Chip card with a contactless energy supply and data transmission devices
US20040180637A1	2004-09-16	Wireless communication IC and wireless communication information storage medium using the same
JPH0869513A	1996-03-12	Noncontact ic card
KR19980081575A	1998-11-25	Smart card with adjustable level of external input voltage
EP0159530B1	1989-01-25	Card reader
JP2002064402A	2002-02-28	Non-contact transponder
JP2004297779A	2004-10-21	Radio communications ic and radio communication information storage medium using the same
US6931234B1	2005-08-16	Data processing device and method of controlling operation of data processing device
US6944246B1	2005-09-13	Data processing device for switching between terminal mode and RF mode with a digital circuit
JP2942809B2	1999-08-30	Non-contact IC card
JP3497527B2	2004-02-16	Data carrier communication control system

Priority And Related Applications

Child Applications (2)

Application	Priority date	Filing date	Relation	Title
EP97105219A	1991-05-22	1992-05-21	Division	Non-contact type IC card
EP97105219.6		1997-03-27	Division-into	

Priority Applications (5)

Application	Priority date	Filing date	Title
JP3146760A	1991-05-22	1991-05-22	Non-contact type ic card
JP146760/91		1991-05-22	
JP3169169A	1991-06-14	1991-06-14	Non-contact IC card
JP169169/91		1991-06-14	
PCT/JP1992/000653	1991-05-22	1992-05-21	Non-contact type ic card

Applications Claiming Priority (1)

Application	Filing date	Title
EP97105219A	1992-05-21	Non-contact type IC card

Legal Events

Date	Code	Title	Description

IPR2025-00645 Page 01621

1993-04-02	PUAI	Public reference made under article 153(3) epc to a published international application that has entered the european phase	**Free format text:** ORIGINAL CODE: 0009012
1993-05-19	17P	Request for examination filed	**Effective date:** 19930222
1993-05-19	AK	Designated contracting states	**Kind code of ref document:** A1 **Designated state(s):** DE FR GB
1994-03-30	RHK1	Main classification (correction)	**Ipc:** G06K 19/07
1994-08-24	AK	Designated contracting states	**Kind code of ref document:** A4 **Designated state(s):** DE FR GB
1994-08-24	A4	Supplementary search report drawn up and despatched	
1995-10-18	17Q	First examination report despatched	**Effective date:** 19950904
1997-02-19	GRAG	Despatch of communication of intention to grant	**Free format text:** ORIGINAL CODE: EPIDOS AGRA
1997-06-04	GRAH	Despatch of communication of intention to grant a patent	**Free format text:** ORIGINAL CODE: EPIDOS IGRA
1997-06-04	GRAG	Despatch of communication of intention to grant	**Free format text:** ORIGINAL CODE: EPIDOS AGRA
1997-09-05	GRAH	Despatch of communication of intention to grant a patent	**Free format text:** ORIGINAL CODE: EPIDOS IGRA
1997-10-17	GRAA	(expected) grant	**Free format text:** ORIGINAL CODE: 0009210
1997-12-03	AK	Designated contracting states	**Kind code of ref document:** B1 **Designated state(s):** DE FR GB
1997-12-03	XX	Miscellaneous	**Free format text:** TEILANMELDUNG 97105219.6 EINGEREICHT AM 27/03/97.
1998-01-15	REF	Corresponds to:	**Ref document number:** 69223381 **Country of ref document:** DE **Date of ref document:** 19980115
1998-03-13	ET	Fr: translation filed	
1998-10-09	STAA	Information on the status of an ep patent application or granted ep patent	**Free format text:** STATUS: NO OPPOSITION FILED WITHIN TIME LIMIT
1998-11-25	26N	No opposition filed	
2002-01-01	REG	Reference to a national code	**Ref country code:** GB

IPR2025-00645 Page 01622

			Ref legal event code: IF02
2003-05-08	PGFP	Annual fee paid to national office [announced via postgrant information from national office to epo]	**Ref country code:** FR **Payment date:** 20030508 **Year of fee payment:** 12
2003-05-19	PGFP	Annual fee paid to national office [announced via postgrant information from national office to epo]	**Ref country code:** GB **Payment date:** 20030519 **Year of fee payment:** 12
2003-05-29	PGFP	Annual fee paid to national office [announced via postgrant information from national office to epo]	**Ref country code:** DE **Payment date:** 20030529 **Year of fee payment:** 12
2004-05-21	PG25	Lapsed in a contracting state [announced via postgrant information from national office to epo]	**Ref country code:** GB **Free format text:** LAPSE BECAUSE OF NON-PAYMENT OF DUE FEES **Effective date:** 20040521
2004-12-01	PG25	Lapsed in a contracting state [announced via postgrant information from national office to epo]	**Ref country code:** DE **Free format text:** LAPSE BECAUSE OF NON-PAYMENT OF DUE FEES **Effective date:** 20041201
2005-01-12	GBPC	Gb: european patent ceased through non-payment of renewal fee	**Effective date:** 20040521
2005-01-31	PG25	Lapsed in a contracting state [announced via postgrant information from national office to epo]	**Ref country code:** FR **Free format text:** LAPSE BECAUSE OF NON-PAYMENT OF DUE FEES **Effective date:** 20050131
2005-03-04	REG	Reference to a national code	**Ref country code:** FR **Ref legal event code:** ST

Data provided by IF CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

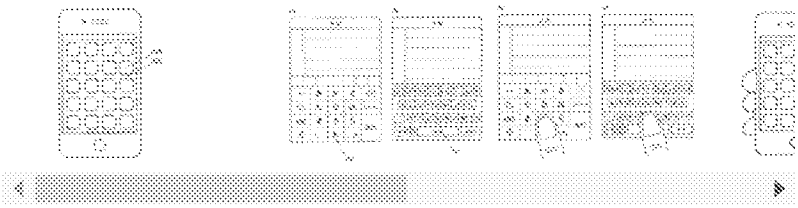
Patents JP3180086

Touch panel type small terminal operation tool

Abstract

An operation tool for a touch panel type small terminal that allows a human to perform an input operation in a natural state.
Two protrusions 12 are arranged in the circumferential direction at an angle of 30 ° to 150 ° in the vicinity of the tip of a sack body 11 for fitting on a finger.
[Selection] Figure 5

Images (7)



JP3180086U
Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: 和久 原

Worldwide applications

2012 JP

Application JP2012004401U events

2012-07-19 Application filed by 和久 原, 上原 みさ代
2012-07-19 Priority to JP2012004401U
2012-12-06 Application granted
2012-12-06 Publication of JP3180086U
Status Expired - Fee Related
2022-07-19 Anticipated expiration

Info: Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (4)

Hide Dependent

1. a) a sack body to fit on the finger.
b) An operation tool for a small-sized touch panel terminal, having two protrusions arranged at an angle of 30 ° to 150 ° in the circumferential direction near the tip of the sack body.

2. The touch panel type small terminal operating tool according to claim 1, wherein a portion of the nail is vacant.

3. The touch panel type small terminal operating tool according to claim 1 or 2, wherein means for attaching an artificial nail is provided at a nail portion.

4. The operation tool for a touch panel type small terminal according to any one of claims 1 to 3, wherein a link for connecting to a touch panel type small terminal as an operation target is fixed.

Description

The present invention is an operation for operating a touch panel type small terminal such as a smartphone (for example, Apple's iPhone (trademark) of the US) or a small portable music player (for example, the company's iPod (trademark)). Concerning ingredients. The touch panel type small terminal referred to in the present application is an information terminal device (including both a device having a telephone function and a device having no telephone function) that is large enough to be placed on one palm of a human. Various inputs can be made by placing the terminal on the palm of the hand and touching the panel with the finger of the other hand (or the thumb of the hand holding the terminal) while viewing the image displayed on the screen of the terminal panel Says the equipment that performs.

In recent years, touch panel type small terminals, mainly smartphones, have become increasingly popular due to their convenience and high functionality.

In many recent touch panel type small terminals, in addition to the operation of simply touching a certain point with one finger (tap), the operation of moving the finger while touching the panel with a finger (slide, flip), multiple times in a short time Various operations such as touching with two fingers (double tap), touching with multiple fingers (two-finger tap, etc.), touching with two fingers to open and close both fingers (pinch-in / pinch-out), etc. Operation is possible.

JP 2009-259062

Various operations in the touch panel type small terminal are basically based on an operation (tap) of touching a predetermined portion of the panel with one finger according to the display on the screen. At present, many touch-panel type small terminals employ a capacitive touch panel, and an operator does not need to press the screen strongly with a finger, but can input with a light touch. However, there is a problem that there are many erroneous inputs. That is, the user may accidentally touch an adjacent icon or key in an attempt to touch an icon or key.

IPR2025-00645 Page 01624

FIG. 1 shows an initial screen which is one of display screens of a smartphone. In this screen form, 4 × 5 = 20 relatively large icons 101 are displayed on the screen. The size of one icon is about 10 mm × 10 mm, but there is a gap of about 3 mm between icons, and when including this, the distance between adjacent icons is about 13 mm. Further, since the area 102 between adjacent icons is an input insensitive area, erroneous input is unlikely to occur in such a screen form.

However, in the case of a Japanese character input screen as shown in FIG. 2A, the size of one character input area (key area) 103 is 10 mm × 10 mm, which is substantially the same as the icon 101 on the initial screen. Although the size is large, there is no gap between adjacent key areas, so a finger often touches the adjacent area and erroneously inputs. Furthermore, in the Roman character (English) input screen as shown in FIG. 2 (b), the size of one key area 104 is only 4mm x 6mm, and the width when the panel is pressed is about 5-10mm. The possibility of erroneous input is very high (Fig. 3).

In the case of a relatively small smartphone (or a person with a large hand), it is often performed to operate with one hand. That is, as shown in FIG. 4, the icon is operated with the thumb of the hand holding the smartphone. In this case, in addition to the thumb being wider than the other fingers, the thumb to be operated is necessarily inclined with respect to the panel surface, so that the possibility of erroneous operation is further increased.

There is a method of using a dedicated pen as one of the panel operation methods for touch panel type small terminals. However, when performing document operations such as taking notes at the same time as the operation of the small terminal, the terminal pen and the document pen are used one by one. There is a problem that it is troublesome. In addition, when a dedicated pen is used, a touch panel type small terminal must be placed on a desk or the like or held with the other hand, so that a convenient method of operating with one hand cannot be used.

On the other hand, there is a method in which a sac provided with a small protrusion at the tip is fitted to a finger, and the touch panel type small terminal is operated by the protrusion (Patent Document 1). In the sac described in Patent Document 1 (in Patent Document 1, the sack body is referred to as a jig 11, the protrusion provided at the tip thereof is referred to as a pen tip portion 12, and the sac as a whole thereof is referred to as a touch pen 10). Since it is provided at the forefront of the sack body, the finger with the sack must be operated perpendicular to the screen of the small terminal. Therefore, in the case of the operation with the thumb as shown in FIG. 4, the operation is performed with a finger in a very unnatural state, and there is a problem that it is difficult to operate and is easily fatigued.

The problem to be solved by the present invention is to provide a touch panel type small terminal operating tool that allows a human to perform an input operation in a natural state.

An operation tool for a touch panel type small terminal according to the present invention, which has been made to solve the above problems,
a) a sack body to fit on the finger,
b) In the vicinity of the tip of the sack body, there are two protrusions arranged at an angle of 30 ° to 150 ° in the circumferential direction.

In the touch panel type small-sized terminal operating tool according to the present invention, a portion corresponding to a nail when fitted on a finger may be left open. As a result, it is possible to prevent the fingertips from being steamed, and the use for a long time becomes easy. In addition, a person with a long nail or a person with a false nail can be used.

Means for attaching an artificial nail may be provided on the nail portion of the touch panel type small terminal operating tool. By attaching artificial nails with various shapes and colors here, fashionability is enhanced, and users can easily find their own when multiple touch panel type small terminal operating tools are mixed. Will be able to.

You may attach the link (a string, an expansion coil, a wedge, etc.) for connecting with the touch panel type small terminal operation tool concerning the present invention with the touch panel type small terminal which is the operation object. That is, the touch panel type small terminal operation tool according to the present invention is attached to the touch panel type small terminal as an accessory. Thereby, when it is desired to operate the touch panel type small terminal, the touch panel type small terminal operating tool according to the present invention can be immediately fitted on the finger.

In the touch panel type small terminal operating tool according to the present invention, since the two protrusions are provided in the vicinity of the tip of the sack body, the center is directly below (that is, 2 with respect to the center plane of the finger). By fitting the fingertips so that the protrusions are symmetrical with each other, the protrusion that is the location where the touch panel is operated becomes slightly oblique. In other words, when the protrusion is placed directly underneath the finger in this way, the finger is slightly rotated (that is, the finger's center plane is slightly tilted from the state perpendicular to the panel surface). The touch panel is operated in (Status). Thereby, when the operator operates the panel of the touch panel type small terminal with the thumb, the thumb becomes a natural posture, and the input can be performed easily and surely.

Moreover, even when operating with a finger other than the thumb (for example, the index finger), the touch panel type small terminal operating tool according to the present invention is easy to operate. That is, normally, such a touch panel type small terminal operation tool fits on the finger on the dominant hand side, but when operating the touch panel with the finger on the dominant hand side, the palm should face the center side of the body or yourself. It is a natural posture to tilt your finger. Since the touch panel type small terminal operating tool according to the present invention can operate the touch panel with such a natural finger posture, it can be used for a long time without getting tired. Further, since the finger is in a natural posture, the operation is reliable and the target input area (icon, key, etc.) can be operated without error.

The two protrusions are provided so that both right-handed and left-handed people can use it easily. Of course, right-handed people (or left-handed people) The two protrusions may be properly used depending on the operation.

The external view of the initial screen state of the smart phone which is an example of a touchscreen type small terminal. It is an external view of a character input screen of a smartphone, (a) is a Japanese (Kana) input screen, (b) is a Roman character (English) input screen. FIG. 3 is an external view when inputting characters with the index finger on the Japanese (kana) input screen (a) and the Roman character (English) input screen (b) of FIG. 2; The external view in the case of operating a smart phone with one hand. BRIEF DESCRIPTION OF THE DRAWINGS It is an external view of the operation tool for touchscreen type small terminals concerning this invention, (a) is a bottom view, (b) is a top view, (c) is a side view, (d) is a front view. It is an external view of a touch panel type small terminal operating tool provided with an opening in the nail portion, (a) is a bottom view, (b) is a top view. The external view of the operation tool for touchscreen type small terminals which provided the link for connecting with a touchscreen type small terminal.

An example of the touch panel type small terminal operating tool according to the present invention is shown in FIG. The touch panel type small terminal operating tool 10 of this example includes a sack body 11 having a length enough to cover up to the first joint of the fingertip, and two protrusions 12 fixed near the tip. As shown in FIG. 5 (d), the two protrusions 12 are provided apart from each other by a central angle θ, which is in the range of 30 ° to 150 °. The height of the protrusion 12 is preferably about 2 to 5 mm.

The sack body 11 is made of a conductive rubber sheet (for example, EPDM (ethylene / propylene diene rubber) sheet) having a thickness of about 0.5 to 2 mm, and the protrusion 12 is also made of conductive rubber. It is desirable that the surface of the projecting portion 12 be subjected to a treatment for making it slip easily on the surface of the touch panel. Further, a slippery coating (for example, Newlite film NLAS (B) (Sakushin Kogyo Co., Ltd.)) may be provided on the surface.

IPR2025-00645 Page 01625

Another example of the touch panel type small terminal operating tool according to the present invention is shown in FIG. In the touch panel type small terminal operating tool 20 of this example, an opening 23 is provided in a nail portion of the sack body 21. The arrangement, shape, and the like of the protrusion 22 may be the same as in the above example. The material and the like may be the same as in the above example. When operating the panel of a touch panel type small terminal with a natural finger without using any tools, it is extremely difficult to operate with an artificial nail attached. The panel can be operated even with nails attached.

FIG. 7 shows still another example of the touch panel type small terminal operating tool according to the present invention. In the touch panel type small terminal operating tool 30 of this example, an expansion / contraction coil 34 for connecting to a touch panel type small terminal (not shown) is fixed to the sack body 31. The arrangement, shape, and the like of the protrusion 32 may be the same as in the above example. The material and the like may be the same as in the above example.

10, 20, 30 .. touch panel type small terminal operation tool 101 ... icon 102 .. area between adjacent icons (insensitive area)
103 ... Japanese (Kana) character key area 104 ... Romaji (English) key area 11, 21, 31 ... Sack body 12, 22, 32 ... Projection 23 ... Opening 34 ... Telescopic coil

Similar Documents

Publication	Publication Date	Title
CN103064629B	2016-06-15	It is adapted dynamically mancarried electronic aid and the method for graphical control
WO2012049942A1	2012-04-19	Mobile terminal device and display method for touch panel in mobile terminal device
JP4880304B2	2012-02-22	Information processing apparatus and display method
JP2014203183A	2014-10-27	Information processing device and program
JP2015531527A	2015-11-02	Input device
US20030117376A1	2003-06-26	Hand gesturing input device
WO2012162932A1	2012-12-06	Method and terminal for displaying left and right hands self-adaptive virtual keyboard
US20140055384A1	2014-02-27	Touch panel and associated display method
KR20140047515A	2014-04-22	Electronic device for inputting data and operating method thereof
JP2012199888A	2012-10-18	Portable terminal
US10671269B2	2020-06-02	Electronic device with large-size display screen, system and method for controlling display screen
TWI659353B	2019-05-11	Electronic apparatus and method for operating thereof
CN103927114A	2014-07-16	Display method and electronic equipment
CN102629184A	2012-08-08	Handheld terminal and operation method thereof
US20140359541A1	2014-12-04	Terminal and method for controlling multi-touch operation in the same
CN101124532A	2008-02-13	Computer input device
US20080024957A1	2008-01-31	Portable apparatus with thumb control interface
KR20160019762A	2016-02-22	Method for controlling touch screen with one hand
US20150172430A1	2015-06-18	Keypad for mobile terminal
US20140292689A1	2014-10-02	Input device, input method, and recording medium
TWI615747B	2018-02-21	System and method for displaying virtual keyboard
JP3180086U	2012-12-06	Touch panel type small terminal operation tool
JP6034140B2	2016-11-30	Display device, display control method, and program
TWI552064B	2016-10-01	Handheld touch device
US20170075453A1	2017-03-16	Terminal and terminal control method

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2012004401U	2012-07-19	2012-07-19	Touch panel type small terminal operation tool

Applications Claiming Priority (1)

Application	Filing date	Title
JP20120044011U	2012-07-19	Touch panel type small terminal operation tool

Legal Events

Date	Code	Title	Description
2012-09-29	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20120928
2012-11-14	R150	Certificate of patent (=grant) or registration of utility model	**Free format text:** JAPANESE INTERMEDIATE CODE: R150
2012-11-15	FPAY	Renewal fee payment (prs date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20151114 **Year of fee payment:** 3
2015-11-14	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

IPR2025-00645 Page 01627

Patents AU5079498

Transaction terminal for electronic purse transactions and the like

Classifications

G07F7/0866 Mechanisms actuated by objects other than coins to free or to actuate vending, hiring, coin or paper currency dispensing or refunding apparatus by coded identity card or credit card or other personal identification means by active credit-cards adapted therefor

View 3 more classifications

AU5079498A

Australia

Find Prior Art Similar

Inventor: James Arakaki

Current Assignee : Verifone Inc

Worldwide applications

1997 AU WO US

Application AU50794/98A events

1996-10-18	Priority to US28962968P
1996-10-18	Priority to US36002896Z
1997-10-17	Application filed by Verifone Inc
1997-10-17	Priority to PCT/US1997/017550
1998-05-15	Publication of AU5079498A
Status	Abandoned

Info: Patent citations (10), Cited by (89), Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (10)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US4032931A *	1975-12-22	1977-06-28	Haker Floyd H	Money transfer device keyboard terminal
US4277837A *	1977-12-30	1981-07-07	International Business Machines Corporation	Personal portable terminal for financial transactions
US4454414A *	1982-06-16	1984-06-12	Vericard Corporation	Funds transfer system using optically coupled, portable modules
US02898195 *	1984-07-19	1987-05-12	Diebold, Incorporated	Electronic funds transfer terminal or similar article
JPS6143397A *	1984-08-08	1986-03-01	Tokyo Electric Co Ltd	Merchandize selling data processing system
US4634845A *	1984-12-24	1987-01-06	Ncr Corporation	Portable personal terminal for use in a system for handling transactions
US5267149A *	1986-08-20	1993-11-30	Oki Electric Industry Co. Ltd.	System and method for registering passwords
JPS63118896A *	1986-11-06	1988-05-23	Omron Tateisi Electronics Co	Clearance terminal
FR2696032B1 *	1992-09-21	1994-12-23	Oberthur Okd	Device for carrying out transactions with microprocessor cards, and method for carrying out a transaction with such a device.
US5438184A *	1993-10-26	1995-08-01	Verifone Inc.	Method and apparatus for electronic cash transactions

* Cited by examiner, † Cited by third party

Cited By (89)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				

IPR2025-00645 Page 01628

US6847367B1 *	1998-07-23	2005-01-25	Hewlett-Packard Development Company, L.P.	Display for port area of electronic equipment
FR2785070B1 *	1998-10-26	2001-01-12	Xiring	DISPLAY SYSTEM COMPRISING A MICROCIRCUIT CARD AND A READER
EP1001388B1 *	1998-11-09	2004-04-14	Fujitsu Limited	Electronic transaction apparatus
US7222742B2 *	1999-06-17	2007-06-05	Lenovo (Singapore) Pte. Ltd.	System for organizing one or more personal computer accessory devices
FR2827058B1 *	2001-07-09	2005-05-27	A S K	ELECTRONIC CASH SYSTEM FOR ELECTRONIC COIN PURSE
US9224142B2	2002-02-05	2015-12-29	Square, Inc.	Card reader with power efficient architecture that includes a power supply and a wake up circuit
US9495675B2	2002-02-05	2016-11-15	Square, Inc	Small card reader configured to be coupled to a mobile device
US8678277B2	2010-10-13	2014-03-25	Square, Inc.	Decoding system coupled to a payment system that includes a cryptographic key
US9324100B2	2002-02-05	2016-04-26	Square, Inc.	Card reader with asymmetric spring
US8573489B2	2010-10-13	2013-11-05	Square, Inc.	Decoding systems with a decoding engine running on a mobile device with a touch screen
US9495676B2	2002-02-05	2016-11-15	Square, Inc.	Method of transmitting information from a power efficient card to a mobile device
US8602305B2	2010-10-13	2013-12-10	Square, Inc.	Decoding systems with a decoding engine running on a mobile device configured to be coupled and decoupled to a card reader with wake-up electronics
US8640955B2	2010-10-13	2014-02-04	Square, Inc	Decoding system running on a mobile device and coupled to a payment system that includes at least one of, a user database, a product database and a transaction database
US9262777B2	2002-02-05	2016-02-16	Square, Inc.	Card reader with power efficient architecture that includes a wake-up circuit
US9916581B2	2002-02-05	2018-03-13	Square, Inc.	Back end of payment system associated with financial transactions using card readers coupled to mobile devices
US9305314B2	2002-02-05	2016-04-05	Square, Inc.	Methods of transmitting information to mobile devices using cost effective card readers
US9262757B2	2002-02-05	2016-02-16	Square, Inc.	Method of transmitting information from a card reader with a power supply and wake-up circuit to a mobile device
US20120005039A1	2002-02-05	2012-01-05	Jack Dorsey	Method of conducting financial transactions
US8612352B2	2010-10-13	2013-12-17	Square, Inc.	Decoding systems with a decoding engine running on a mobile device and coupled to a payment system that includes identifying information of second parties qualified to conduct business with the payment system
US9286635B2	2002-02-05	2016-03-15	Square, Inc.	Method of transmitting information from efficient communication protocol card readers to mobile devices
US8571989B2	2010-10-13	2013-10-29	Square, Inc.	Decoding systems with a decoding engine running on a mobile device and coupled to a social network
US8701997B2	2010-10-13	2014-04-22	Square, Inc.	Decoding systems with a decoding engine running on a mobile device and using financial transaction card information to create a send funds application on the mobile device
US8701996B2	2010-10-13	2014-04-22	Square, Inc.	Cost effective card reader and methods to be configured to be coupled to a mobile device
US9582795B2	2002-02-05	2017-02-28	Square, Inc.	Methods of transmitting information from efficient encryption card readers to mobile devices
WO2004017255A1 *	2002-08-16	2004-02-26	Fujitsu Limited	Transaction terminal unit, and transaction terminal control method
JP4175464B2 *	2003-01-20	2008-11-05	旭精工株式会社	Smart card read / write device
US8364547B2 *	2003-03-17	2013-01-29	Gate Gourmet Switzerland, Gmbh	System for real-time sales and inventory reconciliation
US20060085308A1 *	2003-03-17	2006-04-20	Abanco International, Llc	System and method for sales and service reconciliation
WO2004084031A2 *	2003-03-17	2004-09-30	Abanco International Llc	System and method for sales and inventory reconciliation
US20050263590A1 *	2004-02-03	2005-12-01	James Branck	Point of sale terminal having integrated customer and operator interfaces
US20050181875A1 *	2004-02-18	2005-08-18	Coin	Mobile lottery, gaming and wagering system and method

			Mechanisms, Inc.	
US20050284004A1 *	2004-06-23	2005-12-29	Peters Margaret T	Secure shoe and method of using same
GB2422238B *	2005-01-21	2008-07-23	Lipman Electronic Engineering	Collapsible shield
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US8825073B1	2006-10-31	2014-09-02	United Services Automobile Association (USAA)	GPS validation for transactions
US7669759B1	2006-10-31	2010-03-02	United Services Automobile Association (Usaa)	GPS validation for transactions
US7669760B1 *	2006-10-31	2010-03-02	United Services Automobile Association (Usaa)	GPS validation for transactions
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080142585A1 *	2006-12-19	2008-06-19	Thales Avionics, Inc.	System and method for tendering payment on a vehicle, such as an aircraft
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US7975912B2 *	2007-12-07	2011-07-12	Dresser, Inc.	Method and system for operating a hybrid card reader
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8348112B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US9010643B2 *	2008-11-04	2015-04-21	Symbol Technologies, Inc.	Selective working distance range restriction in imaging system
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9436955B2	2009-06-10	2016-09-06	Square, Inc.	Methods for transferring funds using a payment service where financial account information is only entered once with a payment service and need not be re-entered for future transfers
US8500018B2	2010-10-13	2013-08-06	Square, Inc.	Systems and methods for financial transaction through miniaturized card reader with decoding on a seller's mobile device
US9619797B2	2010-10-13	2017-04-11	Square, Inc.	Payment methods with a payment service and tabs selected by a first party and opened by a second party at an geographic location of the first party's mobile device
US8870070B2	2010-10-13	2014-10-28	Square, Inc.	Card reader device
US9454866B2	2010-10-13	2016-09-27	Square, Inc.	Method of conducting financial transactions where a payer's financial account information is entered only once with a payment system
US8573487B2 *	2010-10-13	2013-11-05	Square, Inc.	Integrated read head device
US8870071B2 *	2010-10-13	2014-10-28	Square, Inc.	Read head device with selected sampling rate
US8573486B2	2010-10-13	2013-11-05	Square, Inc.	Systems and methods for financial transaction through miniaturized card reader with confirmation of payment sent to buyer
US8235287B2	2010-10-13	2012-08-07	Square, Inc.	Read head device with slot configured to reduce torque
US9016572B2	2010-10-13	2015-04-28	Square, Inc.	Systems and methods for financial transaction through miniaturized card with ASIC
MX2012004397A	2009-10-13	2012-08-15	Square Inc	Systems and methods for financial transaction through miniaturized card reader.
US8887600B2 *	2010-10-13	2014-11-04	Square, Inc	Read head device with selected output jack characteristics
US8950676B2	2010-08-20	2015-02-10	Symbol Technologies, Inc.	Image capture based on working distance range restriction in imaging reader
US9576159B1	2011-01-24	2017-02-21	Square, Inc.	Multiple payment card reader system

GB2499431A *	2012-02-16	2013-08-21	Mobipaypoint Uk Ltd	Hybrid payment terminal with viewing window for CVV code
US9741045B1	2012-09-16	2017-08-22	Square, Inc.	Ranking of merchants for cardless payment transactions
US8925815B2	2012-09-05	2015-01-06	Symbol Technologies, Inc.	Checkout system for and method of preventing a customer-operated accessory reader facing a bagging area from imaging targets on products passed through a clerk-operated workstation to the bagging area
US9652791B1	2013-02-08	2017-05-16	Square, Inc.	Updating merchant location for cardless payment transactions
US9940616B1	2013-03-14	2018-04-10	Square, Inc.	Verifying proximity during payment transactions
US9922322B2	2013-07-23	2018-03-20	Square, Inc.	Computing distances of devices
US8910868B1	2013-11-27	2014-12-16	Square, Inc.	Firmware management
US8967465B1	2013-11-27	2015-03-03	Square, Inc.	Audio signaling training for bidirectional communications
US8931699B1	2013-12-11	2015-01-13	Square, Inc.	Bidirectional audio communication in reader devices
US9633286B1	2013-12-11	2017-04-25	Square, Inc.	Power harvesting in reader devices
US10198731B1	2014-02-18	2019-02-05	Square, Inc	Performing actions based on the location of mobile device during a card swipe
US9256769B1	2014-02-25	2016-02-09	Square, Inc.	Mobile reader device
US9569767B1	2014-05-06	2017-02-14	Square, Inc.	Fraud protection based on presence indication
US10026083B1	2014-05-11	2018-07-17	Square, Inc.	Tab for a venue
US10304043B1	2014-05-21	2019-05-28	Square, Inc.	Multi-peripheral host device
USD762651S1	2014-06-06	2016-08-02	Square, Inc.	Mobile device case
US9760740B1	2014-06-23	2017-09-12	Square, Inc.	Terminal case with integrated dual reader stack
US9256770B1	2014-07-02	2016-02-09	Square, Inc.	Terminal case with integrated reader and shortened base
US9799025B2	2014-08-19	2017-10-24	Square, Inc	Energy harvesting bidirectional audio interface
US9355285B1	2015-02-12	2016-05-31	Square, Inc.	Tone-based wake up circuit for card reader
US9436933B1	2015-05-13	2016-09-06	Square, Inc.	Transaction payment processing by multiple data centers
US10628811B2	2016-03-15	2020-04-21	Square, Inc.	System-based detection of card sharing and fraud
US10410200B2	2016-03-15	2019-09-10	Square, Inc.	Cloud-based generation of receipts using transaction information
US10636019B1	2016-03-31	2020-04-28	Square, Inc.	Interactive gratuity platform
US10402807B1	2017-02-28	2019-09-03	Square, Inc.	Estimating interchange fees for card payments
US10410021B1	2017-12-08	2019-09-10	Square, Inc.	Transaction object reader with digital signal input/output and internal audio-based communication
US11087301B1	2017-12-19	2021-08-10	Square, Inc.	Tamper resistant device
USD905689S1	2018-07-25	2020-12-15	Square, Inc.	Card reader device

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
AU5079498A	1998-05-15	Transaction terminal for electronic purse transactions and the like
AU741873C	2004-07-08	Electronic transaction
AU3830697A	1998-03-26	Electronic money transaction system
AU682923B2	1997-10-23	Electronic toll payment
AU3830899A	1999-12-13	Terminal and system for implementing secure electronic transactions
AU4588197A	1998-04-24	Payment and transactions in electronic commerce system
AU694694B2	1998-07-23	Electronic purse application system and method thereof
AU729618C	2001-08-23	Shipment transaction system and an arrangement thereof

IPR2025-00645 Page 01631

AU8675398A	1999-02-22	Method and system for conducting electronic commerce transactions
AU9351498A	1999-04-12	Electronic payment system
AU2013797A	1997-11-13	Creating and using an adaptable multiple-contract transaction object
GB9615999D0	1996-09-11	Electronic purse loan system
EP0933731A4	2002-01-09	Electronic transaction system
AU8482698A	1999-02-10	Integrated electronic commerce system and method
AU3765900A	2000-10-04	Systems for financial and electronic commerce
AU3069995A	1996-04-04	Intelligent card useful in telephony and the like
AU3953597A	1998-04-17	Transaction card
AU3264795A	1996-06-19	Electronic money recovering system
AU2867797A	1998-01-29	Electronic purse
AU4216597A	1998-04-17	Improvements relating to electronic transactions
EP0778691A3	1998-03-18	Telephone used for electronic money card transaction and method of operation of the same
GB2319381B	2000-08-30	Transaction processing
AU6642196A	1997-03-05	Secure credit card
AU6512494A	1994-10-11	Electronic terminal for the transfer and receipt of money
AU3806099A	1999-12-06	Financial transaction terminal with limited access

Priority And Related Applications

Priority Applications (3)

Application	Priority date	Filing date	Title
US2896296P	1996-10-18	1996-10-18	*US Provisional Application*
US60028962		1996-10-18	
PCT/US1997/017550	1996-10-18	1997-10-17	Transaction terminal for electronic purse transactions and the like

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents DE19928733

Semiconductor memory chip module

Abstract

The invention relates to a semiconductor memory chip module (2') for a chip card, in which a non-volatile memory chip (EEPROM) (4) and a volatile memory chip (SRAM) (6) are stacked on top of each other and directly coupled with each other by vertical intermediate chip connections (16). The volatile memory with quick access enables programmes to be processed rapidly. Data can be stored permanently and securely through transfer to the non-volatile memory. A chip (8) with decoding circuits can be contained at a further level. A buffer capacitor (20) is also incorporated in a chip and is recharged to a constant supply voltage during operation.

Classifications

H01L23/50 Arrangements for conducting electric current to or from the solid state body in operation, e.g. leads, terminal arrangements ; Selection of materials therefor for integrated circuit devices, e.g. power bus, number of leads

View 5 more classifications

DE19928733A1

Summary

Find Prior Art Similar

Other languages: German

Inventor: Thomas Grasl

Current Assignee : Giesecke and Devrient GmbH

Worldwide applications

1999 DE 2000 ~~6E JP ES AT WO AU BR US EP CA KR CN~~

Application DE19928733A events

1999-06-23 Application filed by Giesecke and Devrient GmbH

1999-06-23 Priority to DE19928733A

2001-01-04 Publication of DE19928733A1

Status Withdrawn

Info: Patent citations (19), Non-patent citations (2), Cited by (16) , Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, DPMA, Discuss

Claims (9)

Hide Dependent

1. A semiconductor memory chip module, having a first memory chip (**4**) of a first type, a second memory chip (**6**) of a second type, and an electrical connection (**14** , **16**) between the first and the second memory chip (**4** , **6**), **thereby characterized** in that the memory chips (**4** , **6**) are arranged one above the other in different levels and are connected via vertical intermediate chip connections (**24** , **26**).

2. Chip module according to claim 1, characterized in that memory cells (C4) of the first memory chip (**4**) are assigned to certain memory cells (C6) of the second memory chip (**6**), and the mutually assigned memory cells (C4, C6) directly to one another are electrically connected.

3. Chip module according to claim 1 or 2, characterized in that the first type a non-volatile memory, for example EEPROM, and the second type corresponds to a volatile memory, for example SRAM.

4. Chip module according to one of claims 1 to 3, characterized in that at least one further chip (**8** , **16**) is provided in a further level.

5. Chip module according to claim 4, characterized in that the further chip contains decoder circuits (**10** , **12**) for the memory chips (**4** , **6**).

6. Chip module according to one of claims 1 to 5, characterized in that that an energy buffer is formed in at least one of the levels.

7. Chip module according to claim 6, characterized in that the energy buffer is designed as an integrated buffer capacitor (**20**).

8. Chip module according to one of claims 2 to 7, designed for a chip map.

9. Chip card with a semiconductor memory chip module according to one of the An sayings 1 to 8.

Description

The invention relates to a semiconductor memory chip module with a plurality of memory cherchips of different types, especially with several in below different manufacturing technology implemented memory chips. In particular re the invention relates to a semiconductor memory suitable for chip cards Chip module and a chip card equipped with such a chip module.

One can depend on the currently available semiconductor memories Manufacturing technology, its operating parameters, its capacity, etc. ver assign different types. One can un semiconductor memory for example differentiate between volatile and non-volatile memories.

Expediently in chip cards and in chip card terminals Non-volatile memory is used, but its content is also deleted and can be overwritten. Semiconductor memories typically used EEPROMs are for this purpose.

Such EEPROMs, i.e. erasable, electrically programmable read-only memories, agree on the deletion and rewriting of data circuitry required and required compared to volatile memories, for example a DRAM or SRAM, relatively much Access time. If such a semiconductor memory is used when processing Software programs are used, so processing is slow the program possible. In addition, with an EEPROM only one limited number of erases and writes is possible, more typical in the order of 10,000 to 100,000.

If one is on the presence of a non-volatile memory, play an EEPROM, instructed, and still want a memory with quick access for program execution So you can think of one in addition to the EEPROM, for example To provide SRAM as volatile memory, with the help of which the Pro grams are processed. If you want to run a program save the results for a long time, so you can reload the Make the required data in the EEPROM.

The different types of semiconductor memory, that is to say in the present case Case of non-volatile memory (EEPROM) and fast volatile memory (SRAM) are based on different manufacturing technologies. Used you put two such different types of semiconductor memory side by side, so considerable effort is required to make the two memories function to connect efficiently. Between the two stores are right relatively long cable routes required. This requires a relatively large one Share of the available chip area.

The invention has for its object to provide a semiconductor memory Specify chip module, which has the advantages of two types of memory chips without the disadvantages mentioned, that means high production costs and long lines, can be reached.

According to the invention, this object is achieved in a semiconductor memory Chip module with different types of memory chips in that the Memory chips are arranged in different levels one above the other and are connected via vertical interconnections. In one particularly preferred embodiment there is a fixed allocation of memory cells of the first memory chip to memory cells of the second memory chip, the memory cells assigned to one another directly via the vertical connections are connected.

In a particularly preferred embodiment, the first type of memory chip around a non-volatile memory, in particular their EEPROM, in the second type a volatile memory, for play an SRAM.

The invention allows the production of a semiconductor memory Chip module with different types of memory chips, in particular memory chips manufactured according to various manufacturing technologies. The According to the invention, chips can be produced separately - with the aid of typical manufacturing processes for them. The finished chips each need only relatively little chip area in itself. The finished chips are then over stacked together, the connections between the chips vertical Connections take up very little additional chip area to take. The chip stack is then formed as a closed unit, in particular encapsulated in a module so that it is in a chip card can be built.

In the simplest embodiment of the invention, two chips levels should be provided. Since every semiconductor memory except the actual Chen memory cells still has a control circuit, here as a decoder called, you can ge these decoders with the respective semiconductor chip train together. In a particularly advantageous embodiment of the Er However, the invention provides for a further chip in a further level with decoder circuits for all memory chips of the chip module see is. The chip allocation area is - in the horizontal direction - not enlarged by the decoder circuits in the further chip. Also the chip with the decoder circuits is Inter-chip connections to the memory chip of the first or the second Type connected, depending on which chip is directly under the chip with the decoder circuits.

A peculiarity when using memory chips in connection with chip cards and chip card terminals is the defense against so-called Power analysis attacks. Such attacks will be fraudulent Intent tries to use current and voltage sensors status of a circuit to be able to draw conclusions about ge to be able to pull protected data. Is used on all connections for Voltage and current levels are taken care of, regardless of internal scarf states always one or one of several defined levels such an attack is not possible.

One can with the help of a constantly recharged capacitor, a so-called called buffer capacitor, the supply voltage for the chip so far smooth that no level changes are noticeable to the outside, the back could allow conclusions about circuit states.

In a preferred embodiment of the invention it is provided that in at least one of the levels of the chip module is an energy buffer, in particular which is designed in the form of an integrated capacitor. This buffer capacitor can occupy an entire chip level, preferably more layered training, however, it can only be on a partial chip area be restricted so that the rest of this level then for memory cells, De encoder circuits or logic circuits are available. That puf Fer capacitor can then be used at the end of processing of a program carried out with the help of the volatile memory which He Results of the program and other data in the non-volatile memory save. For example, by causing external interference Called program termination can be used to restart the program required data using the buffer capacitor in the not volatile memory can be saved permanently.

In the following, exemplary embodiments of the invention are described with reference to the Drawing explained in more detail. Show it:

Fig. 1 is a schematic vertical sectional view through a Halbleiterspei cher-chip module according to a first embodiment of the invention; and

Fig. 2 is a view similar to **Fig.** 1 of a second embodiment of the invention.

Fig. 1 shows a semiconductor memory chip module **2** according to a first embodiment of the invention. The chip module **2** contains three stacked chips, namely a lower chip **4** , here designed as EEPROM, i.e. as a non-volatile memory chip, a middle chip **6** , here designed as SRAM, i.e. as a volatile memory chip, and an upper chip **8** , which two Types of decoder circuits **10** and **12** included.

In the memory chip **4** a predetermined number of memory cell C4 is formed, contains alignment with these in the vertical direction of the memory chip **6** a corresponding number of nonvolatile memory cells C6.

The memory cells C4 and C6 in the memory chips **4** and **6** are aligned vertically, as indicated by vertical lines in **FIG.** 1. There is a direct electrical connection between the respective vertically assigned memory cells C4 and C6 through so-called vertical interchip connections, which are explained in more detail below for the exemplary embodiment shown in **FIG.** 2.

The decoder circuits **10** and **12** contained in the upper level in the upper chip **8** enable different addressing options for the memory chips **4** and **6** . In the present embodiment, the decoder circuits **10** (only one is shown in **FIG.** 1) serve to drive the memory cells C4 in the lower memory chip **4** , the decoder circuits **12** serve to drive the memory cells C6 in the middle memory chip **6** . In a modified embodiment, however, the decoder circuits **10** and **12** can also be used for both memory chips **4** and **6** , respectively.

FIG. 2 shows a second embodiment of a semiconductor memory chip module **2** ', which is structured based on the chip module shown in **FIG.** 1.

As in the first embodiment, a lower memory chip **4 is designed** as an EEPROM, and above it is a memory chip **6 designed** as SRAM in the next level. The memory cells C4 and C6, which are vertically aligned with one another, are directly electrically connected via vertical interchip connections **16** .

The memory chip **6 is** connected to the chip **8** via similar vertical intermediate chip connections, said lines not shown in detail and additionally containing a buffer capacitor **20** . The Pufferkon capacitor **20** is also connected via direct vertical inter-chip connections **22** s with the underlying memory chip **6** and via interchip

IPR2025-00645 Page 01634

connections 22 b with an overlying further chip 16 , it is also via an indicated at 24 connection with those contained in the chip 8 Decoder circuits connected. Through connections, not shown, the buffer capacitor 20 is also connected to the lower memory chip 4 .

In the semiconductor memory chip module 2 'of the embodiment shown in FIG. 2, in addition to the buffer capacitor 20 , which functions as an energy buffer, the top level of the chip 16 , which contains logic circuits, for example, is present for all of the other chips 4 , 6 and 8 is available.

In the embodiment according to FIG. 2, the buffer capacitor 20 is made up of a plurality of alternating electrically conductive or dielectric layers. From a feed line, not shown, the buffer capacitor 20 is constantly kept at a supply voltage level. Its Ka capacity is dimensioned such that it, in the case for example of a Betriebsab the chip module 2 'writing of data from the SRAM of the memory chip 6 in corresponding memory cells of the EEPROM of the Spe ! fraction cherchips 4 allowed.

The invention and the embodiment shown in FIGS . 1 and 2 form a chip module are particularly suitable for installation in a chip card or a chip card terminal, although the invention is not limited to this. As a further modification of the invention, the order of the memory chips can be changed; in FIG. 1, for example, the various chips 4 , 6 and 8 can be exchanged in their order. The same applies to the arrangement according to FIG. 2. The buffer capacitor 20 can also extend over an entire chip level. The decoder circuits, shown in Fig. 1 in the upper chip 8 at 18 and 12 , NEN can also be distributed to different chip levels.

The embodiments of semiconductor memory chip modules shown in FIGS . 1 and 2 contain the chips 4 , 6 , 8 and 16 manufactured in separate manufacturing processes. The separately manufactured chips are stacked on top of one another and bonded together vertically by bonding. The entire arrangement thus obtained is encapsulated and is then available for installation in a chip card, for example. The encapsulation, including the connection connections led to the outside, is not explained in detail here because it is conventional.

Incorporated in a smart card, the semiconductor memory chip module operates accelerator as Fig. 1 or FIG. 2 is then such that the permanently stored data be located in the bottom chip 4, that is in the non-volatile memory EEPROM. When programs are executed, the required data is reloaded into the middle chip, that is, the volatile memory (SRAM). The middle chip 6 then acts like a cache memory. Result data and data to be backed up, for example in the event of an interruption of operation, are then reloaded from the central memory chip 6 into the lower memory chip 4 , for which purpose the energy stored in the buffer capacitor is used.

Patent Citations (19)

Publication number	Priority date	Publication date	Assignee	Title
DE4219031A1 *	1992-06-10	1993-12-16	Siemens Ag	Multi-chip module
DE19511775C1 *	1995-03-30	1996-10-17	Siemens Ag	Carrier module, especially for installation in a card-shaped data carrier, with protection against the examination of secret components
Family To Family Citations				
US4908502A *	1988-02-08	1990-03-13	Pitney Bowes Inc.	Fault tolerant smart card
JPH0254558A	1988-06-24	1990-01-10	Hitachi Ltd	Semiconductor device for chip-on-chip
JP2760062B2 *	1989-06-23	1998-05-28	自動車機器株式会社	Hydraulic booster
JP2591324B2 *	1990-10-29	1997-03-19	日本電気株式会社	Semiconductor memory integrated circuit
US5229647A *	1991-03-27	1993-07-20	Micron Technology, Inc.	High density data storage using stacked wafers
JP2622038B2 *	1991-06-03	1997-06-18	シャープ株式会社	Semiconductor device and manufacturing method thereof
JPH0548000A *	1991-08-13	1993-02-26	Fujitsu Ltd	Semiconductor device
US5422435A *	1992-05-22	1995-06-06	National Semiconductor Corporation	Stacked multi-chip modules and method of manufacturing
JP2605968B2	1993-04-06	1997-04-30	日本電気株式会社	Semiconductor integrated circuit and method of forming the same
WO1994024704A1 *	1993-04-12	1994-10-27	Bolger Justin C	Area bonding conductive adhesive preforms
US5514907A *	1995-03-21	1996-05-07	Simple Technology Incorporated	Apparatus for stacking semiconductor chips
EP0811204B1	1995-07-05	1999-09-22	International Business Machines Corporation	Processing of long messages in a chip card
US5973396A *	1996-02-16	1999-10-26	Micron Technology, Inc.	Surface mount IC using silicon vias in an area array format or same size as die array
JP4011695B2 *	1996-12-02	2007-11-21	株式会社東芝	Chip for multi-chip semiconductor device and method for forming the same
US6037661A *	1996-12-20	2000-03-14	International Business Machines	Multichip module
US5915167A *	1997-04-04	1999-06-22	Elm Technology Corporation	Three dimensional structure memory
KR100328062B1 *	1997-12-13	2002-06-29	이구택	Refining process extra low carbon steel

* Cited by examiner, † Cited by third party

Non-Patent Citations (2)

Title
JP 06291250 A-in: Patents Abstracts of Japan (1994) *
JP 2-5455 A-in: Patents Abstracts of Japan (1990) *

* Cited by examiner, † Cited by third party

Cited By (16)

Publication number	Priority date	Publication date	Assignee	Title
DE10139414A1 *	2001-08-17	2003-02-27	Giesecke & Devrient Gmbh	Semiconductor circuit arrangement with biometric sensor and evaluation unit
DE10317147A1 *	2003-04-14	2004-10-28	Nec Electronics (Europe) Gmbh	Secure storage system with flash memories and cache memory
Family To Family Citations				
KR100528464B1 *	2003-02-06	2005-11-15	삼성전자주식회사	Security system of smart card
KR100689589B1 *	2004-12-30	2007-03-02	매그나칩 반도체 유한회사	Semiconductor device and method for manufacturing the same
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7557597B2 *	2005-06-03	2009-07-07	International Business Machines Corporation	Stacked chip security
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
CN103633048B *	2012-08-22	2016-08-24	成都海存艾匹科技有限公司	Three-dimensional storage containing read/write voltage generator chip
TWI579856B	2014-09-12	2017-04-21	東芝股份有限公司	Semiconductor device
WO2019152877A1 *	2018-02-04	2019-08-08	Hsu Fu Chang	Methods and apparatus for memory cells that combine static ram and non-volatile memory

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
DE19928733A1	2001-01-04	Semiconductor memory chip module
DE69433320T2	2004-09-16	REMOTE CONTROLLED REPROGRAMMABLE PROGRAM MEMORY FOR A MICRO CONTROLLER
DE19880311B3	2017-06-22	Non-volatile memory structure
DE102963311B4	2008-07-24	A storage system for storing data and methods for providing performance within a storage system
DE4417289B4	2007-01-04	Performance-independent, static memory
DE60206624T3	2009-07-16	SEGMENTATION OF THE BIT AND CONTROL BOARD IN A NON-VOLATILE MEMORY
DE3712178C2	1992-08-27	
DE2220721A1	1972-11-09	Data card
DE102007005713B4	2012-02-09	Circuit arrangement with buried control lines
EP1103051B1	2003-04-23	Ferroelectric storage assembly

DE3626803A1	1987-02-26	SEMICONDUCTOR MEMORY DEVICE WITH A REDUNDANCY CIRCUIT
DE2557006B2	1977-02-17	DECODING CIRCUIT FOR SEMICONDUCTOR MEMORY
DE102004044413A1	2006-03-16	Semiconductor memory device
DE60028111T2	2006-09-28	Ferroelectric storage
DE102006010804A1	2007-11-29	Memory module and method for testing a semiconductor chip
WO1996010804A1	1996-04-11	Data carrier arrangement
DE69635842T2	2006-11-30	STORAGE REDUNDANCY SWITCHING USING INDIVIDUAL POLYSILICIDE FLOAT GATE TRANSISTORS AS REDUNDANT ELEMENTS
DE3327874A1	1984-02-09	MEMORY MODULE FOR A PROGRAMMABLE ELECTRONIC DEVICE
DE4135032A1	1992-04-30	EEPROM with memory cells comtg. MOS with charge layer and control gate - has transistor with drain breakdown voltage adjuster for specified operational range
DE60113833T2	2006-11-23	Semiconductor memory with a subdivided wordline structure
WO1998012747A1	1998-03-26	Integrated circuit with housing accommodating the latter
DE2629893A1	1977-01-20	CELL ADDRESSABLE MATRIX
DE102996858T5	2004-08-26	Semiconductor device or semiconductor component and manufacturing method therefor
DE19526012C2	1997-09-11	Electrically erasable and programmable non-volatile memory cell
DE19752695A1	1999-06-02	Electronic switching element for blocking electronic parts in a chip card

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
DE19928733A	1999-06-23	1999-06-23	Semiconductor memory chip module

Applications Claiming Priority (13)

Application	Filing date	Title
DE19928733A	1999-06-23	Semiconductor memory chip module
US09/926,791	2000-06-19	Semiconductor memory chip module
PCT/EP2000/005625	2000-06-19	Semiconductor memory chip module
JP2001506553A	2000-06-19	Semiconductor memory chip module
BR0011868-0A	2000-06-19	Semiconductor memory chip module
EP00942097A	2000-06-19	Semiconductor memory chip module
KR1020017016453A	2000-06-19	Semiconductor Memory Chip Module
AU56835/00A	2000-06-19	Semiconductor memory chip module
DE50001991T	2000-06-19	SEMICONDUCTOR MEMORY CHIP MODULE
ES00942097T	2000-06-19	SEMICONDUCTOR MEMORY CHIP
CNB008094365A	2000-06-19	Semiconductor memory chip module
AT00942097T	2000-06-19	SEMICONDUCTOR MEMORY CHIP MODULE
CA002377175A	2000-06-19	Semiconductor memory chip module

Legal Events

Date	Code	Title	Description
2001-01-04	OP8	Request for examination as to paragraph 44 patent law	
2004-09-02	8130	Withdrawal	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents 2003081519

Portable electronic authorization system and method

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.

Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 11 more classifications

WO2003081519A2

WIPO (PCT)

Download PDF Find Prior Art Similar

Other languages: French

Inventor: Joseph A. Thomas, Karlin B. Jessen, Todd O. Burger, Joshua L. Hassol

Worldwide applications

2003 WO CA EP 2009 US

Application PCT/US2003/008638 events

2002-03-19 Priority to US36609302P

2002-03-19 Priority to US360/366,093

2002-05-13 Priority to US37996402P

2002-05-13 Priority to US60/379,964

2003-03-19 Application filed by Chameleon Network Inc.

2003-10-02 Publication of WO2003081519A2

2004-01-22 Publication of WO2003081519A3

Info: Patent citations (88), Non-patent citations (1), Cited by (26), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, PatentScope, Discuss

Claims

Hide Dependent

1. An apparatus, comprising: a user authenticator that authenticates an identity of a user; and a transponder that 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.

2. The apparatus of claim 1, wherein the wireless signal representing the information and the wireless interrogation signal are radio frequency signals.

3. The apparatus of claim 1 or 2, wherein the apparatus further comprises a memory that stores at least first and second distinct codes, and a user input that permits the user to select any one of the at least first and second codes for transmission in response to an interrogation signal; and wherein the transponder is permitted to emit a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

4. The apparatus of claim 3, further comprising a display that identifies the one of the at least first and second codes the user has selected.

5. The apparatus of claim 3 or 4, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

6. The apparatus of any one of claims 1-5, in combination with an interrogator that wirelessly emits the interrogation signal, and receives from the apparatus the wireless signal representing the information.

7. An apparatus, comprising: a memory that stores at least first and second distinct codes; a user input that permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal; and a transponder that emits a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

8. The apparatus of claim 7, wherein the wireless signal representing the identification information and the wireless interrogation signal are radio frequency signals.

9. The apparatus of claim 7 or 8, further comprising a display that identifies the one of the at least first and second codes the user has selected.

10. The apparatus of any one of claims 7-9, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

11. The apparatus of any one of claims 7-10, in combination with an interrogator that wirelessly emits the interrogation signal, and receives from the apparatus the wireless signal representing the selected one of the at least first and second codes.

12. A token that may be used to engage in a transaction at a point of sale, comprising: a substrate; a rewriteable memory, supported by the substrate, that 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 being

IPR2025-00645 Page 01639

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; and a reconfigurable display, supported by the substrate, that displays at least some of the information that is stored in the rewritable memory.

13. The token of claim 12, wherein rewritable memory stores both an account identifier and a security code separate from the account identifier, and the reconfigurable display displays both the account identifier and the security code.

14. The token of claim 12 or 13, wherein the substrate is substantially the size of a credit card.

15. The token of any one of claims 12-14, wherein the rewritable memory comprises means for selectively storing information on the token that identifies an account that is to be used to engage in the transaction at the point of sale.

16. The token of any one of claims 12-15, wherein the rewritable memory comprises a rewriteable magnetic stripe.

17. The token of any one of claims 12-15, wherein the rewritable memory comprises a circuit that simulates a magnetic stripe.

18. The token of any one of claims 12-15, wherein the rewritable memory comprises a circuit that simulates an account number storage mechanism of a Smartcard.

19. The token of any one of claims 12-18, wherein the reconfigurable display comprises a liquid crystal display (LCD).

20. The token of claim 19, wherein the LCD is flexible.

21. The token of any one of claims 12-29, in combination with an apparatus to which the token is releasably attached, the apparatus being configured to cause the rewritable memory of the token to store the information and to cause the display of the token to display at least some of the information after the token is detached from the apparatus.

22. The combination of claim 21 , wherein the rewritable memory comprises means for selectively storing information on the token that identifies an account that is to be used to engage in the transaction at the point of sale.

23. The combination of claim 21 or 22, wherein the apparatus to which the token is releasably attached comprises a memory that stores at least first information identifying a first account and second information identifying a second account, and a user input that permits the user to select one of the first information and second information for use in the transaction, and wherein the apparatus is further configured to cause the rewritable memory of the token to store the selected one of the first information and second information and to cause the display of the token to display at least some of the selected one of the first information and second information.

24. The combination of claim 23, further comprising a display that identifies the one of the first information and second information the user has selected.

25. The combination of claim 23 or 24, wherein the first information and second information correspond to accounts the user holds with respective first and second unrelated media issuers.

26. A method for using an apparatus, comprising 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.

27. The method of claim 26, wherein the wireless signal representing the information and the wireless interrogation signal are radio frequency signals.

28. The method of claim 26 or 27, wherein the method further 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 the transponder to emit a wireless signal representing the selected one of the first and second codes in response to the interrogation signal. - in -

29 The method of claim 28, wherein the method further comprises steps of: manipulating the user input on the apparatus to select the other of the first and second codes stored in memory; and permitting the transponder to emit a wireless signal representing the other of the first and second codes in response to the interrogation signal.

30 The method of claim 28 or 29, further comprising a step of: in response to the user manipulating the user input, displaying to the user an identification of the one of the first and second codes the user has selected.

31. The method of any one of claims 28-30, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

32 The method of any one of claims 26-31 , further comprising steps of: wirelessly emitting an interrogation signal from an interrogator; receiving the interrogation signal at the transponder; in response to receiving the interrogation signal, emitting from the transponder a wireless signal representing the information; and receiving at the interrogator the wireless signal representing the information.

33. The method of claim 32, further comprising a step of authorizing a transaction based upon the information received at the interrogator.

34. A method for using an apparatus, comprising 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.

35. The method of claim 34, wherein the wireless signal representing the selected one of the at least first and second codes and the wireless interrogation signal are radio frequency signals.

36. The method of claim 34 or 35, wherein the method further comprises steps of: manipulating the user input on the apparatus to select another of the at least first and second codes stored in memory; and permitting the transponder to emit a wireless signal representing the other of the at least first and second codes in response to the wireless interrogation signal.

37. The method of any one of claims 34-36, further comprising a step of: in response to the user manipulating the user input, displaying to the user an identification of the one of the at least first and second codes the user has selected.

38. The method of any one of claims 34-37, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

39. The method of any one of claims 34-38, further comprising steps of: wirelessly emitting an interrogation signal from an interrogator; receiving the interrogation signal at the transponder; in response to receiving the interrogation signal, emitting from the transponder a wireless signal representing the selected one of the at least first and second codes; and receiving at the interrogator the wireless signal representing the selected one of the at least first and second codes.

40. The method of claim 39, further comprising a step of authorizing a transaction based upon the selected one of the at least first and second codes received at the interrogator.

41. A method for configuring a token to be used to engage in a transaction at a point of sale, comprising steps 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 being 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; and configuring a display on the token to display at least some of the information that is stored in the rewritable memory.

42. The method of claim 41 , wherein the step of configuring the rewritable memory includes a step of configuring the rewritable memory to store both an account identifier and a security code separate from the account identifier, and the step of configuring the display includes configuring the display to display both the account identifier and the security code.

43. The method of claim 41 or 42, wherein the token is substantially the size of a credit card.

44. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes using a magnetic head to configure a rewriteable magnetic stripe on the token.

45. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes configuring the rewritable memory to cause a simulated magnetic stripe to be generated on the token.

46. The method of any one of claims 41 -43, wherein the step of configuring the rewritable memory includes configuring the rewritable memory to simulate an account number storage mechanism of a Smartcard.

47. The method of any one of claims 41 -46, wherein: the method further comprises a step of manipulating a user input to select one of at least first information identifying a first account and second information identifying a second account; the step of configuring the rewritable memory includes configuring the rewritable memory to store the selected one of the at least first information and second information, and the step of configuring the display includes configuring the display to display at least some of the selected one of the at least first information and second information.

48. The method of claim 47, further comprising a step of displaying to the user an identification of the one of the at least first information and second information the user has selected.

49. The method of claim 47 or 48, wherein the first information and second information correspond to accounts the user holds with respective first and second unrelated media issuers.

50. The method of any one of claims 41-49, further comprising steps of: interfacing the token with an apparatus at the point of sale to permit the apparatus to read the contents of the memory, displaying the information read from the memory on a display of the apparatus; and comparing the information displayed on the display of the token with the information displayed on the display of the apparatus to verify the authenticity of the token.

Description

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. 60/167,059, 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

IPR2025-00645 Page 01641

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

IPR2025-00645 Page 01642

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.

IPR2025-00645 Page 01643

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

IPR2025-00645 Page 01644

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.

IPR2025-00645 Page 01645

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 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.

Moreover, as is also discussed in more detail below, the Pocket Vault 102 may be configured or programmed to function as an RFID tag that can be used only by an authorized user of the Pocket Vault 102. For example, in response to an interrogation signal from the RFID interrogator 116 (e.g., an interrogator of an automated toll booth), the Pocket Vault 102 (if authorized) can return an appropriate RF signal to authorize payment of the required fee for the toll. In some embodiments, the RFID functionality of the Pocket Vault 102 can be altered by the user so that user is permitted to select the personality of the RFID tag that is embodied by the device. The user may, for example, first use the Pocket Vault 102 as an RFID tag to authorize payment of a toll, and later use the same Pocket Vault 102 as an RFID tag to authorize payment at a service 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, a particular RFID personality, 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

IPR2025-00645 Page 01646

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 2602 may further be sealed in a manner suitable to prevent tampering, for example, using a plastic potting compound, and may even be designed such that any attempt to invade the housing 2602 will damage the Pocket Vault 102 such that it may no longer be used. 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, KevlarTM, GortexTM, 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 include one or more antennas and may be any type of transceiver (or separate transmitter and receiver) capable of communicating with 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. Multiple transceivers (or transmitter/receiver pairs) of the same type may also be employed, if desired.

As discussed in more detail below in connection with Figs. 41 and 42, the transceiver 204 may, for example, serve as the transmitter and receiver of an RFID transponder used to respond to an interrogation signal from an interrogator 116. 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

IPR2025-00645 Page 01647

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, data for various RFID tags, 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 216 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

IPR2025-00645 Page 01648

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

IPR2025-00645 Page 01649

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.

In addition to or in lieu of the virtual magnetic stripe 610 and/or Smartcard components described herein, the token 102 may have disposed on it a conventional magnetic stripe that can be selectively written to by a magnetic read/write head in the Pocket Vault 102 before the token 102a is released from the token port 218. Like the other embodiments described above, the programming and/or use of such a token 102a could be restricted until after the identity of the Pocket Vault holder has been verified via biometric authentication, PIN code entry, or otherwise.

Moreover, in some embodiments, the token 102a may also have disposed on it a flexible LCD 612 or other suitable display mechanism or device. Prior to ejection of the token 102a from the token port 218, the Pocket Vault 102 may transfer information to the token 102a (e.g., via terminals 606) for display on the LCD 612. This transfer may either be direct or indirect (e.g., via a separate integrated circuit on the token 102a), and may involve the transfer of alphanumeric information (which may or may not include a hash code) and/or graphics, such as icons or barcodes. This information transferred may be encrypted, and de-encryption may be employed either in the separate integrated circuit on the token 102a or in a processor packaged with the LCD 612. In any event, the LCD 612 may receive the proper data to display, which would match all or part of the code stored on the card by means of the virtual magnetic stripe 610, a writeable magnetic stripe, Smartcard simulation circuitry, etc.

In some embodiments, the LCD 612 may be powered by a capacitor configured and arranged to drain after a preset time, thereby rendering the LCD 612 inoperable until programmed again by the Pocket Vault 102. Thus, even if the token 102a were still swipeable or otherwise useable, a merchant could opt not to accept it because the requisite authorization information would not longer be displayed for certification purposes.

Instead of or in addition to an LCD or other type of display, some suitable technology may be employed to cause account information, and perhaps other information that is typically embossed or printed on credit cards or Smartcards, to appear temporarily on the token 102a after the token 102a is ejected from the token port 218. One technology that may be appropriate for this purpose is available from E-ink (www.Eink.com). Thus, when an LCD display, a temporary ink technology, or the like, is employed on the token 102a, not only may the token 102a be selectively configured to have an actual or simulated magnetic stripe (or Smartcard personality) like a typical credit card or Smartcard, but it also may be configured to display information that is typically embossed or printed on such cards, including security enhancing information. When used by a consumer, retailers may verify authenticity by matching the information displayed on the token 102a with that revealed in the swipe or other token reading process. Without a match, the token 102a may be rejected.

As discussed above, in some embodiments of the Pocket Vault 102, the transceiver 204 (Fig. 2) may be used as the transmitter and receiver of an RFID transponder, and thereby function as an RFID tag. Such an RFID tag may be selectively configured to have one of several personalities and may be rendered operable only when the holder of the Pocket Vault 102 authenticates his or her identity (e.g., in response to an accurate fingerprint scan by fingerprint scanner 220).

To appreciate the manner in which the Pocket Vault 102 may achieve this functionality, a prior art RFID tag system (shown in Fig. 41) will be briefly described. An RFID system includes at least one "RFID tag" and at least one "interrogator." The interrogator communicates with the RFID tag via an RF signal at some suitable frequency, e.g., somewhere between 10 kilohertz and about 5 gigahertz. The distance between the RFID tag and the interrogator can be as short as near contact or as far as tens of feet away, depending upon the specific technology used. In most applications the RFID tag is a sealed device with no displays or user controls. The interrogator can be a hand held device that is manually operated or can be automated and included in a piece of stationary equipment, for example, at a parking garage, a toll booth, or a service station.

When the RFID tag comes within range of the interrogator, the two devices communicate in a session that may be a one-way read of the RFID tag information by the interrogator, or may be a two-way session in which the interrogator stores information in the RFID tag. The information stored in an RFID tag is typically an identification code such as a serial number. An RFID tag therefore functions much like a bar code, except that it is read by RF. To prevent counterfeiting, the information released from an RFID tag may be signed with a one-way cryptographic key so that it is difficult to decode or duplicate the code. There are four possible types of RFID tags: (1) active, read only RFID tags, (2) passive, read only RFID tags, (3) active, read/write RFID tags, and (4) passive, read/write RFID tags. Read only RFID tags have information that is stored in them at time of manufacture and can only be read (and not written to) by the interrogator. A Read/Write tag might include a mix of read only information but will have some memory in the tag that can be altered by the interrogator. A passive tag has no battery or other permanent energy source. An active tag, on the other hand, has a battery or is plugged into an external energy source.

An example of a prior art RFID tag 4100 is shown in Fig. 41. As shown, the RFID tag 4100 is a self-contained electronic device that includes a receiver 4102a and a transmitter 4102b that share an antenna 4104 and are connected to a micro-controller 4106. The micro-controller 4106 is further connected to either a read-only memory 4108a or a read/write memory 4108b. The RFID tag 4100 is powered by rectifying the RF energy supplied to the antenna 4104 by the interrogator (not shown).; If the RFID tag 4100 were of the "active" type, then an internal battery (not shown) would be employed. In operation, when the RFID tag 4100 receives an interrogation signal from an interrogator (not shown) via the antenna 4104 and receiver 4102a, the micro-controller 4106 retrieves the tag's serial number from the memory 4108 and passes it to the transmitter 4102b and antenna 4104 for RF transmission to the interrogator. When a read/write memory 4108b is employed, the micro-controller 4106 may also write information received from the interrogator to that memory.

In addition to typical electronic transponders such as that shown in Fig. 41, there also exist some RFID technologies that use non-electronic RFID tags. For example, interrogators can gather information from some types of RFID tags based solely on some physical property of the tags. For example, each RFID tag may employ several variable length antennas on a dielectric substrate, so that the interrogator can detect the length of the antennas present by sweeping through a range of frequencies. The

IPR2025-00645 Page 01650

specific pattern of antennas on the substrate thereby forms a unique code that can be recognized by the interrogator. Yet another approach is to use a surface acoustic wave (SAW) filter in which a surface electrode pattern determines a particular code that can be read by an interrogator.

Once programmed, the prior art RFID tag 4100 performs a single, dedicated function, namely, to release a serial number stored in memory 4108 in response to an interrogation signal, and there exists no control over who can use it for that purpose. In contrast, in some embodiments of the present invention, an RFID tag is provided wherein the personality of the tag, e.g., the code that is released upon interrogation, can be selected by the user from a number of possible personalities, and/or wherein the RFID tag can be rendered operational only by authorized users. An example embodiment of an RFID tag system 4200 configured in accordance with this aspect of the invention is shown in Fig. 42. As shown, the system 4200 may include an RFID tag 4202 that is identical to the prior art RFID tag 4100, except that memory 4108 of the prior art device has been bypassed or replace by an I/O connection 4204 to the Pocket Vault 102. In such an embodiment, the Pocket Vault 102, rather than the memory 4108, can supply the information to the micro-controller 4106 of the RFID tag 4202 that is to be released to the interrogator (via the transmitter 4102b and antenna 4104) in response to an interrogation signal from the interrogator.

Accordingly, in such an embodiment, the information that is to be released by the RFID tag 4202 in response to an interrogation signal may be controlled by the holder of Pocket Vault 102. The Pocket Vault's holder may therefore select the personality to be taken on by the RFID tag 4202, for example, by using the user input device 206 (Fig. 2) to scroll through various personalities for the RFID tag 4202 that are displayed on the display 216, much like the holder is able to select a desired personality that is to be taken on by the token 102a. The holder of the Pocket Vault 102 could therefore, for example, at one time select a "FastLane" personality for the RFID tag 4202, enabling the RFID tag to respond to an interrogator at a toll booth, and then at another time select a "Mobile Speedpass" personality, enabling the RFID tag to respond to an interrogator at a Mobile Service Station.

In some embodiments, at least some aspects of the RFID functionality of the Pocket Vault 102 may be exploited only after the identity of the Pocket Vault holder has been authenticated, e.g., using the fingerprint scanner 220 or by proper PEST code entry, thereby providing a level of security for RFID tags that has not heretofore been provided. The Pocket Vault 102 may, of course, permit some non-secure RFID personalities to be taken on by the RFID tag 4202 even without holder authentication.

In some embodiments, the data passed to the RFID tag 4202 can be made to be dependent not just on the recognition of a fingerprint, but based on an actual number tied to a feature extracted from the fingerprint. For example, the area of the finger may be such a feature. The number may then be used as a seed to a cryptographic code generator that creates the data to be sent to the RFID tag 4202.

In the embodiment shown in Fig. 42, the I/O connection 4204 between the Pocket Vault 102 and the RFID tag 4202 may be established in any of a number of ways and the invention is not limited to any particular mechanism or technique for establishing such a connection. In some embodiments, for example, the controller 202 of the Pocket Vault 102 may communicate with the micro-controller 4106 of the RFID tag 4202 via a cable connected between serial or parallel ports on the two devices. Alternatively, the two devices may be directly mated to one another in some suitable manner, or may communicate wirelessly if suitable security precautions are taken. The docking interface 208 of the Pocket Vault 102 may even provide a suitable mechanism for mating the two devices.

In some embodiments, the Pocket Vault 102 may have a separate memory (not shown in Fig. 2) dedicated to the storage of the RFID tag personality that is to be taken on by the RFID tag 4202, and the I/O connection 4204 may give the micro-controller 4106 of the RFID tag 4202 access to that memory. Alternatively, as mentioned above, the personality of the RFID tag 4202 may be communicated directly from the controller 202 of the Pocket Vault 102 to the micro-controller 4106 of the RFID tag 4202 via the I/O connection 4204. The functionality of the RFID tag 4202 may additionally or alternatively be built directly into the Pocket Vault 102 (Fig. 2), rather that existing as a separate item. In some embodiments, for example, the functionality of the transceiver 4102 and microcontroller 4106 of the RFID tag 4202 may be embodied by the transceiver 204 and the controller 202 of the Pocket Vault 102. Alternatively, the Pocket Vault 102 may include a separate micro-controller, transceiver and/or memory dedicated to the RFID functionality discussed above. In yet another alternative embodiment, the functionality of the RFID tag 4202 may be embodied on the token 102a or on different device that may be selectively released from the housing of the Pocket Vault 102. The token 102a or other releasable device may, for example, include a memory that stores a selected personality for an RFID tag for only a predetermined, finite period of time, and then goes blank.

In some embodiments, the Pocket Vault 102 may also control the content of RFID tags that do not use an electronic circuit. This control can be accomplished in a number of different ways, and the invention is not limited to the use of any particular technique. In one embodiment, for example, the Pocket Vault 102 may activate one or more switches to short out one or more antennas, thereby changing the RFID code represented by them. As with the other embodiments, this selective configuration of an RFID tag may at least in certain circumstances be permitted only after proper authentication of the Pocket Vault holder's identity.

It should be appreciated that the RFID functionality discussed above need not be combined with some or all of the other aspects of the Pocket Vault 102. For example, some embodiments of the invention may comprise simply an RFID tag for which one of several personalities can be selected by the user, and/or an RFID tag that is selectively enabled only following proper user authentication, e.g., using a fingerprint scanner or PIN code entry.

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

IPR2025-00645 Page 01651

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 VEREFY 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.

IPR2025-00645 Page 01652

After the steps 806a-810a, the routine proceeds to a step 804b, wherein the holder is prompted to apply a fingerprint from one fmger 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,

IPR2025-00645 Page 01653

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 26 J 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. 26 J, 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

IPR2025-00645 Page 01654

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. Alternatively, the selected wireless transaction may be an RFID transaction if an RFID personality has been selected from amongst the available media. If such an RFID transaction has been selected, an appropriate RFID code may be supplied to the controller responsible for broadcasting an RF signal containing that code in response to an interrogation signal. If that controller is on the Chameleon card, then these steps may alternatively be performed in connection with the PROCESS CARD TRANSACTION routine (step1036) discussed below.

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 using a magnetic read/write head to write to a conventional magnetic stripe on the token 102a, by causing the token 102a to generate a simulated magnetic stripe, by causing the token 102a to have a bar code disposed on it, and/or simply by causing a card number and perhaps security-related information to be visibly displayed it (e.g., using an LCD display or some type of printing technique). The token 102a may possibly be configured to hold such information for only a predetermined, finite period of time, so that it is not useable after such time. 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. 26b).

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,

IPR2025-00645 Page 01656

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

IPR2025-00645 Page 01657

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.

IPR2025-00645 Page 01658

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.

IPR2025-00645 Page 01659

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 1508, 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 1508, 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 1608, 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.

IPR2025-00645 Page 01660

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 1625, 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).

IPR2025-00645 Page 01661

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.

IPR2025-00645 Page 01662

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.

IPR2025-00645 Page 01663

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, barcode reader or RFID interrogator 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, an RF signal receiver, or an RFID interrogator 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, a barcode reader 107, or an RFID interrogator 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.

IPR2025-00645 Page 01664

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 RFID tag loading module 2805, 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.

The RFID tag loading module 2805 may, for example, be responsible for loading data for new RFID tags and storing such data in memory, as well as for transferring this data to the network server 114, when appropriate. Examples of how RFID tag data may be loaded onto the Pocket Vault 102 are discussed below in connection with Fig. 40.

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

IPR2025-00645 Page 01665

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).

IPR2025-00645 Page 01666

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

IPR2025-00645 Page 01667

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) RFID TAG LOADING routine 3315 - discussed below in connection with Fig. 40, (3) SYNCHRONIZATION (see SYNCHRONIZATION routine 3316 - discussed below in connection with Fig. 35), (4) RECOVERY (see RECOVERY routine 3318 - discussed below in connection with Fig. 36), (5) IDENTITY PORTING OPTIONS (see IDENTITY PORTING OPTIONS routine 3320 - discussed below in connection with Fig. 337), (6) BACKUP (see BACKUP routine 3322 - discussed below in connection with Fig. 38), (7) SET PREFERENCES (see SET PREFERENCES routine 3324 - discussed below in connection with Fig. 39), AND (8) 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 man er. 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.

IPR2025-00645 Page 01668

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

IPR2025-00645 Page 01669

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 3810, 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 3812, 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 Ppcket 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 presentinent, 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 3916, 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. Fig. 40 is a flow diagram illustrating an example implementation of the RFID

TAG LOADING routine 3315 shown in Fig. 33.

As shown, the routine 3315 begins at a step 4002, wherein the user may use the website on the network server 114 to create an account for the RFED tag to be loaded onto the Pocket Vault 102. After the step 4002, the routine proceeds to a step 4004, wherein the website on the network server 114 determines whether the account for the RFID tag is valid, for example, by checking with the media that issued the RFID tag account.

When, at the step 4004, it is determined that the account for the RFID tag is not valid, the routine 3315 proceeds to a step 4010, wherein appropriate security precautions are taken.

IPR2025-00645 Page 01670

After the step 4010, the routine 3315 terminates.

When, at the step 4004, a determination is made that the account for the RFID tag is valid, the routine 3315 proceeds to a step 4006, wherein the information for the RFID tag is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 4006, the routine 3315 proceeds to a step 4008, wherein a message is displayed that indicates the RFID tag information has been successfully loaded onto the Pocket Vault 102 for use in future transactions.

After the step 4008, the routine 3315 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:

Patent Citations (88)

Publication number	Priority date	Publication date	Assignee	Title
US5748737A *	1994-11-14	1998-05-05	Daggar; Robert N.	Multimedia electronic wallet with generic card
WO1999038117A1 *	1998-01-27	1999-07-29	Viztec Inc.	Transmitting advertisements to smart cards
WO2001024123A1 *	1999-09-28	2001-04-05	Chameleon Network Inc.	Portable electronic authorization system and associated method
WO2003029942A2 *	2001-10-01	2003-04-10	Chameleon Network, Inc.	Portable electronic authorization device and associated method
Family To Family Citations				
US4701601A *	1985-04-26	1987-10-20	Visa International Service Association	Transaction card with magnetic stripe emulator
US4791283A *	1986-06-03	1988-12-13	Intellicard International, Inc.	Transaction card magnetic stripe emulator
US4829492A *	1986-07-30	1989-05-09	Woodstream Corporation	Depthfinder with color LCD display
US4896791A *	1987-01-20	1990-01-30	The Savings Spot, Ltd.	Coupon dispensing system
US4868376A *	1987-05-15	1989-09-19	Smartcard International Inc.	Intelligent portable interactive personal data system
DE3906349C2 *	1989-03-01	1991-08-08	Hartmut 7000 Stuttgart De Hennige	
KR100191811B1 *	1989-10-24	1999-06-15	이브 오드뱅쿠	Portable electronic device to establish public loyalty to a medium or similar

IPR2025-00645 Page 01671

US5192854A *	1990-07-26	1993-03-09	Counts Reginald D	System for electronically recording and redeeming coupons
US5585787A *	1991-12-09	1996-12-17	Wallerstein; Robert S.	Programmable credit card
US5786582A *	1992-02-27	1998-07-28	Symbol Technologies, Inc.	Optical scanner for reading and decoding one- and two-dimensional symbologies at variable depths of field
US5395181A *	1993-05-10	1995-03-07	Microcom Corporation	Method and apparatus for printing a circular or bullseye bar code with a thermal printer
US5544246A *	1993-09-17	1996-08-06	At&T Corp.	Smartcard adapted for a plurality of service providers and for remote installation of same
US5420606A *	1993-09-20	1995-05-30	Begum; Paul G.	Instant electronic coupon verification system
GB9323489D0 *	1993-11-08	1994-01-05	Ncr Int Inc	Self-service business system
US5380991A *	1993-11-16	1995-01-10	Valencia; Luis	Paperless coupon redemption system and method thereof
US5623552A *	1994-01-21	1997-04-22	Cardguard International, Inc.	Self-authenticating identification card with fingerprint identification
CA2182596C *	1994-02-04	2004-04-20	James E. Biorge	Method and system for allocating and redeeming incentive credits between a portable device and a base device
US5461217A *	1994-02-08	1995-10-24	At&T Ipm Corp.	Secure money transfer techniques using smart cards
US5598474A *	1994-03-29	1997-01-28	Neldon P Johnson	Process for encrypting a fingerprint onto an I.D. card
US5590038A *	1994-06-20	1996-12-31	Pitroda; Satyan G.	Universal electronic transaction card including receipt storage and system and methods of conducting electronic transactions
US5546471A *	1994-10-28	1996-08-13	The National Registry, Inc.	Ergonomic fingerprint reader apparatus
US5870723A *	1994-11-28	1999-02-09	Pare, Jr., David Ferrin	Tokenless biometric transaction authorization method and system
US5979773A *	1994-12-02	1999-11-09	American Card Technology, Inc.	Dual smart card access control electronic data storage and retrieval system and methods
US5598782A *	1995-01-09	1997-02-04	Wales; Forrest A.	Credit card security device having card invalidating electromagnet
US5546523A *	1995-04-13	1996-08-13	Gatto; James G.	Electronic fund transfer system
EP0836726A4 *	1995-06-06	1998-09-02	Ken R Powell	Retail system
US7057492B2 *	1995-10-11	2006-06-06	Motorola, Inc.	Enabling/enhancing a feature of an electronic device using radio frequency identification technology
US5907142A *	1995-12-12	1999-05-25	Kelsey; Craig E.	Fraud resistant personally activated transaction card
US5745574A *	1995-12-15	1998-04-28	Entegrity Solutions Corporation	Security infrastructure for electronic transactions
US5943423A *	1995-12-15	1999-08-24	Entegrity Solutions Corporation	Smart token system for secure electronic transactions and identification
US5777903A *	1996-01-22	1998-07-07	Motorola, Inc.	Solar cell powered smart card with integrated display and interface keypad
JP3590184B2 *	1996-03-08	2004-11-17	株式会社東芝	Fingerprint detection device
US6038551A *	1996-03-11	2000-03-14	Microsoft Corporation	System and method for configuring and managing resources on a multi-purpose integrated circuit card using a personal computer
US6088450A *	1996-04-17	2000-07-11	Intel Corporation	Authentication system based on periodic challenge/response protocol
GB9608747D0 *	1996-04-26	1996-07-03	Philips Electronics Nv	Fingerprint sensing devices and systems incorporating such
US5815657A *	1996-04-26	1998-09-29	Verifone, Inc.	System, method and article of manufacture for network electronic authorization utilizing an authorization instrument
US5854891A *	1996-08-09	1998-12-29	Tritheim Technologies, Inc.	Smart card reader having multiple data enabling storage compartments
US5867795A *	1996-08-23	1999-02-02	Motorola, Inc.	Portable electronic device with transceiver and visual image display
US5917913A *	1996-12-04	1999-06-29	Wang; Yajun Paul	Portable electronic authorization devices and methods therefor
US5915023A *	1997-01-06	1999-06-22	Bernstein; Robert	Automatic portable account controller for remotely arranging for transfer of value to a recipient

IPR2025-00645 Page 01672

US5982913A *	1997-03-25	1999-11-09	The United States Of America As Represented By The National Security Agency	Method of verification using a subset of claimant's fingerprint
US6012636A *	1997-04-22	2000-01-11	Smith, Frank E.	Multiple card data system having first and second memory elements including magnetic strip and fingerprints scanning means
US6356934B1 *	1997-04-28	2002-03-12	Sabre Inc.	Intermediate server having control program for storing content accessed during browsing sessions and playback program for asynchronously replaying browsing sessions
US5920640A *	1997-05-16	1999-07-06	Harris Corporation	Fingerprint sensor and token reader and associated methods
US5974146A *	1997-07-30	1999-10-26	Huntington Bancshares Incorporated	Real time bank-centric universal payment system
US6316693B1 *	1997-10-02	2001-11-13	The Research Foundation Of The State University Of New York	Transgenic mouse model for fatty acid transport
CN1280686A *	1997-12-02	2001-01-17	凯宾技术公司	Multi-transactional network architecture
US6188309B1 *	1998-01-07	2001-02-13	At&T Corp	Method and apparatus for minimizing credit card fraud
US6095416A *	1998-02-24	2000-08-01	Privicorn, Inc.	Method and device for preventing unauthorized use of credit cards
FI980427A *	1998-02-25	1999-08-26	Ericsson Telefon Ab L M	Procedure, arrangement and device for verification
US6182892B1 *	1998-03-25	2001-02-06	Compaq Computer Corporation	Smart card with fingerprint image pass-through
US6334121B1 *	1998-05-04	2001-12-25	Virginia Commonwealth University	Usage pattern based user authenticator
US6604086B1 *	1998-07-20	2003-08-05	Usa Technologies, Inc.	Electronic commerce terminal connected to a vending machine operable as a telephone
US6332128B1 *	1998-07-23	2001-12-18	Autogas Systems, Inc.	System and method of providing multiple level discounts on cross-marketed products and discounting a price-per-unit-volume of gasoline
US6378069B1 *	1998-11-04	2002-04-23	Nortel Networks Limited	Apparatus and methods for providing software updates to devices in a communication network
US6212555B1 *	1998-11-16	2001-04-03	William E. Brooks, Jr.	Audio transfer, storage and playback system
US6085171A *	1999-02-05	2000-07-04	Excel Communications, Inc.	Order entry system for changing communication service
US6466130B2 *	1999-07-29	2002-10-15	Micron Technology, Inc.	Wireless communication devices, wireless communication systems, communication methods, methods of forming radio frequency identification devices, methods of testing wireless communication operations, radio frequency identification devices, and methods of forming radio frequency identification devices
US20020055351A1 *	1999-11-12	2002-05-09	Elsey Nicholas J.	Technique for providing personalized information and communications services
US6535909B1 *	1999-11-18	2003-03-18	Contigo Software, Inc.	System and method for record and playback of collaborative Web browsing session
US6874757B1 *	1999-12-02	2002-04-23	Avner Farkash	Credit card security device
EP1317718A2 *	2000-02-28	2003-06-11	360 Degree Web, Inc.	Smart card enabled mobile personal computing environment
US6882269B2 *	2000-07-14	2005-04-19	Darren Murrey	System and method for remotely coordinating the secure delivery of goods
AU8829301A *	2000-08-16	2002-02-25	Richard M Webb	Scannable barcode display and methods for using the same
US20020031225A1 *	2000-09-08	2002-03-14	Hines Larry Lee	User selection and authentication process over secure and nonsecure channels
US20020062251A1 *	2000-09-29	2002-05-23	Rajan Anandan	System and method for wireless consumer communications
US7353014B2 *	2000-10-31	2008-04-01	Vijay Raghavan Chetty	Universal portable unit
US6950939B2 *	2000-12-08	2005-09-27	Sony Corporation	Personal transaction device with secure storage on a removable memory device
US7099917B2 *	2001-04-18	2006-08-29	Openwave Systems Inc.	Method of providing a proxy server based service to a communications device on a network

IPR2025-00645 Page 01673

US7239226B2 *	2001-07-10	2007-07-03	American Express Travel Related Services Company, Inc.	System and method for payment using radio frequency identification in contact and contactless transactions
CA2357382A1 *	2001-09-17	2003-03-17	Soma Networks, Inc.	Software update method, apparatus and system
US6688093B2 *	2001-09-25	2004-02-03	Ecrio, Inc.	System, method and apparatus for communicating information between a mobile communications device and a bar code reader
WO2003044721A2 *	2001-11-19	2003-05-30	Burchette Robert L. Jr	Transaction card system having security against unauthorized usage
US7487538B2 *	2001-11-19	2009-02-03	Steven Siong Cheak Mok	Security system
US20040159700A1 *	2001-12-26	2004-08-19	Vivotech, Inc.	Method and apparatus for secure import of information into data aggregation program hosted by personal trusted device
US7051932B2 *	2001-12-26	2006-05-30	Vivotech, Inc.	Adaptor for magnetic stripe card reader
US7127236B2 *	2001-12-26	2006-10-24	Vivotech, Inc.	Micropayment financial transaction process utilizing wireless network processing
US7028897B2 *	2001-12-26	2006-04-18	Vivotech, Inc.	Adaptor for magnetic stripe card reader
USD491953S1 *	2002-10-10	2004-06-22	Vivotech, Inc.	Proximity interface with advertising insert for transaction acceptance systems
USD490840S1 *	2002-10-30	2004-06-01	Vivotech, Inc.	Proximity interface for transaction acceptance systems
USD491186S1 *	2002-11-27	2004-06-08	Vivotech, Inc.	Magnetic stripe simulacrum for transaction acceptance systems
USD498236S1 *	2003-01-24	2004-11-09	Vivotech, Inc.	Coreless inductor magnetic stripe simulacrum for transaction acceptance systems
GB2393014B *	2003-02-25	2004-08-11	Coupons Ltd I	Providing discounts at a POS terminal
USD506998S1 *	2003-02-28	2005-07-05	Vivotech, Inc.	Coreless inductor magnetic stripe simulacrum for right angle transaction acceptance systems

* Cited by examiner, † Cited by third party

Non-Patent Citations (1)

Title
MATTHEW FRENCH. "One card for all charges" [Online] 4 September 2001 (2001-09-04) , MASS HIGH TECH XP002258732 Retrieved from the Internet: <URL: http://www.masshightech.com/displayarticle detail.asp?art_id=47203> [retrieved on 2003-10-22] The whole document *

* Cited by examiner, † Cited by third party

Cited By (26)

Publication number	Priority date	Publication date	Assignee	Title
WO2005093644A1 *	2004-03-19	2005-10-06	Nokia Corporation	Detector logic and radio identification device and method for enhancing terminal operations
WO2005096239A1 *	2004-03-30	2005-10-13	Koninklijke Philips Electronics N.V.	Personal multiple-identification device
KR100854526B1 *	2006-09-18	2008-08-26	노키아 코포레이션	Detector logic and radio identification device and method for enhancing terminal operations
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7805615B2	2005-07-15	2010-09-28	Tyfone, Inc.	Asymmetric cryptography with user authentication
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US8189788B2	2005-07-15	2012-05-29	Tyfone, Inc.	Hybrid symmetric/asymmetric cryptography with user authentication
US8233881B2	2000-05-05	2012-07-31	Nokia Corporation	Communication devices and method of communication
US8231061B2	2009-02-24	2012-07-31	Tyfone, Inc	Contactless device with miniaturized antenna
CN103137176A *	2011-11-22	2013-06-05	华东科技股份有限公司	Storage device with a communications function
US8477940B2	2005-07-15	2013-07-02	Tyfone, Inc.	Symmetric cryptography with user authentication

IPR2025-00645 Page 01674

US8814053B2	2008-08-08	2014-08-26	Tyfone, Inc.	Mobile payment device with small inductive device powered by a host device
US8866614B2	2008-08-08	2014-10-21	Tyfone, Inc.	Active circuit for RFID
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
Family To Family Citations				
CA2571811C *	2004-12-22	2012-10-16	Bce Inc.	User authentication for contact-less systems
US20090160617A1 *	2007-12-24	2009-06-25	Dynamics Inc.	Credit, security, debit cards and the like with buttons
JP2009294821A	2008-06-04	2009-12-17	Sony Corp	Information processor, information processing method, program, and information processing system
US20120095919A1 *	2010-10-15	2012-04-19	Hart Annmarie D	Systems and methods for authenticating aspects of an online transaction using a secure peripheral device having a message display and/or user input
US9449324B2	2010-11-11	2016-09-20	Sony Corporation	Reducing TV licensing costs
US8914876B2	2011-05-05	2014-12-16	Ebay Inc.	System and method for transaction security enhancement
US9213822B2	2013-09-10	2015-12-15	Ebay Inc	Mobile authentication using a wearable device
US10083289B1 *	2015-10-07	2018-09-25	Google Llc	Authentication using an interactive cord
US10149036B1	2015-10-07	2018-12-04	Google Llc	Preventing false positives with an interactive cord
US9860785B1	2015-11-02	2017-10-31	Google Inc.	Interactive cord with integrated light sources
US10222924B2	2016-11-25	2019-03-05	Google Llc	Interactive cord with resistance touchpoints
US10733645B2	2018-10-02	2020-08-04	Capital One Services, Llc	Systems and methods for establishing identity for order pick up

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US7340439B2	2008-03-04	Portable electronic authorization system and method
US7080037B2	2006-07-18	Portable electronic authorization system and method
US7003495B1	2006-02-21	Portable electronic authorization system and method
US20100031043A1	2010-02-04	Portable electronic authorization system and method
US20090212909A1	2009-08-27	Portable electronic authorization system and method
US9904808B2	2018-02-27	Portable e-wallet and universal card
US8910862B2	2014-12-16	Retail point-of-transaction systems, program products, and related methods to provide a customized set of identification data to facilitate a retail transaction using electronic coupons
KR101100286B1	2011-12-28	method and system for creating and operating biometrically enabled multi-purpose credential management devices
US7735731B2	2008-04-15	System for associating identification and personal data for multiple magnetic stripe cards or other sources to facilitate a transaction and related methods
US20010034717A1	2001-10-25	Fraud resistant credit card using encryption, encrypted cards on computing devices
EP1508883A2	2005-02-23	Credit card application automation system
US20080126260A1	2008-05-29	Point Of Sale Transaction Device With Magnetic Stripe Emulator And Biometric Authentication
US20070185820A1	2007-08-09	Multi-account security verification system with a virtual account and linked multiple real accounts
EP1061482B1	2004-02-04	Method, system, and apparatus for transmitting, receiving, and displaying information
WO2005043438A1	2005-05-12	Portable electronic authorization system and method
KR20050006628A	2005-01-17	System and method for processing an electronic receipt

Priority And Related Applications

Priority Applications (4)

IPR2025-00645 Page 01675

Application	Priority date	Filing date	Title
US36609802P	2002-03-19	2002-03-19	*US Provisional Application*
US60/366,098		2002-03-19	
US37996402P	2002-05-13	2002-05-13	*US Provisional Application*
US60/379,964		2002-05-13	

Applications Claiming Priority (2)

Application	Filing date	Title
CA002479343A	2003-03-19	Portable electronic authorization system and method
EP03718013A	2003-03-19	Portable electronic authorization system and method

Legal Events

Date	Code	Title	Description
2003-10-02	AL	Designated countries for regional patents	**Kind code of ref document:** A2 **Designated state(s):** 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
2003-10-02	AK	Designated states	**Kind code of ref document:** A2 **Designated state(s):** CA
2003-11-26	121	Ep: the epo has been informed by wipo that ep was designated in this application	
2004-09-15	WWE	Wipo information: entry into national phase	**Ref document number:** 2479343 **Country of ref document:** CA
2004-10-18	WWE	Wipo information: entry into national phase	**Ref document number:** 2003718013 **Country of ref document:** EP
2004-12-22	WWP	Wipo information: published in national office	**Ref document number:** 2003718013 **Country of ref document:** EP
2006-03-31	WWW	Wipo information: withdrawn in national office	**Ref document number:** 2003718013 **Country of ref document:** EP

Data provided by IFI CLAIMS Patent Services

Patents 2003010939

Interface apparatus

Abstract

A memory card (1) includes data terminals (DATA/SDI0, DATA1, DATA2, DATA3) for performing bidirectional communication of 4-bit parallel data with a host by using four data communication lines, a clock terminal (SCLK) for receiving a clock from the host, and a terminal (BS) for receiving from the host a bus state signal indicating the state of the communication lines of the 4-bit parallel data and the transmission start timing. The first data terminal (DATA0/SDI0) is also used as a data terminal of a memory card performing 1-bit serial data communication and is compatible with this memory card.

Classifications

G06K19/077 Constructional details, e.g. mounting of circuits in the carrier

View 4 more classifications

WO2003010939A1

WIPO (PCT)

Download PDF Find Prior Art Similar

Other languages: French, Japanese

Inventor: Hideaki Bando

Worldwide applications

2002 WO JP EP CN SN US KR EP DE DE

Application PCT/JP2002/006496 events

2001-07-25 Priority to JP2001-225052

2001-07-25 Priority to JP2001225052

2002-06-27 Application filed by Sony Corporation

2003-02-06 Publication of WO2003010939A1

Info: Patent citations (25), Non-patent citations (1), Cited by (36), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, PatentScope, Discuss

Patent Citations (25)

Publication number	Priority date	Publication date	Assignee	Title
JPS59161957A *	1983-03-07	1984-09-12	Mitsubishi Electric Corp	Data transmitter
JPS6051046A *	1983-08-30	1985-03-22	Nec Corp	Digital signal transmitting system
JPH08202653A *	1995-01-27	1996-08-09	Ricoh Co Ltd	Parallel signal transmission equipment
JPH1153306A *	1997-06-04	1999-02-26	Sony Corp	Data processor, external storage device, data processing system and data transmission method
JP2000259783A *	1999-03-12	2000-09-22	Sony Corp	Drive device
JP2001005943A *	1999-04-23	2001-01-12	Sony Corp	Semiconductor memory card
Family To Family Citations				
DE3751608T2 *	1986-09-01	1996-06-27	Nec Corp	Serial bus interface system for data transmission with a two-wire line as clock bus and data bus.
US5086427A *	1990-04-09	1992-02-04	Unisys Corporation	Clocked logic circuitry preventing double driving on shared data bus
JPH04274082A	1991-03-01	1992-09-30	Mitsubishi Electric Corp	Semiconductor memory device
US5251305A *	1991-04-04	1993-10-05	Unisys Corporation	Apparatus and method for preventing bus contention among a plurality of data sources
JPH07271928A *	1994-03-29	1995-10-20	Hitachi Ltd	Non-contact parallel data transfer device and memory card
US5646553A *	1995-05-10	1997-07-08	3Com Corporation	Driver for tri-state bus
US5648733A *	1995-11-01	1997-07-15	Lsi Logic Corporation	Scan compatible 3-state bus control
US5767701A *	1996-06-28	1998-06-16	Cypress	Synchronous contention prevention logic for bi-directional signals

			Semiconductor Corp.	
US5789944A *	1996-06-28	1998-08-04	Cypress Semiconductor Corp.	Asynchronous anticontention logic for bi-directional signals
US5966723A *	1997-05-16	1999-10-12	Intel Corporation	Serial programming mode for non-volatile memory
US6411202B1	1998-05-21	2002-06-25	Sony Corporation	System for communicating status via first signal line in a period of time in which control signal via second line is not transmitted
CN1256005A *	1998-01-21	2000-06-07	索尼株式会社	Encoding method and memory device
JP2003532936A *	1998-03-26	2003-11-05	ジェムプリュス	General-purpose interface IC card
US6101567A	1998-06-03	2000-08-08	Lucent Technologies Inc.	Parallel backplane physical layer interface with scalable data bandwidth
KR100275924B1 *	1998-07-18	2000-12-15	김윤호	A apparatus for interfacing smart card
JP3815936B2 *	2000-01-25	2006-08-30	株式会社ルネサステクノロジ	IC card
US6978340B2 *	2000-01-31	2005-12-20	Visteon Corporation	I/O multiplexer and pin controller with serial and parallel capabilities for microprocessor based engine control
JP4649098B2 *	2000-03-08	2011-03-09	株式会社東芝	Information processing apparatus having a card interface, card-type electronic equipment that can be mounted on the apparatus, and operation mode setting method in the apparatus
KR100921851B1 *	2001-06-28	2009-10-13	소니 가부시끼 가이샤	Electronic apparatus, information processing apparatus, adapter apparatus, and information exchange system

* Cited by examiner, † Cited by third party

Non-Patent Citations (1)

Title
See also references of EP1411705A4 *

* Cited by examiner, † Cited by third party

Cited By (36)

Publication number	Priority date	Publication date	Assignee	Title
JP2003091703A *	2001-09-14	2003-03-28	Toshiba Corp	Card device
JP2006079289A *	2004-09-08	2006-03-23	Sony Corp	Communication system
JP2009531746A *	2006-03-28	2009-09-03	モサイド・テクノロジーズ・インコーポレーテッド	Daisy chain layout of non-volatile memory
JP2010506301A *	2006-10-05	2010-02-25	エルエスアイ コーポレーション	Apparatus and method for improved SATA device interaction without a SAS expander
US9230654B2	2005-09-30	2016-01-05	Conversant Intellectual Property Management Inc.	Method and system for accessing a flash memory device
US9240227B2	2005-09-30	2016-01-19	Conversant Intellectual Property Management Inc.	Daisy chain cascading devices
Family To Family Citations				
US7660902B2 *	2004-03-16	2010-02-16	Super Talent Electronics, Inc.	Extended SD and microSD hosts and devices with USB-like high performance packetized interface and protocol
US7137564B2 *	2002-08-09	2006-11-21	Carry Computer Eng. Co., Ltd	Communication protocol for multi-functional mini-memory card suitable for small form memory interface and usb interfaces
DE60305752T2 *	2002-01-24	2007-01-25	Matsushita Electric Industrial Co., Ltd., Kadoma	memory card

US20040039835A1 *	2002-08-21	2004-02-26	Intel Corporation	Method and apparatus for transferring general purpose control information between processors
JP2005123858A *	2003-10-16	2005-05-12	Mega Chips Corp	Camera control device
US8234421B2 *	2004-04-21	2012-07-31	Stmicroelectronics, Inc.	Smart card with selectively allocatable data buffers and associated methods
SE0401531D0 *	2004-06-15	2004-06-15	Hms Ind Networks Ab	Communications module interface
JP4565966B2 *	2004-10-29	2010-10-20	三洋電機株式会社	Memory element
US7586469B2	2004-11-17	2009-07-21	Nokia Corporation	Multimedia card interface method, computer program product and apparatus
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
JP4896450B2	2005-06-30	2012-03-14	株式会社東芝	Storage device
JP5193045B2 *	2005-09-30	2013-05-08	モサイド・テクノロジーズ・インコーポレーテッド	Memory with output controller
JP4956143B2 *	2006-11-02	2012-06-20	株式会社東芝	Semiconductor memory card, host device, and data transfer method
US7613049B2	2007-01-08	2009-11-03	Macronix International Co., Ltd	Method and system for a serial peripheral interface
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
TWI353145B *	2007-12-26	2011-11-21	Ralink Technology Corp	Method for receiving data with sdio interface and
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US20100125689A1 *	2008-11-20	2010-05-20	Mediatek Inc.	Electronic apparatus capable of receiving different types of memory cards
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
JP5746201B2	2009-11-05	2015-07-08	ラムバス・インコーポレーテッド	Interface clock management
US9929972B2	2011-12-16	2018-03-27	Qualcomm Incorporated	System and method of sending data via a plurality of data lines on a bus
TWI519964B *	2012-08-01	2016-02-01	慧榮科技股份有限公司	Storage medium, data transmittal system and control method thereof
TWI482084B *	2013-05-17	2015-04-21	Wistron Corp	Interface card
KR102166908B1 *	2014-02-13	2020-10-19	삼성전자주식회사	Data interface method having de-skew function and Apparatus there-of
US9552318B2 *	2014-06-04	2017-01-24	Qualcomm Incorporated	Removable memory card type detection systems and methods
US9792965B2 *	2014-06-17	2017-10-17	Rambus Inc.	Memory module and system supporting parallel and serial access modes
CN104866442B *	2015-06-03	2018-01-12	山东鲁能电力科技有限公司	A kind of digital facility interface and method for interchanging data
CN111124023B *	2020-01-19	2021-10-26	惠州Tcl移动通信有限公司	Insertion detection circuit and method of flash memory card, and electronic device

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
WO2003010939A1	2003-02-06	Interface apparatus
US7308516B2	2007-12-11	Bi-directional serial interface for communication control
KR100833176B1	2008-05-28	Efficient connection between modules of removable electronic circuit cards
EP1584065B1	2009-11-11	Means for communicating with usb smart cards using full-speed or high-speed transfers
WO2004055638A3	2005-08-18	Wireless communication between computing devices
WO2002019266A3	2002-04-18	Cooperative interconnection and operation of a non-volatile memory card and an input-output card

IPR2025-00645 Page 01679

WO2002047860A8	2003-06-19	System for carrying out a welding process
EP1533706A4	2006-05-10	Ic card, terminal device, and data communication method
TW200715665A	2007-04-16	Connector
EP1619609A3	2006-06-07	Memory card, memory card communication control method, electronic device, and wireless communication system
EP1559511A3	2010-05-05	System and method for communicating over power terminals in cordless dc tools
EP1457901A3	2005-07-06	System and method for simulating USB smart cards connected to USB host
WO2001065827A3	2002-06-13	Portable information terminal and digital camera therefor, and portable digital camera information terminal system
WO2002054643A8	2003-06-26	Method and system for administering digital collectible cards
TW200715129A	2007-04-16	Method and apparatus for data transmission in a wireless communication system and data transmission method
EP1587277A3	2006-03-01	Device, system and method for defining a response waiting time before timeout
EP1658631A4	2009-06-17	Non-contact information medium and communication system using the non-contact information medium
EP1263174A3	2003-09-24	Information communication apparatus and information communication method
WO2000062134A3	2001-09-27	Improved inter-device serial bus protocol
US9078922B2	2015-07-07	Apparatus and method for decoding data transmissions
MY119255A	2005-04-30	Pcmcia rf connector
EP1071067A3	2001-10-24	Display driver IC and electronic device using the same
WO2001082090A3	2002-02-21	Extended cardbus/pc card controller with split-bridge technology
SG115352A1	2005-10-28	Handheld device, smart card interface device (ifd) and data transmission method
WO1998040976A3	1998-12-03	Device and method for dect-standard cordless communication

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
JP2001-225052		2001-07-25	
JP2001225052		2001-07-25	

Applications Claiming Priority (5)

Application	Filing date	Title
EP02738823A	2002-06-27	Interface apparatus
US10/381,311	2002-06-27	Interface apparatus
KR1020037004027A	2002-06-27	Interface apparatus
JP2003516195A	2002-06-27	Interface device
DE60229137T	2002-06-27	INTERFACE DEVICE

Legal Events

Date	Code	Title	Description
2003-02-06	AK	Designated states	**Kind code of ref document**: A1 **Designated state(s)**: CN JP KR **Kind code of ref document**: A1 **Designated state(s)**: CN JP KR US
2003-02-06	AL	Designated countries for regional patents	**Kind code of ref document**: A1

			Designated state(s): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR **Kind code of ref document:** A1 **Designated state(s):** AT BE CH CY DE DK ES FI FR GB IE IT LU MC NL PT SE TR
2003-03-17	WWE	Wipo information: entry into national phase	**Ref document number:** 2003516195 **Country of ref document:** JP
2003-03-19	WWE	Wipo information: entry into national phase	**Ref document number:** 2002738823 **Country of ref document:** EP
2003-03-20	WWE	Wipo information: entry into national phase	**Ref document number:** 1020037004027 **Country of ref document:** KR
2003-03-24	WWE	Wipo information: entry into national phase	**Ref document number:** 10381311 **Country of ref document:** US
2003-04-02	121	Ep: the epo has been informed by wipo that ep was designated in this application	
2003-04-25	WWE	Wipo information: entry into national phase	**Ref document number:** 028027620 **Country of ref document:** CN
2004-02-27	WWP	Wipo information: published in national office	**Ref document number:** 1020037004027 **Country of ref document:** KR
2004-04-21	WWP	Wipo information: published in national office	**Ref document number:** 2002738823 **Country of ref document:** EP
2008-10-01	WWG	Wipo information: grant in national office	**Ref document number:** 2002738823 **Country of ref document:** EP

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents TWI457835

An article carrying a thin film integrated circuit

Classifications

G06K19/00 Record carriers for use with machines and with at least a part designed to carry digital markings

View 8 more classifications

TWI457835B
Taiwan

Download PDF Find Prior Art Similar

Other languages: Chinese

Inventor: Yasuyuki Arai, Mai Akiba, Yuko Tachimura, Yohei Kanno

Worldwide applications

2005 TW US KR CN 2006 US

Application TW094102340A events

2004-02-04 Priority to JP2004027699

2005-01-26 Application filed by Semiconductor Energy Lab

2005-09-01 Publication of TW200529088A

2014-10-21 Application granted

2014-10-21 Publication of TWI457835B

Info: Patent citations (17), Cited by (101), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (22)

Hide Dependent

1. An article carrying a thin film integrated circuit, comprising: an antenna comprising a thin film transistor and a thin film integrated circuit device connected to the antenna; and a filling layer surrounding the antenna, wherein a resin layer is used as the A fill layer, and one of the fillers is included in the fill layer.

2. An article as claimed in claim 1, wherein the article is an ID tag.

3. For example, the article of claim 1 is an ID card.

4. For example, the article of claim 1 is an ID tag.

5. The article of claim 1, further comprising a separation layer bonded to the filling layer by a layer of a bonding material inserted therein.

6. The article of claim 1, wherein the filler layer comprising the filler has a coefficient of thermal expansion that is less than or equal to twice the coefficient of thermal expansion of the electrically conductive material of the antenna.

7. The article of claim 1, wherein the filler has a function of reducing or increasing a thermal expansion coefficient of the filling layer, and reducing a conductive material between the filling layer and the antenna or forming a thin film of the thin film. The function of the difference in thermal expansion coefficient.

8. An article as claimed in claim 1, wherein the shape of the filler it is spherical or cylindrical.

9. An article according to claim 1, wherein a protective film is formed at least above or below the thin film integrated circuit device, and includes yttrium oxide, tantalum nitride, SiO_xN_y (x>y), and SiN_xO A single layer or laminate of at least one of $_y$ (x>y).

10. The article of claim 1, wherein the semiconductor film of the thin film transistor included in the thin film integrated circuit device contains at least one of hydrogen and halogen at a concentration of from 1×10^{19} to 5×10^{20} cm^{-3}.

11. The article of claim 1, wherein the thin film integrated circuit device has a thickness of 0.1 to 3 μm.

12. The article of claim 1, wherein the antenna comprises a material selected from the group consisting of Ag, Au, Al, Cu, Zn, Sn, Ni, Cr, Fe, Co, or Ti, and combinations thereof.

13. The article of claim 1, wherein the resin is one selected from the group consisting of photosensitive organic materials, non-photosensitive organic materials, and thermally resistant organic resins.

14. The article of claim 1, wherein the filler comprises a material selected from the group consisting of vermiculite (SiO_2), aluminum oxide (Al_2O_3), boron nitride (BN), manganese oxide, aluminum nitride (AlN), Group of tantalum nitride, glass fiber, cerium oxide, carbon fiber, calcium carbonate, mica (talcan), mica, silver

IPR2025-00645 Page 01682

powder, copper powder, nickel powder, and copper powder covered with silver One of the materials.

15. The article of claim 5, wherein the bonding material layer comprises a material selected from the group consisting of a cyanoacrylate adhesive material and a vinyl acetate resin emulsion. A material consisting of a rubber material, a (poly)vinyl chloride resin material, a vinyl acetate solvent material, an epoxy material, and a hot melt (hot melt) material.

16. The article of claim 5, wherein the separation layer comprises a material selected from the group consisting of paper, synthetic paper, plastic, PET, polypropylene, polyethylene, polystyrene, nylon, and inorganic materials.

17. An article carrying a thin film integrated circuit, comprising: a substrate, an antenna on the substrate; a thin film integrated circuit device including the thin film transistor and operatively connected to the antenna; operatively connecting the antenna and the thin film integrated body a connection pad of the circuit device; a filling layer surrounding the antenna; an operation connecting the thin film integrated circuit device and a wire of the antenna, wherein a resin layer is used as the filling layer, and one of the fillers is included in the In the fill layer.

18. The article of claim 17 wherein the filler layer comprising the filler has a coefficient of thermal expansion that is less than or equal to twice the coefficient of thermal expansion of the electrically conductive material of the antenna.

19. A method of manufacturing an article carrying a thin film integrated circuit, the method comprising the steps of: forming a thin film integrated circuit device on a substrate; operatively connecting the thin film integrated circuit to an antenna, and a filling layer inserted therebetween; wherein the thin film integrated circuit device is operatively connected to the antenna via a connection pad, wherein a resin layer is used as the filling layer, and one of the fillers is included in the filling layer to be in contact with the substrate.

20. The method of claim 19, wherein the filler layer comprising the filler has a coefficient of thermal expansion that is less than or equal to twice the coefficient of thermal expansion of the electrically conductive material of the antenna.

21. A method of manufacturing an article carrying a thin film integrated circuit, the method comprising the steps of: forming an antenna on a first substrate; operatively connecting a thin film integrated circuit device to the antenna; attaching the first substrate to a second a substrate, wherein the first filling layer is interposed therebetween, and the first substrate to the third substrate is attached, and the second filling layer is interposed therebetween, wherein the first substrate is interposed between the second substrate and the third substrate.

22. The method of claim 21, wherein the first filling layer and the second filling layer have a coefficient of thermal expansion that is less than or equal to twice the coefficient of thermal expansion of the electrically conductive material of the antenna.

Description

Article carrying a thin film integrated circuit

BACKGROUND OF THE INVENTION 1. Field of the Invention This invention relates to an article carrying a very thin mode film integrated circuit that can have a memory, a microprocessor (central processing unit, CPU or MPU), and other mechanical functions. The item includes, for example, an ID tag, an ID tag, and an ID card, which are mainly used to identify persons, animals and plants, commodities, and the like.

In recent years, various industries, such as the food industry, the manufacturing industry, or the like, have demanded an increase in the safety and management systems of commodities, thereby increasing the amount of information on goods. However, the main information on the goods is only the manufacturing country, manufacturer, serial number or other information, mainly provided by a dozen symbols in the bar code, the amount of information is very small. In addition, in the case of using barcodes, it is performed manually one by one, so that it takes a long time to read the barcode. Therefore, instead of the bar code system, the automatic identification technology of the non-contact IC tag using electromagnetic waves, also called RFID (Radio Frequency (Radio Frequency) Recognition Technology), has attracted extensive attention

In addition, in order to ensure the safety of animals and plants (eg, origin, or infection with infectious diseases), systems have become more and more popular by implanting IC wafers directly into animals and plants, and by animals and plants. An in vitro information reading device (reading head) to acquire and manage information.

In addition, a variety of personal-only cards have recently appeared, and all of these non-contact IC cards that use electromagnetic fields for communication have become very popular, for example, electronic money and electronic tickets (refer to Non-Patent Document 1).

(Non-Patent Document 1) Nikkei Electronics (Nikkei Business Publications, Inc.), published on November 18, 2002, pp. 67-76.

Now, in products and ID cards that bond non-contact or contact ID or ID tags, a large number of products and ID cards can be used under a wide temperature range depending on the type. In the case of such a product to which a non-contact ID mark or an ID tag is bonded, there is a concern that a coefficient of thermal expansion is large due to a difference in thermal expansion coefficient of the antenna for communication and the resin provided around the antenna. The resin generates stress, causing the resin to break. Further, in the case where the contact IC wafer is bonded to a commodity, it is feared that the resin is broken due to the difference between the contact electrode and the coefficient of thermal expansion of the resin provided around the contact electrode. These naturally affect the manufacturing yield, service life and reliability of the ID mark, among others.

The present invention has been made in view of the above circumstances, and it is therefore an object of the present invention to provide a technical structure such as an ID tag, an ID tag, and an ID card, and a manufacturing method thereof, so that it is possible to prevent a resin covering an antenna or a contact electrode from being broken due to stress, even in When there is a large difference in the temperature of the ID tag, the ID tag, and the ID card.

1) The ID mark according to the present invention has features including an antenna, a thin film integrated circuit device including a thin film transistor connected to the antenna, a filling layer including a filler around the antenna, a bonding layer, and a separation layer.

2) The ID tag according to the present invention has features including an antenna, a thin film integrated circuit device including a thin film transistor connected to the antenna, and a filling layer including a filler around the antenna.

The ID chip carries an antenna and is capable of radio communication, also known as a wireless chip.

3) The ID mark according to the present invention has features including an antenna, a thin film integrated circuit device including a thin film transistor connected to the antenna, a filling layer including a filler around the antenna, a bonding layer, and a spacer.

The ID tag, ID tag, ID card, and wireless chip according to the present invention may also be referred to as "semiconductor devices."

Each of the thin film integrated circuit devices of the ID tag, the ID tag, and the ID card according to the present invention includes a thin film active element such as a thin film transistor TFT (thin film nonlinear element. For example, a thin film product is fabricated using TFT). In the case of a bulk circuit, a thin film integrated circuit device including a TFT is characterized by low-cost mass production by separating a device by forming a TFT on a substrate to be peeled off and then peeling off the substrate to be peeled off. The method of the substrate can be broadly classified into a physical peeling method using a chemical peeling method such as etching to remove the peeling layer or a peeling layer by externally applying an impact (stress). However, the method is not limited thereto.

The concept of a thin film integrated circuit device is different from a conventional "IC (Integrated Circuit) wafer" formed on a germanium wafer, and the integrated circuit device shown includes a thin film active device typical of a TFT, and the thin film active devices are connected to each other. Wiring and wiring to connect the thin film active device to an external structure (for example, an antenna in the case of a contactless ID mark or a contact electrode in the case of a contact ID mark). Of course, the components of the thin film integrated circuit device are not limited thereto. The device may be referred to as a thin film integrated circuit device as long as at least one thin film active device such as a TFT is included in the device.

The thin film integrated circuit device used in the present invention is a film different from a conventional IC wafer, and may be referred to as an IDT wafer (identifying thin wafer) or the like. Further, the thin film integrated circuit device used in the present invention is not, in principle, used of a germanium wafer, but uses, for example, a glass substrate or a quartz substrate, and can be easily transferred to a flexible substrate as will be described below. Discussed, it can be referred to as an IDG wafer (identified glass wafer), an IDF wafer (identifying a flexible wafer), a soft wafer, or the like. Hereinafter, the "thin film integrated circuit device" may be referred to as "IDF wafer" or the like

The ID tag (identification tag) has a function of identifying a product distributed in the market and storing product information, and may also be referred to as an ID seal, an ID tag, or the like. Basically, one side of the ID mark is a bonded surface, so that the ID mark can be attached to the article and the like, and the ID mark includes the function of repeating the bond multiple times. Of course, the ID tag is not limited to this as long as it is still classified as a mark, a seal, a mark, a badge, and a mark in a general case.

The antenna has a function of communicating with an external reader/writer or the like, and may be formed on a substrate on which an ID mark, an ID tag or an ID card is formed, or integrated together in a thin film integrated circuit device. The substrate itself may be an exposed substrate or a non-exposed substrate (internal or inner substrate). The substrate may have a single layer structure or a laminated structure, and the material thereof is not particularly limited. The substrate can act as a covering or coating.

The ID tag has the function of identifying the attributes of the goods in the market and retrieving the information of the goods, just like the ID tag. Management is made easy by installing ID tags or ID tags on the product. For example, in the case of stolen goods, the thief can be caught by tracking the whereabouts of the merchandise. In this way, by providing the ID tag, it is possible to distribute the so-called traceable fine goods (in this case, in the case where problems occur in the steps of manufacturing and distributing the finished goods, the trace of the cause of the problem can be quickly found To arrange it). In addition, the use of ID tags helps identify the exact whereabouts of special singles, such as babies, students or the elderly, in the face of increasing facts such as odious crimes and thefts, thereby reducing the likelihood of their involvement in the accident. .

The ID card refers to a card including a micro-minifilm integrated circuit device capable of storing various kinds of information, and refers to all cards such as a cash card, a credit card, a payment card, an electronic ticket, an electronic money, a telephone card, and a membership card.

The filler is a filler material or a mixture having a function of lowering or increasing the coefficient of thermal expansion of the packed layer. Materials as fillers include, but are not limited to, cerium oxide (SiO_2), aluminum oxide (Al_2O_3), boron nitride (BN), manganese oxide, aluminum nitride (AlN), tantalum nitride. , glass fiber (continuous glass fiber such as columnar glass rod), cerium oxide (for example, spherical cerium oxide), carbon fiber, calcium carbonate, mica (talc) and mica Preferably, the use of these materials can reduce the difference in thermal expansion coefficient of a conductive material forming a film or an antenna of a thin film active device such as a TFT. This makes it possible to avoid peeling and cracking of the filling layer which is caused by the difference in thermal expansion coefficient between different materials used in the integration of the antenna and the TFT. For example, in the case where a resin is used as the filling layer, since the resin has a larger coefficient of thermal expansion (CTE) than the conductive material or the semiconductor material, by including a filler in the filling layer, the CTE of the resin is close to the conductive material or The CTE of the semiconductor material can thereby reduce thermal expansion. Preferably, the filled layer has high formation properties (low viscosity, low thixotropy, high bond stability and optimum particle size), heat dissipation characteristics and high heat transfer.

Now, various ID tags, ID tags, and ID cards according to the present invention each have an antenna formed on a substrate formed by an ID tag, an ID tag, and an ID card; a thin film integrated circuit device including a thin film transistor and an antenna Connecting, and filling comprising a filler and contacting the substrate, making it possible to reduce the difference in thermal expansion coefficient between the filling layer and the conductive material of the antenna or between the filling layer and the film forming the thin film active element such as TFT Floor. Therefore, it is possible to eliminate stress caused by a difference in thermal expansion coefficient between different materials, so that peeling and cracking of the filling layer provided around the antenna and between the antenna and the TFT can be avoided.

Further, various thin film integrated circuit devices of ID tags, ID tags, and ID cards according to the present invention have features including thin film active elements such as TFTs. Therefore, the thin film integrated circuit device can be produced at a low cost and in large quantities, for example, a method of separating the device by forming a TFT on a substrate to be peeled off and then peeling off the substrate to be peeled off can be employed. Further, since the thin film active element is provided to form the thin film integrated circuit device, the obtained ID mark, ID label, and ID card can be made thinner as compared with the conventional ID mark, ID tag, and ID card.

Further, unlike forming an IC wafer on a conventional germanium substrate, backgrinding may not be required. Therefore, the processing can be significantly simplified, so that the manufacturing cost can be significantly reduced As the substrate to be peeled off, a substrate which is much cheaper than the ruthenium substrate, for example, a glass substrate, a quartz substrate, a solar cell grade ruthenium substrate, and a substrate which needs to be peeled off can be used again, so that a cost reduction can be obtained.

In addition, unlike IC manufacturing using a germanium wafer, it is not necessary to perform back grinding due to polishing and cracking, and the thickness unevenness of the device depends on the non-uniformity of deposition of each film and is about several hundred Nano, as compared to the non-uniformity of several to several tens of micrometers by back grinding, can be significantly reduced.

Further, the thin film integrated circuit device used in the present invention is thinner (0.1 to 3 μm) than a conventional ID wafer having a thickness of about 0.06 mm (60 μm), and is very suitable for being inserted as thin as a wafer. In particular, it includes paper or a thin article such as a film resin. The IDF wafer, which can have a very thin thickness, can be filled with an organic resin material to form a composite object. This makes it possible to avoid adverse effects on the IDF wafer due to bending stress.

The use of the highly elastic organic material as the filling layer can significantly concentrate the stress on the insulating film and the protective film including the organic

IPR2025-00645 Page 01684

material due to the deformation, and then cause the films to be deformed. Therefore, the stress applied to the thin film transistor can be reduced. Further, since the portion where the stress is mainly applied at the time of deformation is not at the edge of the semiconductor film but at the edge of the base film, stress concentration at the edge or interface of the semiconductor film can be suppressed.

As discussed above, according to the present invention, it is possible to provide various items such as ID tags, ID tags, and ID cards which are low-cost mass-produced and thinner, and which are excellent in functions.

Embodiment modes and embodiments of the present invention will be discussed below with reference to the accompanying drawings. The present invention may, however, be embodied in various embodiments and various modifications and modifications are apparent to those skilled in the art. Therefore, unless such changes and modifications depart from the scope of the invention, they should be included. For example, any embodiment mode and embodiment are suitable for implementing the invention in combination. Therefore, the embodiment modes and examples are not intended to be limiting of the invention.

(Embodiment Mode 1)

The structure and manufacturing method of the ID mark according to the present invention will be discussed mainly with reference to Figs. 1A, 4A and 4B and Figs. 5A and 5B. 1A is a perspective view illustrating an ID mark structure according to the present invention, in which, for the sake of simplicity, a substrate (referred to as "bonded paper") which forms a part of an ID mark adhered to a commodity or the like is shown below, but Not limited to paper), the separation layer used as the marking plate is shown above.

Fig. 1A shows a case in which an antenna 11 and a connection pad 12 for pre-forming a thin film on an antenna and a substrate 10 forming an ID mark (hereinafter referred to as "substrate" or "marking substrate") are included. Connecting the connecting portions of the bulk circuit device, and then bonding the formed thin film integrated circuit device 13 to the marking substrate, respectively, on the surface of the marking substrate (the back side of the drawing), such as characters, symbols or Printing 14 such as graphics. In the case of discussing a so-called hybrid ID mark having a non-contact type and a contact type function, a printing method can be employed to form a wiring pattern having a connection end.

Next, the filling layer 24 including the filler 28 is formed in contact with the substrate 10 on which the antenna 11 and the thin film integrated circuit device 13 are formed. In the drawings for explanation, each of the fillers is drawn in an actual size enlargement manner. As the filling layer 24, a photosensitive or non-photosensitive organic material such as epoxy, polyimide, acrylic, polyamide, resist, and benzocyclobutane, and a heat-resistant organic resin can be used, for example, a decane (a material having a bismuth (Si) and oxygen (O) bond forming a backbone, and including at least one of hydrogen as a substituent or at least one selected from the group consisting of fluorine, an alkyl group, and an aromatic hydrocarbon. base). As a method of forming the same, the following methods may be employed depending on the material, for example, spin coating, dipping, spraying, or droplet dripping (for example, inkjet, screen printing, lithography or gravure printing), doctor blade, roller coating. , curtain coating or scraping. The filling layer 24 may have a single layer structure including the above materials or may have a laminated structure in which the above materials are used in combination.

Suitable materials for filler 28 include, but are not limited to, vermiculite, alumina, boron nitride, magnesia, aluminum nitride, tantalum nitride, glass fiber, ceria, carbon fiber, calcium carbonate, talc, and Mica. It is preferable to use a material capable of reducing a difference in thermal expansion coefficient of a conductive material forming a film or an antenna of a thin film active element such as a TFT. The filling layer 24 may also have the function of protecting the substrate 10. The fill layer may form an integral cover substrate or may form a partial cover substrate.

Now, a brief discussion of the advantages of the filling layer 24 including the filler 28 such as cerium oxide, in which case an epoxy resin (coefficient of thermal expansion: about 25×10^{-6} to 90×10^{-6} /° C.) is used as the filling layer. 24, and Cu (coefficient of thermal expansion: 16.5×10^{-6} /° C.) is used as a conductive material of the antenna 11. In the case where 50% by weight of the filler is included in the epoxy resin, the coefficient of thermal expansion can be reduced to about half (about 12.5×10^{-6} to 45×10^{-6} / ° C). Further, in the case where 75% by weight of the filler is included in the epoxy resin, the coefficient of thermal expansion can be reduced to about one third (about 8×10^{-6} to 30×10^{-6} / ° C). However, as the filler content increases more and more, the viscosity of the epoxy resin increases, thereby reducing its forming properties. Therefore, it is preferred that the filler content is limited to 75% by weight or less than 75% by weight. On the basis of this, as long as the coefficient of thermal expansion including the resin of the filler 28 is reduced to be less than or equal to twice the coefficient of thermal expansion of the conductive material of the antenna, the generation of stress due to the difference between the coefficients of thermal expansion can be remarkably avoided.

Further, a combination of a conductive material having a higher coefficient of thermal expansion and a resin having a lower coefficient of thermal expansion may have a lower filler content. A conductive material having a higher coefficient of thermal expansion generally includes: Ag (coefficient of thermal expansion: 19.6×10^{-6} /° C.), Al (coefficient of thermal expansion: 24.6×10^{-6} /° C.), and Sn (coefficient of thermal expansion: 21 × 10) in addition to Cu. $^{-6}$ / ° C), Zn (coefficient of thermal expansion: 30×10^{-6} / ° C), Pb (coefficient of thermal expansion: 29×10^{-6} / ° C), Au (coefficient of thermal expansion: 14.2×10^{-6} / ° C) or the like. Resins having a lower coefficient of thermal expansion generally include: an anthracene resin (about 5×10^{-6} to 55×10^{-6} /° C.), an alkyd resin (about 15×10^{-6} to 55×10^{-6} /° C.) in addition to an epoxy resin.), amino resin (about 10×10^{-6} to 60×10^{-6} / ° C), phenolic resin (about 15×10^{-6} to 125×10^{-6} / ° C) and allyl resin (about 25×10^{-6} to 115×10^{-6} / ° C).

In the case where the filling layer 24 is provided only in the portion where the thin film integrated circuit device 13 and the antenna 13 are connected, a conductive filler can be used. As the conductive filler, a metal-based conductive filler such as silver powder, copper powder, nickel powder, and copper powder coated with silver, a non-metal-based conductive filler, and a carbon-based conductive material can be generally used. Sex filler. Of course, conductive fillers are not considered to be only limited thereto.

For the thin film integrated circuit device 13, a thin film active element such as a TFT can be used. The specific structure and manufacturing method of the TFT will be discussed below. The thin film integrated circuit device 13 can be formed using a thin film active device such as a TFT, and can be formed into a film thickness of about 5 μm or less, preferably 0.1 to 3 μm (except for the TFT). The thickness of the protective film in the case of forming a protective film). The IDF wafer size may have an area of 25 mm^2 or less than 25 mm^2, preferably 0.09 mm^2 to 16 mm^2. Preferably, the protective film formed on the upper and lower sides of the TFT has a size larger than that of the IDF wafer.

Further, the substrate 10 having the provided filling layer 24 is bonded to the separation layer 16 with a layer of bonding material 15 inserted therein to complete the ID mark 20.

As the substrate 10 forming the ID mark, a resin material such as paper, synthetic paper, plastic, PET, polypropylene, polyethylene, polystyrene, and nylon, an inorganic material, or the like can be generally used. However, the substrate is not limited to this. In order to allow the ID mark to be bonded not only to the flat shaped article but also to various shapes of the article, it is preferred to use the flexible material as the marking substrate. As the resin material, for example, high density polyethylene (HDPE) as disclosed in Japanese Patent Application Laid-Open No. 2001-30403 can be used. In addition, two or more of the above materials may be combined and used.

As the conductive material for the antenna 11 and the connection pad 12, a metal such as Ag, Au, Al, Cu, Zn, Sn, Ni, Cr, Fe, Co or Ti, and an alloy which already includes the above metal may be used. Of course, the conductive material is not limited to this. However, it is preferable that aluminum can be used from the viewpoints of workability and cost. Preferably, the film has a thickness of from 5 to 60 μm.

The materials of the antenna 11 and the connection pad 12 may be different from each other. The antenna 11 and the connection pad 12 may be formed by patterning using a sputtering method after forming all of the conductive materials, or directly selectively by a droplet dropping method. The above materials may be laminated to form the antenna 11 and the connection pad 12. After the conductive pattern is formed using the above method, an electroplating method may be employed to form a conductive material that is the same as or different from the connection pattern. With the above description, the connection pad portion can be provided on one side of the TFT.

The antenna 11 and the connection pad are formed to have flexibility and ductility, and more preferably, the thickness of the film can withstand stress due to deformation. In order to be able to reliably connect the thin film integrated circuit device 13, it is preferable to form the connection pad 12 as far as possible.

For the bonding material layer 15, some well-known materials can be used, for example, a cyanoacrylate adhesive (mainly used as an instant bonding agent) which reacts with a small amount of water in the air, a vinyl acetate resin emulsion, a rubber material, Transparent, fast drying and waterproof (poly) vinyl chloride resin materials, vinyl acetate solvent materials, epoxy materials, and hot melt (hot melt) materials. Of course, the layer of the bonding material is not limited thereto as long as the material has adhesiveness. In the case where the ID mark is bonded to a product or the like and then peeled and bonded, the bonding material can be repeatedly bonded and separated, and such as "Post-it" (registered trademark) manufactured by 3M INNOVATIVE PROPERTIES and A product such as "NOTESTIX" (registered trademark) manufactured by NOPRE BUSINESS FORMS INC For example, an acrylic binder, a synthetic rubber binder, and a natural rubber binder disclosed in Japanese Patent Application Publication No. 2001-30403, Japanese Patent Publication No. 2998092, and Japanese Patent Application Publication No. Hei No. 6-299127 can be used.

As the separation layer 16, a resin material and an inorganic material including, for example, paper, synthetic paper, plastic, PET, polypropylene, polyethylene, polystyrene, and nylon can be used. However, the substrate is not limited to this Printing can be formed on the marking substrate using, for example, well known printing methods. As the thin film integrated circuit device 13, a thin film active element such as a TFT can be generally used. The following describes the special structure and its structural manufacturing method.

4A and 4B and Figs 5A and 5B show cross-sectional views of the marking substrate along the line X-Y shown in Fig. 1A. In the thin film integrated circuit device 13, a plurality of TFTs 23 are formed, and a connection wiring 21 to which the antenna 11 is connected is also formed. For the connection wiring 21, various materials can be selected. Generally used: silver (Ag), copper (Cu), gold (Au), nickel (Ni), platinum (Pt), chromium (Cr), tin (Sn), palladium (Pd), antimony (Ir), antimony (Rh), ruthenium (Ru), ruthenium (Re), tungsten (W), aluminum (Al), tantalum (Ta), indium (In), tellurium (Te), molybdenum (Mo), cadmium (Cd), zinc (Zn), iron (Fe), titanium (Ti), bismuth (Si), germanium (Ge), zirconium (Zr), barium (Ba), antimony-lead alloy, indium antimony oxide, fluorine-doped zinc oxide, carbon , graphite, glassy carbon, lithium, strontium, sodium, magnesium, potassium, calcium, strontium, manganese, zirconium, gallium, strontium, potassium silicate, such as magnesium/copper compounds, magnesium/silver compounds, magnesium/aluminum compounds, a magnesium/indium compound, an aluminum/alumina compound, and a compound such as a lithium/aluminum compound, and a halogen silver particle or a dispersed nanoparticle, indium tin oxide (ITO), or zinc oxide (ZnO) which can be used as a transparent film.), gallium-doped zinc oxide (GZO), indium oxide mixed with 2 to 20% zinc oxide, indium zinc oxide (IZO), organic indium compound, organotin compound, and ITO conductive material including cerium oxide (hereinafter It is easy to discuss what is called "ITSO"). Also, the connection wiring 21 can be formed by laminating layers composed of these materials.

In order to facilitate the connection of the antenna 11, the connection wires 21 may have a shape similar to a comb shape, or form a comb conductor, respectively.

4A and 4B, the connection wiring 21 of the thin film integrated circuit device 13 and the connection pad 12 of the marking substrate are connected by an anisotropic conductive film 22 disposed therein (hereinafter, the anisotropic conductive film is simply referred to as "ACF". "Or an anisotropic conductive paste (ACP)). In the present embodiment mode, the method of inverting and bonding the thin film integrated circuit device can be referred to as a face down method.

ACF has a structure in which a layer including a main compound of a formed bonding material, which is called a bonding layer, has a structure in which conductive particles are dispersed. Therefore, it is possible to ensure conductivity even when the thin film integrated circuit device 12 and the connection pad 12 are bonded. As discussed below, after a plurality of thin film integrated circuit devices are fabricated, the device may be separated from each other by cutting or the like, and each of the thin film integrated circuit devices may be carried by, for example, a small vacuum tweezers, so that the thin film integrated circuit device It can be bonded to the desired portion of the marking substrate.

Next, the cross-sectional structure of the antenna will be discussed. In the present embodiment mode, the case of the electromagnetic induction type and the non-contact type ID mark using the coil type antenna is discussed, as shown in Fig. 1A. For the current flowing through the antenna, when the coil antenna is close to the electromagnetic field generated by the reader/writer (hereinafter simply referred to as "R/W", not shown in the drawing), due to the electromagnetic induced current It will flow in the closed loop coil, thereby triggering the thin film integrated circuit device 13. Therefore, the thin film integrated circuit device 13 must be connected to both ends of the antenna, such as the outer end and the inner end, as shown in Fig. 1A.

In this case, in order to prevent the short circuit of the output of the antenna together, the cross wiring 18 as shown in Figs. 1A and 4A and 4B is provided to connect the thin film integrated circuit device 13 and the external end point by the contact portion 19. connection. Preferably, the contact portion 19 is provided on the marking substrate in advance. The crossover wires 18 can be formed using materials that are the same as or different from the antennas 11. The method of forming it is not limited to this. The cross wiring 18 can be formed using a method similar to an antenna.

As shown in FIG. 4B, a filler 28 may be contained in the intermediate layer film 53 of the thin film integrated circuit device 13. This makes it possible to reduce the difference in the coefficient of thermal expansion between the formation of the TFT 23 and the intermediate layer 53, and to prevent the peeling of the interlayer film 53. The discussion will be discussed in detail below.

5A and 5B show the case where the thin film integrated circuit device 13 and the marking substrate are bonded by the non-conductive bonding material layer 15, and the connection wiring 21 of the thin film integrated circuit device 13 and the connection pads 12 are directly connected to each other. For the bonding material layer 26, the above material can be used as the bonding material layer 15. For example, each thin film integrated circuit device can be bonded to a desired portion of the marking substrate by the use of a small vacuum tweezers. Also, in the case of Figs. 5A and 5B, the filler 28 is contained in the intermediate film of the TFT 23 in the thin film integrated circuit device 13.

As with the bonding method of the thin film integrated circuit device 13 and the marking substrate 10, a method different from that shown in Figs. 4A and 4B and Figs. 5A and 5B can be employed. For example, a method of using a double-sided adhesive tape and a method of forming a resin-covered thin film integrated circuit device are not shown in the drawings.

In the method of the present embodiment, since the cross-wiring 18 is exposed outside the marking substrate 10, a coating 17 for flattening the surface of the marking substrate 10 can be formed (refer to Figs. 1A, 4A and 5B). For the coating 17, a transparent resin material such as plastic, PET, polypropylene, polyethylene, polystyrene, and nylon, DLC (diamond-like carbon), or the like can be used

IPR2025-00645 Page 01686

In the present embodiment mode, an electromagnetic induction type antenna structure can be used. However, it is also possible to appropriately apply an electromagnetic coupling type of coil mutual inductance caused by an AC magnetic field, a microwave type that transmits and receives data using microwaves (2.45 GHz), and an optical communication type that updates an ID mark such as a near-infrared ray using optical space transmission. Any kind of structure. In the present embodiment mode, although two contact points are provided between the thin film integrated circuit device 13 and the antenna 11, the number of contact points is not limited to these numbers.

(Embodiment Mode 2)

The structure and manufacturing method of the ID mark according to the present invention will be discussed below mainly with reference to FIGS. 1B and 6A. 1B is a perspective view illustrating an ID mark structure in accordance with the present invention, wherein for convenience of explanation, the lower half shows the portion of the marking substrate that needs to be bonded to the article, and the upper portion shows the separating layer used as the marking plate.

1B is the same as FIG. 1A, showing the formation of the antenna 11 on the marking substrate 10 and the connection pad 12 connecting the antenna to the thin film integrated circuit device, and then bonding the separated thin film integrated circuit device 13 to the marking substrate 10. The above case, and the feature of the cross wiring 18 which forms the connection film integrated circuit device 13 and the antenna 11 inside the marking substrate 10.

In this case, an insulating layer 27 is provided in order to prevent a short circuit between the antenna 11 and the cross wiring. Further, a contact portion 19 is formed in the insulating layer 27 in order to connect the ends of the antenna 11 and the cross wiring 18. Fig. 6A shows a schematic cross-sectional view of the line X-Y shown in Fig. 1B.

For the insulating layer 27, organic resins such as polyimide, acrylic acid, polyamide, resist, and decane, and inorganic materials such as cerium oxide, cerium nitride, cerium oxynitride (including Nitrogen oxide ruthenium); includes films like DLC or carbon nitride (CN); PSG (phosphorus bismuth glass), and BPSG (boron bismuth glass). However, in order to avoid unnecessary thickening of the total thickness of the ID mark, it is preferable that the film thickness including the insulating layer 27 and the cross wiring 18 is equal to or smaller than the film thickness of the thin film integrated circuit device 13, as shown in FIG. 6A. Shown. In the present embodiment mode,

although the anisotropic conductive film 22 can be used to interconnect the thin film integrated circuit device 13 and the marking substrate 10 as shown in Figs. 4A and 4B, the method described in Fig. 5B can also be used. Other structures may be the same as those of Embodiment Mode 1.

In the present embodiment mode, since the cross wiring 18 is formed inside the marking substrate 10, it is not necessary to provide a coating layer on the surface of the marking substrate 10, so that the entire ID mark can be made thinner.

In the present embodiment mode, an antenna structure using an electromagnetic induction type is employed. However, any one of electromagnetic coupling type, microwave type, and optical communication type can also be suitably employed. The ID tag can be a hybrid ID tag that can have both a non-contact type and a contact type. In the present embodiment mode, although only two contact points are provided between the thin film integrated circuit device 13 and the antenna 11, the number of contact points is not limited to this number.

(Embodiment Mode 3)

The structure of the ID mark and the manufacturing method according to the present invention will be discussed mainly with reference to FIGS. 2A and 6B. 2A is a perspective view illustrating an ID mark structure in accordance with the present invention, wherein for convenience of explanation, the lower half shows the portion of the marking substrate that needs to be bonded to the article, and the upper portion shows the separating layer used as the marking plate.

2A is the same as FIG. 1A, showing the formation of the antenna 11 on the marking substrate 10 and the connection pad 12 connecting the antenna to the thin film integrated circuit device, and then bonding the separated thin film integrated circuit device 13 to the marking substrate 10. The above case and the feature of the cross wiring 18 which forms the connection film integrated circuit device 13 and the antenna 11 inside the thin film integrated circuit device.

The substrate forming the antenna 11 and the thin film integrated circuit device 13 may be covered with a filling layer 24 containing a filler 28. The material and shape of the filler 28 can be appropriately selected. As the material suitable for the filling layer 24, the above materials can be used. Although the filling layer 24 also has the function of protecting the thin film integrated circuit device 13 and the antenna 11, it is also possible to form a protective film of an inorganic thin film around the film. As the protective film, for example, a film including a material such as cerium oxide, cerium nitride or cerium oxynitride (cerium oxide including nitrogen) which has a function of blocking impurities such as Na element, is preferably used. More preferably, the material may be laminated to form a protective film.

Fig. 6B is a schematic cross-sectional view showing the line X-Y shown in Fig. 2A. In order to form a connection region in the region of the TFT 23 to which the inner end point and the outer end point of the antenna 11 can be connected, connection wirings 21a to 21c are provided. A cross wiring 18 is provided between the outer end point of the connection antenna 11 and the connection wiring 21a of the TFT 23. The cross wiring 18 can be formed by fabricating a region where the TFT 23 is formed, then the first intermediate layer 30a is formed, a contact hole is formed, and then the conductive material is deposited by sputtering or by dropping a conductive material by a droplet. Further, in order to prevent a short circuit between the cross wiring 18 and the antenna 11, a second intermediate layer 30b is formed, and a connection wiring 21c is formed. For the connection wirings 21a to 21c and the cross wiring 18, the above-mentioned conductive material can be suitably employed. Further, a protective film 31 may be formed on the second interlayer film 30b.

As the material of the intermediate layer (the first and second interlayer films 30a and 3b) discussed above, a photosensitive or non-photosensitive organic material such as polyimide, acrylic, polyamide, resist, and the like may be used. Benzocyclobutane, and a heat resistant organic resin such as a decane. As the manufacturing method thereof, a method such as spin coating, dipping, spraying, or droplet dripping may be employed depending on the material. Further, an SOG film obtained by coating (For example, a SiO_x film including an alkyl group) may also be used. Also, an inorganic material may be used, and in this case, it may be used including, for example, cerium oxide, cerium nitride, cerium oxynitride (cerium oxide including nitrogen), including similar DLC or carbon nitride, PSG, BPSG or oxidation Materials such as aluminum. As a method of forming the same, a method such as plasma CVD, low pressure CVD (LPCVD) or plasma under atmospheric pressure can be used. The intermediate layer films 30a and 30b may be made of the same or different materials from each other.

For the protective film 31, in addition to a silicon oxide (SiO_X) and silicon oxide ($SiO_X N_Y$) containing nitrogen, are preferred, such as the use of silicon nitride (e.g., SiN_X, Si_3N_4 or $SiNO_X$) and a material such as tantalum nitride ($SiN_X O_Y$) containing oxygen, which may have a function of blocking an alkali metal element such as an N element. Especially ID tags, ID cards, ID tags and the like are often handled directly by hand. In this case, Na penetration in human sweat can be prevented. More preferably, the above materials can be laminated. For example, SiN, a film in which two layers of SiNO and SiO_2 are sequentially laminated, a film in which three layers of SiN, TFT, and SiNO are sequentially laminated, or a film of three layers of SiON, TFT, or SiNO can be used. These laminated structures can be freely combined. Further, not only the material can be used to cover the upper and lower layers of the TFT, but also materials can be used to cover the peripheral portion. Hereinafter, a concentration of niobium oxide ($SiO_X N_Y$) containing nitrogen and niobium nitride ($SiN_X O_Y$) containing oxygen is collectively referred to as "niobium oxynitride". It is preferable to form the protective film 31 as far as possible to prevent penetration of mixed impurities, which can be omitted.

IPR2025-00645 Page 01687

in the case where the bonding material including the organic resin material is provided in contact with the protective film, the protective film using the above material can protect the TFT to avoid impurities contained in the bonding material layer. The protective film can prevent penetration of conductive materials (particularly, Cu and Ag) in the case where the formed antenna is in contact with the protective film or inside the protective film.

Although the anisotropic conductive film 22 can be connected to the thin film integrated circuit device 13 and the marking substrate 10 in the embodiment mode shown in Figs. 4A and 4B, the method shown in Fig. 5B can also be used. Other structures may be the same as in embodiment mode 1

Since the cross wiring 18 is formed in the integrated circuit device in the present embodiment mode, it is not necessary to provide a coating on the surface of the marking substrate 10 or to form a contact hole in the marking substrate 10.

In the present embodiment mode, an antenna structure using an electromagnetic induction type can be employed. However, any one of electromagnetic coupling type, microwave type, and optical communication type can also be suitably employed. The ID tag can be a hybrid ID tag that can have both a non-contact type and a contact type. In the present embodiment mode, although two contact points are provided between the thin film integrated circuit device 13 and the antenna 11, the number of contact points is not limited to this number.

(Embodiment Mode 4)

The structure and manufacturing method of the ID mark according to the present invention will be discussed below mainly with reference to FIGS. 2B and 7A. Figure 2B is a perspective view illustrating the ID mark structure in accordance with the present invention, wherein the upper portion shows the portion of the marking substrate that needs to be bonded to the article, and the lower portion shows the separation layer used as the marking plate.

The present embodiment mode is characterized in that an antenna 11 and a connection pad as a connection portion connecting the antenna and the thin film integrated circuit device on the internal substrate 32 (insertion substrate) are formed in advance, and the thin film integrated circuit to be separated is formed. The device 13 is bonded to the inner substrate 32 and bonded to the marking substrate 10.

As a method of disposing the antenna 11 and the thin film integrated circuit device 13 on the internal substrate 32, a method similar to that employed in the case of the marking substrate in the embodiment mode discussed above (refer to Figs. 4A to 6B) can be employed. However, in order to prevent the total thickness of the ID mark from being thickened, it is preferable to use the film substrate as the inner substrate 32. As the material thereof, a resin material such as paper, synthetic paper, plastic, PET, polypropylene, polyethylene, polystyrene, and nylon, and an inorganic material can be used. However, the inner substrate 32 is not limited thereto. In order to allow the ID mark to be bonded not only to a flat shaped article but also to articles of various shapes, it is preferred to use a flexible material as the inner substrate. This makes it easier to handle ID tags. As the resin material, for example, high density polyethylene (HDPE) as discussed in Japanese Patent Application Laid-Open No. 2001-30403 can also be used.

Fig. 7A is an enlarged cross-sectional view showing the finished product of the ID mark manufactured according to the mode of the present embodiment. An antenna 11 and a thin film integrated circuit device 13 are formed around the inner substrate 32, and are covered with a filling layer 24 containing a filler 28. The material and shape of the filling layer 24 can be appropriately selected. For example, a cylindrical filler can be used. As the material of the filling layer 24, the above materials can be used. Although the filling layer 24 can also be used as a film for protecting the thin film integrated circuit device 13 and the antenna 11, a protective film of an inorganic thin film can be separately formed around it. As the protective film, for example, a film of a material such as cerium oxide, cerium nitride or cerium oxynitride (including cerium oxide of nitrogen), which has a function of blocking impurities such as Na element, is preferably used. More preferably, the material may be laminated to form a protective film.

The separately formed inner substrate 32 may be bonded to the marking substrate 10 with a layer of bonding material 15 therebetween. On the surface of the marking substrate 10 (printing surface 33), printing can be performed as needed. In the present embodiment mode, since the size of the inner substrate 32 is smaller than the size of the marking substrate 10, the bonding material layer 15 may be formed on one side of the inner substrate 32, so that the separation layer 16, the inner substrate 32, and the marking substrate 10 may be bonded together.

In the case where the ID mark is actually bonded to the article or the like, the marking substrate separated from the separation layer 16 by the bonding material layer 15 may be bonded, and the substrate 32 and the marking substrate 10 may have substantially the same size, and may be on the inner substrate. A layer of bonding material is provided on both the upper and lower sides of 32 to facilitate bonding of the marking substrate 10 and the separation layer 16. The shape of the inner base 32 and the antenna 11 is not limited to the shape shown in Fig. 7A.

In the present embodiment mode, an antenna structure using an electromagnetic induction type can be employed. However, any one of electromagnetic coupling type, microwave type, and optical communication type can also be suitably employed. The ID tag can be a hybrid ID tag that can have both a non-contact type and a contact type. In the present embodiment mode, although only two contact points are provided between the thin film integrated circuit device 13 and the antenna 11, the number of contact points is not limited to this number.

(Embodiment Mode 5)

The structure and manufacturing method of the ID card according to the present invention will be discussed below mainly with reference to Figs. 3A and 3B and Fig. 7B. 3A and 3B are perspective views illustrating the structure of an ID card in accordance with the present invention.

3A shows the case where the antenna 11 and the connection pad 12 connecting the antenna 11 and the thin film integrated circuit device are respectively formed on the lower substrate 37b suitable for the ID card, and the surface area circuit device formed separately is bonded to the lower surface. On the card substrate 37b. Further, the upper card substrate 37a is disposed on the lower card substrate 37b with the filling layer 24 inserted therein. Printing is performed as needed on the upper card substrate 37a or the lower card substrate 37b. In the case where the cross-wiring 18 for connecting the connection pad 12 and the antenna 11 is exposed on the surface of the lower card substrate 37b, the coating layer 17 can be formed separately.

For each card substrate, a resin material such as plastic, PET, polypropylene, polyethylene, polystyrene, and nylon can be used. However, materials such as paper, synthetic paper, and inorganic materials can also be used. Usually, there is no chance that the ID card will be folded. However, in the case where it is necessary to fold the ID card, it is preferable to use a flexible material as the card substrate. As the resin material, for example, high density polyethylene (HDPE) as discussed in Japanese Patent Application Laid-Open No. 2001-30403 can also be used. Also, a combination of two or more of the above materials may be used.

An antenna structure including a cross wiring as shown in Embodiment Modes 1 to 4 and a method of connecting the thin film integrated circuit device and the antenna can be employed. Thus, the ID card 41 is completed. The shape of the inner base 32 and the antenna 11 is not limited to the shape shown in Fig. 7C.

Fig. 3B shows another case where the antenna and the bonded integrated circuit device 13 are formed on the inner substrate 32, and the filling layer 24 provided around the inner substrate 32 is used so that the upper card substrate 37a and the lower card substrate 37b can encapsulate the inner substrate. 32. When the inner substrate 32 is made smaller than the card substrate (the upper card substrate 37a and the lower card substrate 37b), a layer of bonding material may be provided around the inner

is made smaller than the card substrate (the upper card substrate 37a and the lower card substrate 37b), a layer of bonding material may be provided around the inner substrate 32 so that the ID card can be made thinner.

Fig. 7B is an enlarged cross-sectional view showing the finished product of the ID card manufactured according to the mode of the present embodiment. The antenna 11 and the thin film integrated circuit device 12 are formed around the inner substrate 32, and covered with a protective film 54, in which the above material can be used as the protective film 54.

Further, the inner substrate 32 covered with the protective film 54 may be covered with a filling layer 24 including a filler 28. As the material of the filling layer 24 and the filler 28, the above materials can be used. The filling layer 24 may be formed before the protective film 54 is formed.

The separately formed inner substrate 32 can be held by the upper card substrate 37a and the lower card substrate 37b having the protective film 54 and the filling layer 24 forming the ID card, thereby completing the ID card. On the surface of the card substrate (printing surface 39), printing 14 can be performed as needed

In the present embodiment mode, an antenna structure using an electromagnetic induction type can be employed. However, any one of electromagnetic coupling type, microwave type, and optical communication type can also be suitably employed. The ID tag can be a hybrid ID tag that can have both a non-contact type and a contact type. In the present embodiment mode, although only two contact points are provided between the thin film integrated circuit device 13 and the antenna 11, the number of contact points is not limited to this number.

(Embodiment Mode 6)

The structure and manufacturing method of the ID tag according to the present invention will be discussed below mainly with reference to FIG. 7C. 7C shows that the inner substrate 32 forming the antenna 11 and the bonded thin film integrated circuit device 13 may be packaged with a filling layer 24 including a filler 28. As the inner substrate 32, the filler 28, and the filling layer 24, the above materials can be employed. After the filling layer 24 is formed, it can be pressed as needed to obtain a flatness. In the case where the ID tag is placed at a position that is not visible from the outside, for example, by embedding the ID tag in other entities, the flat processing steps can be omitted. The periphery of the filling layer 24 may be covered with a protective film including an inorganic material or a substrate such as a pulp material (for example, paper or synthetic paper) or a resin. The substrate can be suitably selected to suit a variety of purposes, such as baggage tags, price tags, name tags, and brand tags. The shape of the inner base 32 and the antenna 11 is not limited to the shape shown in Fig. 7C.

In the present embodiment mode, an antenna structure using an electromagnetic induction type can be employed. However, any one of electromagnetic coupling type, microwave type, and optical communication type can also be suitably employed. The ID tag can be a hybrid ID tag that can have both a non-contact type and a contact type. In the present embodiment mode, although only two contact points are provided between the thin film integrated circuit device 13 and the antenna 11, the number of contact points is not limited to this number.

(Embodiment Mode 7)

The structure, manufacturing method and ID card of the ID card according to the present invention will be discussed below mainly with reference to Figs. 8A and 8B and Figs. 9A and 9B. Figure 8A is a perspective view illustrating an ID mark structure in accordance with the present invention, wherein the upper portion shows the portion of the marking substrate that needs to be bonded to the article, and the lower portion shows the separation layer used as the marking plate.

Fig. 8A shows a case where, in the ID mark 49, the antenna integrated thin film integrated circuit device 46 (hereinafter referred to as "antenna integrated IDF wafer") in which the antenna 47 and the thin film integrated circuit device 48 are integrated is used, including a filler. The filling layer 42 of 48 is covered and bonded to the separation layer 16 with a layer 15 of bonding material inserted therein. The marking substrate 10, the bonding material layer 15, the separation layer 16, the filler 28, and the filling layer 24 are all based on the above embodiment modes. The shape of the IDF wafer and the antenna is not limited to the shape shown in Fig. 8A. The filling layer 24 including the filler 28 may be formed only above and below the antenna integrated film integrated circuit device 46.

8B shows that in the ID mark 41, the antenna integrated thin film integrated circuit device 46 (in which the antenna 47 and the thin film integrated circuit device 48 are integrated) is covered with a filling layer 42 including a filler 48, and is employed. A layer of bonding material 15 (not shown) inserted therein is bonded to the upper card substrate 37a and the lower card substrate 37b. Both the card substrate 10 and the bonding material layer 15 are based on the above embodiment mode. The shape of the IDF wafer and the antenna is not limited to the shape shown in Fig. 8B. The filling layer 24 including the filler 28 may be formed only above and below the antenna integrated film integrated circuit device 46.

9A and 9B are cross-sectional views showing the antenna integrated IDF wafer (only the antenna integrated thin film integrated circuit device 46) along the ID mark 49 and the ID card 41 of the line X-Y shown in Figs. 8A and 8B. The case shown in Fig. 9A is that the island-shaped semiconductor film 57 and the gate insulating film 58 are formed on the protective film 55, and then the gate electrode 56 (which is a two-layer structure) and the cross wiring 52 are simultaneously formed. Further, an antenna 47, a wiring 51a for interconnecting the TFT and the antenna, and a wiring 51b for interconnecting the TFTs are formed by the contact holes formed in the passivation film 59 and the interlayer film 53. Preferably, the gate electrode 56, the crossover line 52, the antenna 47, and the wirings 51a and 51b are fabricated in the same processing technique, which may be formed in stages.

Fig. 9B shows a case where the island-shaped semiconductor film 57 and the gate insulating film 58 are formed on the protective film 55, and then the gate electrode 56 (which is a two-layer structure) and the antenna 47 are simultaneously formed. Further, by the intermediate layer film 53, wirings 51a for connecting TFTs and antennas, cross wirings 52, and wirings 51b for interconnecting TFTs are formed. Preferably, the gate electrode 56, the crossover line 52, the antenna 47, and the wirings 51a and 51b are fabricated in the same processing technique, which may be formed in stages.

In FIGS. 9A and 9B, the filling layer 28 may also be mixed in the interlayer film 53. However, the filler 28 in the interlayer film 53 can be omitted. Although the TFT employs an upper gate structure, a lower gate structure can also be used. A special method suitable for manufacturing TFTs will be discussed below. In order to prevent the impurities from diffusing into the island-shaped semiconductor film 57, it is preferable to form the protective film 55 of a single layer structure or a laminated structure. Further, it is preferable that the protective film 54 may be formed after the antenna 47 is formed. The protective films 54 and 55 may be made of a material such as tantalum nitride, hafnium oxide or hafnium oxynitride, and preferably include tantalum nitride which can block impurities such as Na.

The antenna integrated thin film integrated circuit device 46 in this embodiment mode can be mounted on the ID tag as in the example shown in Fig. 7C.

This embodiment mode shows an example of a structure in which a TFT and an antenna are integrally formed, but is not always limited thereto.

(Embodiment Mode 8)

The method of manufacturing the ID mark according to the present invention will be discussed below mainly with reference to Figs. 10A and 10B.

10A and 10B are diagrams illustrating a manufacturing line of ID marks in accordance with the present invention. First, the label paper for the ID mark substrate is supplied from the label paper supply mechanism 300 (small wheel 1), and the IDF wafer (thin film integrated circuit device) is bonded to a desired portion in the label paper. In this case, a material such as a bonding material or ACF or a method such as ultraviolet bonding or UV bonding may be suitably used. In this embodiment mode, it is envisaged to form an antenna on the marking paper, and using the ACF supply mechanism 301 and the IDF wafer bonding mechanism 302, the marking carton IDF

IPR2025-00645 Page 01689

wafer can be placed in which the ACF is bonded together, of course, formed on the marking paper. The antenna and IDF wafer are interconnected. In addition to the ACF supply mechanism 301, a supply mechanism for the non-conductive bonding material can be provided. Thereby the manufactured ID mark can have a structure as shown in FIG. 5B.

Next, the filling layer and the bonding material layer are respectively provided by the filling layer supply mechanism 308 and the bonding material layer supply mechanism 303, and bonded to the separable paper (separation layer) provided by the separation paper supply mechanism 304 (small wheel 2). On, to complete the ID tag. Finally, the ID tag can be picked up by the tag picking mechanism 305 (mini wheel 3). The ID mark substrate is preferably separated in advance to form separate marks, and it is preferred to provide strip paper as the separation paper. In this case, the ID marks 20 separated from each other can be obtained on the drum marking the main board 118 (separation layer) as shown in Fig. 24A.

For the provision of the marking paper and the provision of the separating paper, the order can also be reversed, as shown in Fig. 10B. In the drawing, since it is assumed that an antenna is formed on an IDF wafer, the ACF supply mechanism 301 or the non-conductive bonding material supply mechanism may be omitted. After the plurality of ID marks of the strip shape are formed, the mark separation mechanism 306 such as a knife can be used to separate the ID marks, thereby forming the respective separated ID marks, and then the ID mark can be collected by the collecting mechanism 307. As a product. Of course, Figures 10A and 10B can also be combined.

The method according to the mode of the present embodiment can be suitably applied not only to the ID card and the ID tag according to the present invention, but also to banknotes, coins, credit cards, tickets, and securities that are combined with the thin film integrated circuit device. For example, in the case of an ID card, the lower base material and the upper base material may be held by the small wheel 1 and the small wheel 2, respectively.

(Embodiment Mode 9)

The structure and manufacturing method of the ID card and the ID tag according to the present invention will be discussed below mainly with reference to Figs. 11A and 11B. 11A and 11B are enlarged views showing a pattern of a manufacturing line of an ID card and an ID tag according to the present invention, and a completed product.

First, as shown in Fig. 11A, the label paper for the ID mark substrate is provided by the label paper supply mechanism 300 (small wheel 1), and the IDF wafer is bonded to the desired position of the substrate using the IDF wafer bonding mechanism 302. In this case, a material such as a bonding material or ACF or a method such as ultraviolet bonding or UV bonding may be suitably used. Next, when the substrate is disposed in a strip form, the substrate separating mechanism 309 can be used to separate the substrate with respect to each individual ID card or ID tag. Subsequently, a lamination system 310 is used to perform a lamination process on the periphery of the individual substrates. In this case, it is preferable that the periphery of the IDF wafer is covered with the filling layer 24 containing the filler 28 in advance. A filler 28 may be included in the laminated resin layer 45.

In this way, the ID card or ID tag is completed. After forming the IDF wafer at the desired location of the strip substrate and performing the lamination process, the substrate can be separated relative to each ID card or ID tag. The ID card or ID tag after the cascading process can be collected by the collecting mechanism 307.

Figure 11B is an enlarged cross-sectional view showing the finished product of the ID card or ID tag manufactured by the method according to the mode of the present embodiment. In the marking substrate, the antenna 11 and the thin film integrated circuit device 13 to which the antenna 11 is connected are formed, and the laminated resin layer 45 having the filling layer 24 filled therein is used to cover the antenna 11 and the thin film product which have been formed. The marking substrate of the bulk circuit device 13. In order to protect the thin film integrated circuit device 13 and the antenna 11 in the heat treatment of the lamination process or the like, it is preferable that the filling layer 24 uses a heat resistant organic resin such as decane. Further, a protective film may be separately formed. As the protective film, a film including carbon such as DLC or carbon nitride, a carbon nitride film, and a carbon nitride film containing oxygen can be used, however, the protective film is not limited thereto. As a method of forming the same, a method such as plasma CVD or atmospheric pressure plasma can be used.

This manufacturing process technology can be applied not only to ID cards and ID tags, but also to other products, as long as the products are applied to the cascading process technology.

(Example 1)

In the present embodiment, a special manufacturing method of the thin film integrated circuit device will be discussed with reference to FIGS. 12A to 16B. For the sake of simplicity, the cross-sectional structure of the memory of the CPU and the TFT using the n-channel TFT and the p-channel can be discussed. This manufacturing method.

First, a peeling layer 61 is formed on the substrate 60 (Fig. 12A). Here, a thickness of 50 μm (500) is formed on a glass substrate (for example, a Corning 1737 substrate) by CVD. a-Si (amorphous germanium) film. As the substrate, in addition to the glass substrate, a substrate such as a quartz substrate, a substrate including an insulating material such as alumina, a germanium wafer substrate, and a heat resistant plastic substrate capable of withstanding the processing temperature of subsequent processing may be used.

As the release layer, in addition to the amorphous germanium, a layer including germanium as its main component, for example, polycrystalline germanium, single crystal germanium or SAS (semi-amorphous germanium (also referred to as microcrystalline germanium)) may be used. These release layers are formed by sputtering instead of CVD. Preferably, the release layer has a film thickness of 500 to 540 . As SAS, high film thickness is 300 to 500 .

Next, a protective film 55 (which may also be referred to as a base film or a base insulating film) is formed on the peeling layer 61 (FIG. 12A). Although a three-layer structure in which a SiON film having a film thickness of 100 nm, a SiNO film having a film thickness of 50 nm, and a SiON film having a film thickness of 100 nm are sequentially laminated on a substrate may be employed herein, the material, film thickness, or number of layers is not limited thereto. For example, instead of the underlying SiON film, a thermal resistance resin such as decane having a film thickness of 0.5 to 3 μm may be formed by spin coating, dicing coating or droplet dropping. In addition, a tantalum nitride film (for example, SiN or Si_3N4) can be used. Preferably, each layer has a film thickness of 0.05 to 3 μm and can be conveniently selected in the above range.

A cerium oxide film is formed by a mixed gas such as SiH_4/O_2 or TEOS (tetraethoxy decane) / O_2 by a method such as thermal CVD, plasma CVD, atmospheric CVD or offset ECRCVD. The tantalum nitride film can be generally formed by plasma CVD using a SiH_4/NH_3 mixed gas. The SiON film or the SiNO film can be generally formed by plasma CVD using a SiH_4/N_2O mixed gas.

In the case of using a material including ruthenium such as a-Si as the main component as the material of the peeling layer 61 and the island-shaped semiconductor film 57 formed as a protective film in contact therewith, it can be used from the viewpoint of ensuring adhesion. SiO_XN_Y .

Next, a TFT for forming a CPU and a memory of the thin film integrated circuit device is formed on the protective film 55. In addition to the TFT, a thin film active element such as an organic TFT and a thin film diode can also be formed.

In the method of manufacturing a TFT, an island-shaped semiconductor thin film 57 is first formed on the protective film 55 (Fig. 12B). The island-shaped semiconductor thin film 57 can be formed using an amorphous semiconductor, a crystalline semiconductor or a semi-amorphous semiconductor. In any case, it is possible to use a

thin film 57 can be formed using an amorphous semiconductor, a crystalline semiconductor, or a semi-amorphous semiconductor. In any case, it is possible to use a semiconductor film including a material such as germanium or germanium-tellurium (SiGe) as a main component.

In the present embodiment, an amorphous germanium having a film thickness of 70 nm was formed, and a surface containing amorphous nickel was treated with a solution containing nickel. Further, a crystalline germanium semiconductor thin film is obtained by a thermal crystallization treatment method at a temperature of 500 to 750 ° C, and laser crystallization is performed to increase the degree of crystallization. As a method of deposition, a method such as plasma CVD, sputtering, or LDCVD can be used. As a method of crystallization, thermal crystallization such as laser crystallization, thermal crystallization, or using other catalysts (for example, Fe, Ru, Rh, Pd, Os, Ir, Pt, Cu, or Au) may be used, or The above method is alternately used several times.

For the crystallization of a semiconductor film using an amorphous structure, a continuous wave laser can be used. In order to obtain large crystal grains by crystallization, it is preferred to use a continuous wave solid laser and to use the second to fourth harmonics in the fundamental wave (in this case, crystallization is called "CWLC"). In general, a secondary (532 nm) harmonic or a tertiary (355 nm) harmonic of a Nd:YVO $_4$ laser (the fundamental is 1064 nm) can be used. In the case of continuous wave lasers, the laser emitted by a continuous wave YVO $_4$ laser (10 W output power) can be converted to harmonics using nonlinear optical components. Still another method is to place a crystal of a YVO $_4$ crystal and a GdVO $_4$ crystal with a nonlinear optical element in a resonator to emit a harmonic. Subsequently, it is preferred to form a rectangular or elliptical laser beam on the surface radiated by the optical system to radiate the object to be processed. In this case, the required laser energy is about 0.01 to 100 MW/cm ^{2} (preferably, 0.1 to 10 MW/cm ^{2}). The semiconductor film can be moved relative to the laser beam at a speed of about 10 to 2000 cm/s.

In the case of using a pulse oscillating laser, a frequency bandwidth of several tens to several hundreds Hz can generally be used. However, it is also possible to use a pulse oscillating laser having an oscillation frequency of 10 MHz or higher, which is a higher frequency bandwidth (in this case, crystallization can be referred to as "MHz LC"). Since the time from the start of the radiation semiconductor film using the pulsed laser beam to the completion of the solidification of the semiconductor film is said to be several tens to several hundreds of nanoseconds, the use of the above higher frequency bandwidth allows the use of a laser by the next laser. The pulse causes the semiconductor film to change from melting to solidification. Therefore, the solid-liquid interface can continuously move the semiconductor film, and unlike the case of using a conventional pulse oscillation laser, the formed semiconductor film has grain growth which can continuously move toward the scanning direction. In particular, the grain production mechanism has a width in the scanning direction of about 10 to 30 μm and a width in the scanning direction of about 1 to 5 μm. The formation of the single crystal grains extending in the scanning direction makes it possible to form a semiconductor thin film in which there is almost no grain boundary in the channel direction of at least one of the TFTs.

In the case where a heat-resistant organic resin such as decane is used as the partial protective film 55, heat can be prevented from leaking from the semiconductor film during the above crystallization, so that effective crystallization can be performed.

According to the method discussed above, a crystalline germanium semiconductor thin film can be obtained. Preferably, the crystal can be oriented in the source-channel-dip diode direction, and the formed film has a thickness of 20 to 200 μm (typically, 40 to 170 μm, more preferably 50 to 150 μm). Thereafter, an oxide film inserted therein is formed on the semiconductor film to form an amorphous germanium film which can absorb the metal catalyst, and the absorption is performed by heat treatment at 500 to 750 °C. Further, in order to be able to control the threshold voltage of the TFT, boron ions of the order of 10 ^{13} /cm ^{2} may be implanted into the crystalline germanium film. Thereafter, etching is performed using a resist as a mask to form an island-shaped semiconductor thin film 57.

When a crystalline semiconductor thin film is formed, acetylene (Si $_2$ H $_6$) and germanium tetrafluoride (GeF $_4$) can be used as a raw gas for directly forming a polycrystalline germanium semiconductor thin film by LPCVD, whereby a crystalline semiconductor thin film can be obtained. In this case, the gas flow rate may be set to Si $_2$ H $_6$ /GeF $_4$ =20/0.9, the deposition temperature may be set to 400 to 500 ° C, and a He or Ar carrier gas may be used. However, this condition is not limited to this.

Preferably, the TFT channel region, especially the incorporation of $^1 \times 10^{19}$ to 1×10^{22} cm $^{-3}$ hydrogen or halogen, preferably is, $^1 \times 10^{19}$ to 5×10^{20} cm $^{-3}$, or in the case of SAS is 1×10^{19} to 2×10^{21} cm $^{-3}$. In any case, it may include more than the amount of hydrogen or halogen contained in the single crystal used as the IC wafer. Thus, even if local fracture occurs in the TFT, it is possible to terminate such partial fracture by hydrogen or halogen.

Next, a gate insulating film 58 is formed on the island-shaped semiconductor film 57 (Fig. 12B). Preferably, a single layer or a laminated layer structure formed by a method of forming a thin film such as plasma CVD or sputtering may be employed as the gate insulating film, and these layers may include tantalum nitride, hafnium oxide, Niobium nitride containing oxygen or niobium oxynitride (ruthenium oxide containing nitrogen). In the case of lamination, for example, it is preferable to use a three-layer film structure made of a ceria film, a tantalum nitride film, and a ceria film on one side of the substrate.

Next, the gate electrode 56 is formed (Fig. 12C). In the present embodiment mode, the gate electrode 56 can be formed by laminating using the resist 62 as a mask and forming Si and W (tungsten) by sputtering. Of course, the material, structure or manufacturing method of the gate electrode 56 is not limited thereto, and it can be appropriately selected. For example, a laminated structure of NiSi (nickel germanium) laminated structure or TaN (tantalum nitride) and W doped with or without n-type impurities may be employed. Additionally, a variety of different electrically conductive materials can be used to form the single layer gate electrode 56.

A resist mask such as SiO $_x$ may also be used instead of the resist mask 62. In this case, it is necessary to increase the processing technique of forming a mask such as SiO $_X$ or SiON (referred to as a hard mask) by patterning. However, since the mask is less reduced than the resist during the etching process, a gate electrode layer of a desired width can be formed. Further, the resist 62 is not used, and the gate electrode 56 can be selectively formed by a droplet dropping method.

As the conductive material, various materials can be selected depending on the function of the conductive film. In the case where the gate electrode and the antenna are simultaneously formed, the material can be selected in consideration of their functions.

As the etching gas in the case where the gate electrode is formed by etching, a mixed gas of CF $_4$, Cl $_2$ and O $_2$ or a Cl $_2$ gas can be used. However, the etching gas is not limited to this.

Next, the portion to be the p-channel TFTs 70 and 72 is covered with the resist 63, and the island-shaped semiconductor film of the portions of the TFTs 69 and 71 where the n-channels are to be formed is doped at a lower concentration using the gate electrode layer as a mask. An impurity element 64 (typically, P (phosphorus) or As (arsenic)) which affects n-type conductivity (first doping treatment technique shown in Fig. 12D) is incorporated. The conditions of the first doping treatment are: dose: 1×10^{13} to 6×10^{13} /cm ^{2} , acceleration voltage. 50 to 70 KeV. However, this condition is not limited to this. The first doping treatment is doped by the gate insulating film 58 to form a pair of lower concentration impurity regions 65. The first doping process can be applied to all regions where the p-channel TFT region is not covered with a resist.

Next, after the resist 63 is removed by a method such as ashing, a new resist 66 is formed to cover the n-channel TFT region, and a gate electrode is used for the island-shaped semiconductor film in which the p-channel TFTs 70 and 72 are to be formed. The electrode layer is used as a mask to incorporate an impurity element 67 (typically B (boron)) which affects p-type conductivity at a higher concentration (second doping treatment technique shown in Fig. 12E). The second doping treatment

IPR2025-00645 Page 01691

conditions that dosage: 1×10^{16} to $3 \times 10^{16}/cm^2$; acceleration voltage: 20 to 40KeV. The second doping treatment is doped by the gate insulating film 58 to form a pair of higher concentration P-type impurity regions 68.

Next, after the resist 66 is removed by a method such as ashing, an insulating film 75 is formed on the substrate (Fig. 13A). In this embodiment mode, plasma CVD can be used to form a SiO_2 film having a film thickness of 100 nm. Thereafter, the entire area of the substrate is covered by the resist 44, and the resist 44, the insulating film 75, and the gate insulating film 58 are etched by self-alignment, and the sidewalls 76 (side walls) are formed by etch back removal (Figure 13B). As the etching gas, a mixed gas of CHF_3 and He can be used. The processing technique for forming the sidewalls is not limited to the processing method shown in the embodiment mode.

In the case where the insulating film 75 is formed and an insulating film is also formed on the back surface of the substrate, the insulating film (back surface treatment) on the back surface can be etched and removed using the resist 44 as a mask.

The method of forming the side walls 76 is not limited to the above method. For example, the methods shown in Figures 16A and 16B can be used. Fig. 16A shows an example of an insulating film having a two-layer or multi-layer laminated structure. For example, for the insulating film 75, a two-layer structure of SiNO (yttrium oxynitride) having a film thickness of 100 nm and an LTO film (low-temperature oxide film) having a film thickness of 200 nm can be used, wherein a plasma CVD can be used to form a SiON film. And low pressure CVD can be used to form SiO_2 as an LTO film. Thereafter, the L-shaped and circular side walls 76 can be formed by etch back by using the resist 44 as a mask.

Fig. 16B shows an example in which the gate insulating film 58 is left by etching by etch back. The insulating film 75 in this case may have a single layer structure or a laminated structure.

When subsequently doped with a higher concentration of n-type impurities, the sidewalls 76 may have a function as a mask for forming a lower concentration impurity region or a non-doped bias region lower than the sidewall 76. In any of the above methods of forming the sidewalls, the etching conditions may be appropriately changed depending on the width of the desired lower concentration impurity region or the bias region.

Next, a new resist 77 is formed to cover the p-channel TFT region, and the gate electrode layer 56 and the sidewall 76 are used as a mask, and an impurity element 78 (typically, P or As) which affects n-type conductivity is employed. A higher concentration of doping is performed (the third doping treatment technique shown in Fig. 13C). The third doping treatment can be carried out under the following conditions: dose: 1×10^{13} to $5 \times 10^{15}/cm^2$; acceleration voltage: 60 to 100 KeV. The third doping treatment is doped by the gate insulating film 58 to form a pair of higher concentration n-type impurity regions 79.

After the resist 77 is removed by a method such as ashing, the impurity region can be thermally excited. For example, after forming a 50 nm SiON film, heat treatment at a temperature of 500 ° C for 4 hours is performed under a nitrogen atmosphere. Further, after forming a thin SiNx thin film containing 100 nm of hydrogen, a heat treatment at 410 ° C for 1 hour under a nitrogen atmosphere may be performed to improve defects of the crystalline semiconductor film. This is a treatment, for example, for terminating the existing dangling bonds in the crystal crucible, and is referred to as a hydrotreating technique. Further, thereafter, a SiNO film having a film thickness of 600 nm was formed as a cap-shaped insulating film for protecting the TFT. The hydrotreating process can be carried out after the formation of the SiON film. In this case, a SiON film can be continuously formed on the SiN_X film. Thus, a three-layer insulating film composed of a base SiON, SiN_X, or SiON can be formed on the TFT. However, the structure or material of the insulating film is not limited thereto. Preferably, these insulating films are formed to have a function of protecting the TFTs.

Next, an interlayer film 53 is formed on the TFT (Fig. 13D). As the intermediate layer film 53, an epoxy, a polyimide, an acrylic, a polyamide, and a heat-resistant organic resin such as a decane can be used. As a method of forming the same, a method such as spin coating, dipping, spraying or droplet dripping may be employed depending on the material. Also, an inorganic material may be used, and in this case, a film including a material such as cerium oxide, cerium nitride, cerium oxynitride, PSG, BPSG, or aluminum may be used. These insulating films may be laminated to form the interlayer film 53.

Further, a protective film 54 may be formed on the interlayer film 53. As the protective film 54, a film including carbon such as DLC or carbon nitride, or a film such as a ceria film, or a tantalum nitride film containing oxygen can be used. As a method of forming the same, a method such as a plasma CVD or an atmospheric pressure power system can be used. Further, photosensitive or non-photosensitive organic materials such as polyimine, acrylic acid, polyamide, resin, and benzocyclobutane, and a heat-resistant organic resin such as decane may be used.

In order to avoid peeling and peeling of the interlayer film 53 and the protective film 54 due to stress generated by a difference in thermal expansion coefficient between the interlayer film 53 or the protective film 54 and a material such as a conductive material to be subsequently formed, it is possible to The filler is mixed in the intermediate layer film 53 or the protective film 54.

Next, after the resist is formed, a contact hole is formed by etching, and then a wiring 51 for connecting the TFTs and a connection wiring 21 for connecting the external antenna are formed (Fig. 13D). As the etching gas used for forming the contact hole, a mixed gas of CHF_3 and He can be used. However, the gas used for etching is not limited thereto. The wiring 51 and the connection wiring 21 may be simultaneously formed using the same material, or may be separately formed. The wiring 51 connected to the TFT may have a five-layer structure formed of Ti, TiN, Al-Si, Ti, and TiN, which may be formed by patterning after forming a thin film by a sputtering method.

By mixing Si in the Al layer, it is possible to prevent pinholes generated in the resist baking of the wiring pattern. Approximately 0.5% of copper (Cu) may be mixed to replace Si. Further, by sandwiching the Al-Si layer between Ti and TiN, the performance of the pinhole prevention can be further improved. In the patterning process, it is preferred to use the above-described hard mask containing a material such as SiON. The material of the wiring and the method of forming are not limited thereto. The above materials used as the gate insulating layer can be used.

The present embodiment shows the case where the integration forms only the TFT regions which form the CPU 73 and the memory 74 or the like and is connected to the antenna. However, the present invention can also be applied to the case of integrating the formation of a TFT region and an antenna. In this case, it is preferable to form an antenna on the interlayer film 53 and the protective film 54, and it is also possible to cover with another protective film. As the conductive material for the antenna, an alloy such as Ag, Au, Al, Cu, Zn, Sn, Ni, Cr, Fe, Co or Ti, or a metal may be used. However, the material is not limited to this. The wiring and the antennas may be different materials from each other. The wiring and the antenna can be formed to have a ductile and flexible metal material, and more preferably, the film is formed to withstand the stress due to the deformation.

As a method of forming the same, patterning can be performed using a resist mask after the entire surface deposition is performed by a sputtering method or by selecting a nozzle using a droplet dropping method. The wiring and the antenna can be formed at the same time, or they can be formed in advance, and then another one is formed on the sample.

After the above processing technique is employed, a thin film integrated circuit device including a TFT is completed. Although the structure of the upper gate is employed in the embodiment mode, the structure of the lower gate (reverse step structure), the material of the base insulating film, the interlayer insulating film, and the wiring may be mainly provided without such as TFT. Preferably, in the region of the thin film active device, the region can occupy 50% or more of the entire thin film integrated circuit device. More preferably, it occupies 70% to 95%. This makes it easier to form a folded IDF wafer and process a finished product such as an ID tag. In this case, it is

IPR2025-00645 Page 01692

preferable that the island-shaped semiconductor region (island shape) including the active elements of the TFT portion may occupy 1 to 30% of the entire thin film integrated circuit device, and more preferably, occupy 5% to 15 %.

Further, as shown in Fig. 13D, it is preferable that the thickness of the upper and lower protective films of the intermediate layer film can be controlled so that the distance from the semiconductor layer of the TFT to the lower protective film in the thin film integrated circuit device (t_{under}) and the distance (t_{over}) from the semiconductor layer to the upper interlayer film (the protective film in the case of forming the protective film) are equal or substantially equal to each other. By employing this method, a semiconductor layer is provided in the middle of the thin film integrated circuit device, so that stress on the semiconductor layer can be eliminated, and the generated cracking can be avoided.

The TFT fabricated according to the present embodiment has an S value (sub-critical value) equal to or less than 0.35 V/dec (preferably, 0.07 to 0.25 V/dec) and a mobility equal to or greater than 10 cm^2 V/sec. And also having a characteristic equal to or greater than 1 MHz (on 3 to 5 V) at the ring oscillator level, preferably 10 MHz or higher or having a frequency equal to or greater than 100 KHz, preferably equal to or greater than 1 MHz (at Each gate frequency characteristic of 3 to 5V).

In the case where a plurality of TFTs, protective films, various wirings, and antennas are integrated on the substrate 60 (which may also be referred to as a "thin film integrated circuit device"), an antenna (FIG. 14A) is formed, and then the film can be integrated. A groove 81 is formed in the boundary region between the circuit devices 13 by a diamond wheel dicing method (Fig. 14B). In this case, a method of dicing the blade using a diamond wheel dicing system (a dicing machine) can be generally employed. The blade is a diamond-grinding millstone having a width of about 30 to 50 μm. By rapidly moving the blade, the thin film integrated circuit devices can be separated from each other. The area required for the diamond wheel may be referred to as a street, and it is preferable to have a width of 80 to 150 μm in view of damage to the device.

In addition to using a diamond wheel dicing machine, the grooves 81 may be formed using a method such as scribing or etching using a mask. In the case of scribing, there may be a diamond scribing and a laser scribing. In the case of using a laser scribing line, for example, a resonator using a Nd:YAG laser, 200 to a pulse resonance such as a fundamental wave having a resonance wavelength of 1064 nm or a second harmonic resonance wavelength of 532 nm can be used. Linear laser beam of 300W power.

In the case of performing etching, after the mask pattern is formed in accordance with the processes of exposure and development, the device can be formed by each other by an etching method such as dry etching. In dry etching, atmospheric pressure plasma can be used. As the gas for dry etching, a chlorine-based gas classified by Cl_2, BCl_3, $SiCl_4$ or the like, or a fluorine-based gas classified by CF_4, SF_6, NF_3, CHF_3 or the like may be used. Gas, or O_2 gas. However, the gas used for etching is not limited thereto. Atmospheric pressure plasma can be used for etching. In this case, it is preferred to use a mixed gas of CF_4 and O_2 as an etching gas. The groove 81 can be formed by multiple etching using different gases. Of course, the wet etching can be used to form the groove 81.

When the groove is formed, the groove may have a depth capable of at least reaching a point at which the surface of the peeling layer is exposed, and preferably, a method such as a diamond wheel dicing machine may be appropriately controlled so as not to scratch the substrate, so that the groove The substrate 60 can be reused.

Next, the jig 83 (supporting substrate) having the protruding portion 82 is bonded so that the respective thin film integrated circuit devices 13 are fixed together with the bonding material 84 inserted therein (Fig. 14C). The jig may have a function of temporarily fixing a plurality of thin film integrated circuit devices in order to prevent dispersion of the thin film integrated circuit device after the peeling layer is removed. Preferably, the clamp has a structure similar to the projection of the comb, as shown in Figure 14C, such that it facilitates the introduction of a gas or liquid containing a halogen fluoride later. However, a flat jig can be used. More preferably, the opening 85 is provided such that it facilitates the introduction of a gas or liquid containing a halogen fluoride later.

As the jig, for example, a glass substrate, a quartz substrate, and a stainless steel (SUS) substrate including cerium oxide can be used as its main mechanism, and these substrates are not damaged by halogen. As long as materials that are not damaged by halogen fluoride are used, the jig is not limited to these substrates.

As the bonding material, a material whose bonding force (cohesiveness) can be reduced or lost by UV light radiation can be used. Here, a UV radiation stripping tape manufactured by Nitto Denko was used. In addition, the bonded and peeled bonding materials such as "Post-it" (registered trademark) manufactured by 3M INNOVATIVE PROPERTIES and "NOTESTIX" (registered trademark) manufactured by MOORE BUSINESS FORMS INC. . For example, acrylic adhesives, synthetic rubber binders, and natural rubber binders disclosed in Japanese Patent Application Publication No. 2001-30403, Japanese Patent Publication No. 2 092092, and Japanese Patent Application Publication No. Hei No. 6-299127 can be used. Of course, as long as the clamp is easily removed, the bonding material is not limited to these materials.

Next, an a-Si film as a peeling layer was etched and removed by introducing a halogen fluoride gas into the groove 81 (Fig. 15A). Here, the low-pressure CVD system shown in Fig. 18 is used to etch and remove the a-Si film under the following conditions: gas: ClF_3 (chlorine trifluoride), temperature: 350 ° C, flow rate: 300 sccm, pressure: 6 Torr, and time :3 hours. However, the conditions are not limited and can be changed as appropriate. In addition, a gas of ClF_3 mixed with nitrogen gas may be used, and it is necessary to appropriately set the flow rates of the two gases. In addition to ClF_3, a gas such as BrF_3 or ClF_2 can also be used.

The operation of the low pressure CVD system shown in Fig. 18 is to introduce a halogen fluoride gas such as ClF_3 gas 86 into the bell-shaped sintering furnace 100 in the reaction field so that the gas circulates in the substrate 101. Further, a heater 102 is disposed outside the bell-shaped sintering furnace, and the remaining gas is discharged from the exhaust duct 103.

In the process of selectively etching ruthenium using a halogen fluoride such as ClF_3, ruthenium dioxide, ruthenium nitride, $SiO_X N_Y$ or $SiN_X O_Y$ is difficult to be etched. Therefore, it takes time to etch the peeling layer 61 so that the substrate 60 can be finally peeled off (Fig. 15B). On the other hand, a base film (protective film), an interlayer film or a protective film including a material such as cerium oxide, cerium nitride, cerium oxynitride containing nitrogen or a heat-resistance resin is difficult to etch, thereby Damage to the thin film integrated circuit can be avoided. Of course, the stripped substrate 60 can be reused, which reduces cost.

The base material to be peeled off later is not limited to the above-described ruthenium-based material as long as the release layer 61 can be removed using a halogen fluoride such as ClF_3. Further, the material of the protective film or the interlayer film is not limited to the above materials as long as the layer is not damaged by halogen fluoride such as ClF_3.

Next, UV light radiation can be employed to reduce or eliminate the adhesion of the bonding material 84 such that the jig is separated from the thin film integrated circuit device. This makes it possible to mass-produce the thin film integrated circuit device 13. Preferably, the jig is reused to reduce cost (Fig. 15C).

The thin film integrated circuit device 13 which can be fabricated by the above method can be carried by using, for example, a small vacuum tweezers, and bonded to a desired portion of a product such as an ID mark and an ID card.

As a method of separating the substrate, a method may be employed in which stress is applied to the substrate of the formed thin film integrated circuit device to physically separate the substrate. In this case, a material such as W, SiO_2 and WO_3 may be used as the release layer. In order to provide stress, it may be applied using a

IPR2025-00645 Page 01693

diamond pen or the like. This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments.

(Example 2)

In the present embodiment, a case where the substrate 60 is repeatedly used is discussed, in which case the substrate 60 is divided in the formed groove 81 using a method such as a diamond dicing saw.

As a first method, a flat film 89 is formed on the substrate 88 used, as shown in Fig. 19A. As the flat film 89, a film such as spin coating, spray or droplet dripping can be used to form a film such as polyimide, acrylic, polyamide or a thermal resistance resin such as decane. In view of the subsequent treatment technique of the heat treatment, it is preferred to use a heat resistant resin film such as a siloxane. In addition, inorganic materials such as PSG (phosphorus phosphide), BPSG (borophosphon glass) or aluminum may also be used. The following processing techniques are the same as those in other embodiment modes or embodiments.

As a second method, which is not shown in the drawings, a CMP (Chemical Mechanical Polishing) method can be used to planarize the surface of the substrate, which is particularly effective in the case of using the substrate 88 in which slight scratches are present. In the CMP, polishing is performed by providing a polishing solvent called a slurry in a pad, and polishing is performed by rotating a wafer holder and rotating a turntable of a weighing scale to perform flattening. As the slurry, a slurry mixed with an alkaline colloidal alumina can be usually used. The following processing may be the same as in the other embodiment modes or embodiments. This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments.

(Example 3)

In the present embodiment, the case of using a substrate which is not a glass substrate or a quartz substrate as a release substrate is discussed.

In the first example, a tantalum wafer 90 is prepared, and an oxide film 91 (cerium oxide film) is formed on the surface of the tantalum wafer 90 by heat treatment to obtain a hot tantalum oxide substrate 92 (Fig. 19B). As the heat treatment method, for example, heat treatment at 800 to 1200 ° C (preferably, about 900 ° C to 1150 ° C) may be carried out in an atmosphere in which oxygen and nitrogen are present, but is not limited to these temperatures.

Although it is possible to oxidize all surfaces or at least a portion of the surface around the semiconductor substrate, it is preferred to oxidize all surfaces around the semiconductor substrate to form cerium oxide to facilitate subsequent use of a halogen fluoride such as ClF_3. The compound does not damage the semiconductor substrate when the thin film integrated circuit is separated from the substrate. The substrate forming the semiconductor substrate is not limited to germanium.

A substrate having a nitrided or oxynitrided surface can be used in place of a semiconductor substrate having an oxidized surface. For example, a substrate such as a single-layer germanium substrate or a thermal yttrium oxide substrate such as nitrogen ions may be implanted into the surface thereof. Also, a substrate including a metal such as a stainless steel substrate (SUS substrate) may be used, and an insulating film such as ruthenium dioxide or tantalum nitride may be formed on the surface thereof.

Thereafter, on the oxide film 91, a peeling layer, a base protective film, and a TFT are formed, and a gas such as a halogen fluoride is used for separation. After the TFT is directly formed on the oxide film 91 without providing a lift-off layer or a base protective film, the germanium wafer 90 can be removed for separation.

In a second example, a tantalum wafer is prepared and doped to implant oxygen ions. Subsequently, the buried oxide film 94 is formed by heat treatment at 900 to 1200 ° C (Fig. 19C). The heat treatment temperature is not limited to this. However, since the heat treatment also has a function of improving the crystallinity of the single crystal ruthenium layer on the surface side (upper c-Si layer 95) damaged by doping and the function of forming a buried oxide film, it is necessary to perform these functions according to these functions. Control the temperature of the heating. Thus, the SIMOX substrate 96 composed of the lower c-Si layer 93, the buried oxide film 94, and the upper c-Si layer 95 can be obtained.

The SOI substrate can be obtained by doping the nitrogen ions to replace the oxygen ions. Although not shown in the drawings, a polished substrate (so-called laminated substrate) having a device wafer for forming an oxide film (Si substrate on the side where the device is to be formed) and a processing wafer (Si substrate) and mutual bonds may be used. Together, the oxidized film is centered.

Thereafter, when a TFT is formed, the upper c-Si layer 95 can be used as a semiconductor layer (active layer) of the TFT. In the case of separation using a halogen fluoride gas, the lower c-Si layer 93 may be removed in whole or in part. The buried oxide film 94 has a function of a protective film (base film). This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments.

(Example 4)

In the present embodiment, a thin film integrated circuit device and a method of fabricating the same according to the present invention are discussed with reference to Figs. 17A and 17B. This manufacturing method does not use a jig for bonding bonding. First, the state shown in Fig. 14B (the state in which the groove is formed) is formed by the same method as the above embodiment.

Next, in the state shown in Fig. 14B, a plurality of substrates 99 to be used may be used as a tray on which a thin film integrated circuit device is formed, which is placed face down in a low pressure CVD furnace (bell sintered) The furnace is referred to and fixed in Fig. 18). In this case, the substrate forming the thin film integrated circuit device also has a function of accommodating the tray of the thin film integrated circuit device. Of course, the substrate and the tray can be provided separately. Subsequently, when a lift-off layer is etched using a halogen fluoride such as ClF_3, the separated upper film integrated circuit device can be detached from the back surface (plate area) of the substrate 99 to be used as a tray on the area A lower film integrated circuit device is formed.

The distance between the plate area and the thin film integrated circuit device is preferably 0.5 to 1 mm in order to avoid separate separation of the separated thin film integrated circuit device and to easily provide a halogen fluoride such as ClF_3. Further, in order to be able to avoid separate separation of the separated thin film integrated circuit devices, it is preferable to form a protruding portion at the center of the plate region of the substrate 99 to be used according to the size of the thin film integrated circuit device, as shown in Fig. 17A. Show.

After the device has been separated, the thin-film vacuum tweezers 97 or other absorbents can be used to carry the thin film integrated circuit device (Fig. 17B) on the plate area and transferred to the desired product.

As the substrate and the substrate 99 used also as a tray, various substrates such as a thermal yttrium oxide substrate, an SOI substrate such as a SIMOX substrate, a glass substrate, a quartz substrate, a SUS substrate, an aluminum substrate can be used. And a thermally resistant flexible substrate (plastic wafer, etc.). However, it is preferred to use a halogen fluoride and heat resistant.

With the above method, it is possible to mass-produce a thin film integrated circuit device without using a jig. This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments.

(Example 5)

IPR2025-00645 Page 01694

In the present embodiment, a method is discussed with reference to Figs. 20A to 20C and Figs. 21A to 21D, in which an antenna formed on a flexible substrate and a thin film integrated circuit device separately fabricated from the antenna are followed. Connected to each other.

20A to 20C show a case of manufacturing an ID mark, an ID card, and the like, in which case an antenna 105 is formed on the foldable flexible substrate 104, and the separately formed IDF wafer 107 is connected to the antenna 105. And then, the flexible substrate is folded into half for sealing, wherein the antenna 105 is formed by patterning after sputtering or the like, and can also be selectively instilled by using a droplet instillation including a conductive material. It is formed and subsequently dried and sintered to form the composition. After the antenna 105 is formed, a method such as CMP or compaction can be employed to improve its flatness.

For the antenna 105, a connection pad 106 for interconnecting the antenna 105 and the thin film integrated circuit device (IDF wafer) 107 can be formed. The connection pad 106 can be formed on the side of the thin film integrated circuit device. The thin film integrated circuit device 107 and the antenna 105 may be connected using an anisotropic conductive film or a well-known method such as bonding. The shape of the antenna 105 is not limited to the shape shown in Figs. 20A to 20C, and in the case of the electromagnetic induction type, the antenna 105 has a symmetrical coil shape as long as it is folded. Of course, other communication systems such as an electromagnetic coupling type, a microwave type, and an optical communication type can also be suitably employed.

Figure 21A is a schematic cross-sectional view showing the state of the folded antenna substrate along the line X-Y shown in Figure 20C. A method for interconnecting a folded antenna substrate and a thin film integrated circuit device (IDF wafer) can now be discussed with reference to Figs. 21A to 21D.

First, a peeling layer 51 including a material such as a-Si is formed on the substrate 104, and a protective film 55 is formed. In this case, a connection end point is formed which can be used to connect the lower layer antenna 105b after folding the antenna substrate (Fig. 21A). After the connection end points are formed by patterning of the conductive film, a flattening process can be performed, and then a protective film is formed. Further, after the protective film is formed to selectively leave the portion where the connection end is to be formed, the connection end point can be formed by dripping and the conductive material can be filled by a method such as droplet dripping.

Next, after forming a TFT constituting a CPU, a memory, or the like according to the above embodiment, the first interlayer film 30a is formed, and then a contact hole is formed to form an upper layer connection wiring 109a for connecting the upper layer antenna 105a, and the lower layer is connected The lower layer of the antenna 105b

is connected to the wiring 109b and the wiring 51 (Fig. 21B). Next, after the second interlayer film 30b is formed, a contact hole is formed to form an upper layer connection wiring 109a (Fig. 21C) for connecting the upper layer antenna 105a. A filler may be mixed between the first interlayer film 30a and the second interlayer film 30b.

Next, the formed IDF wafer including various wirings is bonded to the connection pads 106 of the flexible substrate 104 forming the antenna 105. In this case, the IDF wafer can be connected according to the methods shown in FIGS. 4A and 4B and FIGS. 5A and 5B. In the present embodiment, the connection end 108 and the connection pad 106 provided on the lower layer antenna 105b are connected to each other with the ACF 22 provided therebetween. In addition to ACF, bonding methods such as well-known bonding, ultraviolet bonding, or UV bonding can also be used.

Next, the flexible substrate 104 is folded, and the connection pads of the upper layer antenna 105a are connected to the upper layer connection wiring 109a in the same manner as the ACF inserted therein. Preferably, a material such as an epoxy resin between the antenna and the thin film integrated circuit device is molded. In this case, the stress caused by the difference in thermal expansion coefficient between the resin and the antenna due to the inclusion of the filler in the resin can be avoided. This makes it possible to prevent peeling and peeling of the resin.

As discussed in the present embodiment, the antenna is connected to the upper and lower portions of the thin film integrated circuit device by the folded antenna, and the antenna can be formed on the upper and lower portions of the thin film integrated circuit device, so that the receiving area can be increased to facilitate improve the accuracy of acceptance. This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments.

(Example 6)

In the present embodiment, a method in which a device separated using a halogen fluoride gas can be directly bonded to an ID card such as an ID card without removing the jig 83 for bonding the IDF wafer is discussed with reference to FIGS. 22a to 22C. On the goods.

First, a plurality of IDF wafers 110 may be formed by the method of the above embodiment, and the jig 83 is bonded by the bonding material 84 inserted therein. As the jig 83, a jig having the protruding portion 82 can be used as shown in Fig. 22A. As the bonding material 84, a material in which UV light radiation reduces or loses adhesion is used. Further, a protective film 54 including an organic material or an inorganic material is provided to prevent damage to the device. Subsequently, the mutual separation of the devices is performed by etching using a halogen fluoride such as ClF_3.

Next, the device with the bonding fixture is transferred and aligned on the steps of an article such as an ID card. In this case, the alignment marks 111 and 112 provided by the jig and the step can be used, as shown in Fig. 22A, and are not shown in the drawing, and the mark formed directly on the article can be used. On the part of the article where the thin film integrated circuit device is to be formed (here, the lower card substrate 37a of the ID card), the bonding material 113 is formed in advance, and the desired device can be bonded to the desired position of the article by controlling the position of the jig. (Fig. 22A).

Next, the device that adheres the lower card substrate 37b is selectively irradiated with UV light 114 by a mask to reduce or lose the adhesion of the bonding material 84 and thereby separate the jig from the device (Fig. 22B). This makes it possible to form the desired ID wafer 110 in the desired portion of the article. After the device is formed, the device can be covered with, for example, an upper card substrate 37a (Fig. 22C). Although shown here in the case of forming the antenna 11 in the card substrate, an antenna can also be formed in the device.

By using the method discussed in Example embodiment of the present invention, the device may require a desired portion is formed, without the need to use such as ClF_3 or the like halogen fluoride separation means are separated from each other during etching by means.

It is apparent that this embodiment can be applied not only to an ID card but also to various commodities. This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments

(Example 7)

In the present embodiment, a TFT structure such as a case where an ID mark is folded in one direction and an IDF wafer can be arbitrarily placed on a commodity is discussed.

FIG. 23 is a schematic plan view of the island-shaped semiconductor thin film 57 in the TFT in the IDF wafer 110 formed in the ID mark 20. In the island-shaped semiconductor thin film 57, a source region 115 and a drain region 117 which provide n-type or P-type impurities and a channel region 116 which does not provide impurities are formed. The semiconductor region of at least one of the TFTs in the IDF wafer 110 is connected to the antenna 11.

IPR2025-00645 Page 01695

The bending direction of the ID mark 20 may be set such that its direction is substantially perpendicular to the direction in which the source (S), the channel (C), and the drain (D) are formed or the direction in which the crystal grains are produced in the semiconductor film. Therefore, when the ID mark 20 is bent, the peeling generated in the island-shaped semiconductor film 57 can be avoided, and stable TFT operation can be provided regardless of the operation of the ID mark 20.

(Example 8)

In the present embodiment, the case of using high temperature polycrystalline germanium (HPS) in the treatment of Example 1 is discussed. In general, semiconductor processing including crystallization treatment at an upper limit temperature (about 600 ° C) of the glass substrate or higher than the upper limit temperature may be referred to as high temperature treatment.

After the semiconductor thin film is formed, the above catalyst such as Ni is added to the semiconductor thin film, and then heat treatment is performed in an LPCVD furnace. At a temperature of about or higher than 700 ° C, crystal nuclei are generated in the semiconductor film to promote crystallization.

Thereafter, after the island-shaped semiconductor film, a gate insulating film is formed by a method of LPCVD. For example, an HTO film (high temperature oxide film) is formed at a high temperature of 900 ° C or higher using a gas of a N_2 or O_2 decane gas.

Next, a gate electrode layer was formed by depositing polycrystalline germanium (p-Si) including a n-type impurity such as phosphorus with a film thickness of 150 nm. Further, W-Si (tungsten-telluride) having a film thickness of 150 nm was deposited. As a method of its production, a method such as sputtering or CVD can be suitably employed. Thereafter, the immersion treatment can be carried out in the same manner as in Example 1.

After the immersion treatment, a heat-acting treatment at a temperature of 950 ° C for 30 minutes was performed to actuate the impurity region. In addition, BPSG can be applied to reflow, and etching using a resist can be used to achieve leveling. Further, hydrogen burning annealing was performed at a temperature of 350 ° C to recover the damage of the plasma.

Other treatments can be carried out in the same manner as in the first embodiment. Although the TFT has an upper gate structure in this embodiment, a lower gate structure (reverse step structure) may also be used. This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments.

(Example 9)

In the present embodiment, the case where SAS (semi-amorphous germanium) is used for the island-shaped semiconductor thin film 57 in the process of the first embodiment is discussed. SAS can be obtained by glow discharge dissociation of a telluride gas. SiH_4 is a typical telluride gas, and in addition, it is also possible to use gases such as Si_2H_6, SiH_2Cl_2, $SiHCl_3$, $SiCl_4$ and SiF_4. SAS can be conveniently formed when using a vaporized gas diluted with one or more rare gas elements selected from the group consisting of hydrogen, hydrogen, and helium, argon, krypton, and lanthanum. The preferred dilution ratio of the diluted telluride gas ranges from 10 to 1000 times. Of course, under reduced pressure, the pressure reduction range is about 0.1 Pa to 133 Pa, and a gas discharge dissociation method can be used to form a film. In order to be able to generate a glow discharge, an electric power of from 1 to 120 MHz can be provided, preferably a high frequency power of from 13 to 60 MHz. The heat treatment temperature of the substrate is preferably 300 ° C or lower, and the recommended substrate heat treatment temperature is from 100 ° C to 200 ° C.

Further, a carbide gas such as CH_4 or C_2H_6 or a telluride gas such as GeH_4 or GeF_4 may be mixed into the vapor gas to control the band width to 1.5 to 2.4 eV or 0.9 to 1.1. eV.

When no impurity element is added for purposefully controlling valence electrons, SAS exhibits weaker n-type electron conductivity. This is because glow discharge at higher electric power is easier to mix oxygen with the semiconductor film than in the case of depositing an amorphous semiconductor. Thus, by burying the first semiconductor thin film, a channel formation region of the TFT is provided in the thin film, and it is possible to control the threshold voltage while depositing or after deposition to affect the p-type conductivity by the impurity element. As the impurity element which affects the p-type conductivity, boron can be usually used, and an impurity gas such as B_2H_6 or BF_3 can be mixed in the telluride gas at a ratio of 1 to 1000 ppm. For example, in the case of using boron as a p-type impurity element affect conductivity, the concentration of boron can be controlled to 1×10^{15} to 6×10^{16} atoms / cm^3. By forming the channel formation region using SAS, field effect mobility of 1 to 10 cm^2 /V sec can be obtained.

In the case of using SAS, it is also possible to omit the treatment of the crystallized semiconductor thin film (high temperature heat treatment). In this process, the wafer can also be formed directly on the flexible substrate. Although the TFT is not formed on the germanium wafer in principle of the present invention, it is possible to use the germanium wafer as a substrate which needs to be peeled off before the flexible substrate or the like. This embodiment can be combined arbitrarily with any of the other embodiment modes and embodiments.

(Embodiment 10)

In the present embodiment, an application of an ID tag, an ID tag, and an ID card according to the present invention and an example of bonding it to an article are discussed with reference to FIGS. 24A to 24E and FIGS. 25A to 25D.

Figure 24A shows an example of completing a product state in accordance with the ID tag of the present invention. On the marked board 118 (separated paper), a plurality of ID marks of the merged IDF wafer 110 are formed. The ID tag 20 is placed in the cartridge 119. In addition, the ID mark 120 is written with information about the goods or services (for example, the name of the article, the name tag, the trademark, the trademark owner, the seller, and the manufacturer), and the ID number uniquely owned by the product (or a class of products) Assignment to the incorporated IDF chip makes it possible to easily identify counterfeiting and infringement of intellectual property rights such as patents and trademarks, as well as violations such as unreasonable competition. In addition, there is too much information and it is difficult to write clearly on the product container or on the mark, for example, production area, sales area, quality, raw materials, effects, usage methods, quantity, shape, price, production method, direction of use, production time, information on the time, expiration date, and description of the product, as well as information on the intellectual property rights of the product, can be entered into the IDF chip so that both the contractor and the user can use a simple reader to read the information. While the producer can also easily rewrite or delete the information, the organizer or user is not allowed to rewrite or delete the information.

Figure 24B shows an ID tag 120 with a merged IDF die. By placing the ID tag 120 on the merchandise, the management of the merchandise becomes very convenient. For example, in the case of a stolen goods, the thief can be quickly caught by tracking the path of the merchandise. Thus, by providing an ID tag, it is possible to distribute high-quality goods in a so-called traceable manner.

Fig. 24C shows an example of the state in which the ID card 41 according to the present invention completes the product. The ID card may include all cards, such as a cash card, a credit card, a prepaid card, an electronic ticket, an electronic wallet, a calling card, and a membership card.

Figure 24D shows the state of the finished product to which the ticket 122 of the present invention is applied. The ticket 122 has an IDF wafer 110 implanted therein, and a resin is molded around it to protect the IDF wafer 110 in which a filler is contained in the resin. The ticket 122 can be manufactured in the same manner as the ID tag. ID

IPR2025-00645 Page 01696

a resin is molded around it to protect the IDF wafer 110 in which a filler is contained in the resin. The ticket 122 can be manufactured in the same manner as the IC tag, ID tag or ID card according to the present invention. The notes include, but are not limited to, stamps, tickets, membership fees, gift coupons, book coupons, stationery coupons, beer coupons, food coupons, various gifts and various service coupons

Fig. 24E shows the state of the finished product of the film 127 applied to the wrapping paper of the present invention. The film 127 for wrapping paper has an IDF wafer 110, and a resin is molded around it to protect the IDF wafer 110 in which a filler is contained in the resin. The film 27 suitable for wrapping paper can be produced, for example, by arbitrarily spreading an IDF wafer on an underlying film and covering the upper layer of the filling layer with the IDF wafer. A film 127 for wrapping paper can be placed in the box 129 and the desired number of films can be cut and used by the knife 128. The material of the film 127 for wrapping paper is not particularly limited. For example, materials such as a film resin, aluminum foil, and paper can be used.

25A and 25B show a book 123 and a plastic bottle 124 to which the ID mark 20 is bonded, respectively. The ID mark used in the present invention is quite thin. Therefore, when an ID tag is placed on an item such as a book 123, its function or design is not damaged. Further, in the case of the non-contact type thin film integrated circuit device, the antenna and the wafer can be integrally formed, so that it can more easily transfer the non-contact type thin film integrated circuit device directly to the article having the curved surface.

Fig. 25C shows a state in which the ID mark 20 is directly bonded to fresh food such as fruit 131. Further, Fig. 25D shows an example of packaging a fresh food such as vegetables using a film for wrapping paper. When the IDF wafer 110 is bonded to a commodity, it is possible to peel off the IDF wafer 110. However, when the film 127 for packaging is used to package a product, it is difficult to peel off the film 127 for packaging, which is more advantageous for safety. The IDF wafer according to the present invention can be applied to all commodities, including all of the above commodities.

(Example 11)

In the present embodiment, a method of managing a product carrying an ID tag or an ID tag according to the present invention, and a flow of information and merchandise are discussed with reference to FIGS. 26A and 26B, FIG. 27 and FIG.

First, a case where a customer purchases an item in a store is discussed with reference to FIG. 26A. An ID tag 20 or an ID tag storing information such as unique information of the product 132 and production history is attached to the product 132 displayed in the store. When holding the R/W 133 prepared in the store or his or her own R/W on the article 132 by the antenna portion 134 of the R/W 133 and the ID tag 20 or ID tag bonded to the article 132 Communication allows the user to read the information stored in the ID tag 20 or ID tag.

Preferably, the user can use the operation keys 136 to conveniently read information and select to purchase/not purchase. Further, the read information can be displayed on the display portion 135 provided on the R/W 133. This information includes the price of the item. Consumption tax, country of manufacture, manufacturer, place where goods are imported, time of production, deadline for optimal use, and application of goods (for example, in food use law). In addition, the total number of purchases is also displayed at the time of purchase to facilitate.

When the customer's R/W 133 is connected to the POS system 137 (point of sale system: a system for information management at the time of sale, in other words, a system for sales management, customer management, asset management, purchase management, and the like, it can be used by the automatic reader to read the ID mark, ID tag or the like stuck on the product when the product is sold, and directly input to the computer), and the bar code is no longer needed at the inspection and accounting place. Read

When the R/W 133 or POS system 137 is connected to the personal account 138, the electronic money can be automatically transferred to the purchase account without using the registration or the use of cash to purchase expensive valuable items and the like. In addition, when each person has an electronic money card, communication with R/W may be settled on the spot. As an electronic money card, of course, an ID card according to the present invention can be employed. Further, when a door for managing merchandise is provided at the exit of the store, it is possible to check that the merchandise that is not input to the R/W or POS system (generally, is not purchased) to prevent the thief.

The shape or function of the R/W is not limited to that shown in Fig. 26A. For example, as shown in FIG. 26B, a portable information terminal held by an individual, for example, a mobile phone body 180 having an R/W function, can be displayed on the display portion 183 by the sensor portion 181 to carry an ID tag or an ID tag. Information on the product 172. In this way, customers can more easily obtain more information about the product than the information provided by conventional radio frequency tags and the like.

In the case where the non-contact type thin film integrated circuit device is incorporated in the article according to the present invention, the article can be classified according to the distance and frequency between the article such as the card and the reader/writer: very close to the class, close to Classes, adjacent classes, and remote classes. Very close to the class is an electromagnetic induction class with a communication distance of 0 to 2 mm, and the communication frequency used is 4.92 GHz. The proximity class is an electromagnetic induction type with a communication distance of about 10 cm, and the communication frequency used is 13.56 MHz. The adjacent class is an electromagnetic induction type with a communication distance of about 70 cm, and the communication frequency used is 13.56 MHz. The remote control type is a microwave type with a communication distance of about several meters.

The characteristics of the non-contact type IC are that electric power is supplied by electromagnetic induction (electromagnetic induction), mutual inductance (electromagnetic coupling) of the coil antenna, or induction (electrostatic coupling) due to static electricity. By controlling the number of windings of the antenna, the frequency of reception can be selected. For example, by increasing the frequency so that the wavelength becomes shorter, the number of windings of the antenna can be reduced.

Compared with the contact type thin film integrated circuit device, the non-contact type thin film integrated circuit device is not in contact with the reader/writer, and power supply and information communication are performed without contact. Therefore, the non-contact type thin film integrated circuit device can not eliminate the high roughness which is provided, and there is no need to worry about errors due to the static electricity place. In addition, the thin film integrated circuit device can be conveniently handled, which can be held on the reader/writer in an incomplete structure, and briefly discusses carrying an ID tag, an ID tag or the like according to the present invention. Product flow. In Fig. 27, a producer (manufacturer) supplies a product carrying a thin film integrated circuit device to a seller (for example, a retailer or an agent) or a customer. Subsequently, the seller can provide the seller with sales information such as price information, quantity of goods sold, and time of sale according to the settlement of the customer. On the other hand, customers can provide purchase information such as personal information. For example, the customer can provide purchase information to the seller and the manufacturer via the Internet or the like by using a credit card or a personal reader carrying the thin film integrated circuit device or the like. In addition, the seller can use the thin film integrated circuit device to provide product information to the customer, and the seller can obtain the purchase information from the customer. These sales information, purchase information or other information are valuable information and are very useful for future business decisions.

As a means of providing various information, one method is to read information about a thin film integrated circuit device by a vendor or a customer's reader and distribute it to a producer (manufacturer), a seller, or a customer via a computer or a network. . As discussed above, the various information provided by the thin film integrated circuit device can be sent to the department in need of information. Therefore, the ID tag and the ID tag according to the present invention are also very useful

IPR2025-00645 Page 01697

in the exchange of goods and the management of goods. The system discussed above can be applied to the case where a product is redistributed from a customer to a product agent.

Next, the case of the airport baggage check will be discussed with reference to FIG. When the baggage 139 having the ID tag 120 incorporated in the IDF wafer 110 is placed on the transport belt 145 through the reader/writer 140, the electromagnetic wave 142 oscillated by the antenna 141 activates the IDF wafer 110, which will be in the memory. The included information is converted into a signal and sent to the reader/writer 140 so that the computer 143 can recognize the information.

The computer 143 is connected to the database 144, and stores in the database an appropriate allocation (legal distribution) of product information (hereinafter referred to as "identification product") attached to the ID tag or the ID tag or incorporated in the IDF chip. The product information included in the baggage 139 can be verified by the database 144. Subsequently, in the case where the baggage 139 includes an item that is not the identification product, the inspection is performed, and the inspection can be performed according to the need, configuration, abandonment, disposal, or the like. In the case of dangerous goods or weapons, such as the prohibition of carrying the aircraft, even if this is the identification product, the computer 143 will still detect such dangerous goods or weapons. In this case, the software in the computer 143 can be programmed to prevent the baggage from passing through the detection door.

Of course, in the case of illegal items, such as forged items, counterfeits, contraband or smuggled goods that are not identification products, the baggage is not allowed to pass through the detection door. This makes it possible to prevent illegal items from entering or coming out of the country. In addition, dangerous goods and weapons can be detected to prevent terrorist activities.

(Embodiment 12)

In the present embodiment, an example of the communication principle of the ID tag, the ID tag, the ID card, and the like according to the present invention is discussed with reference to Figs. 29 to 31.

Figure 29 shows a block diagram of an item such as an ID tag and reader/writer 414. Marker 400 marks the antenna for input and marker 401 marks the antenna for output. In addition, the mark 402 marks the interface for input, and the mark 403 marks the interface for output. The number of antennas of all kinds is not limited to the number shown in FIG. The shape of the antenna is also not limited to the shape of the coil. The electromagnetic wave 412 received by the antenna 400 can be used to input from the antenna 418 as an output of the reader/writer 414, demodulated or converted to a direct current in the input interface 402, and then, by bus 409 Various circuits such as the CPU 404, the auxiliary processor 405, the ROM 406, the RAM 407, and the non-volatile memory 408 are provided.

When all processing in the thin film integrated circuit device 410 is controllable, the auxiliary processor 405 is used as an auxiliary processor that assists the main processor CPU 404 in operation. In general, the auxiliary processor 405 has the function of an instruction execution unit dedicated to processing code, and is capable of performing processing of code, which is necessary in an application such as settlement. As the non-volatile memory 408, for example, EPROM, EEPROM, UV-EPROM, flash memory or FRAM, it is preferable to use a memory that can rewrite information multiple times.

The non-volatile memory 408 can be divided into program memory (the area in which the program is stored), working memory (the area temporarily stored in the program execution data), and the data memory (in addition to the unique information of the product). The area of the fixed data processed by the program). In general, ROM can be used for program memory and can be used for working memory. In addition, the RAM can also have the function of a buffer in communication with R/W. In order to be able to store data input with a predetermined address as a signal, an EEPROM can generally be used.

The unique information of the product can be stored in the memory, converted into a signal in each of the above circuits, modulated in the output interface 403, and sent to the output R/W 414 via the antenna 401. In the input interface 402, a rectifying line 420 and a demodulating circuit 421 are provided. The AC power source voltage input from the input antenna 400 is rectified in the rectifying circuit 420, and supplied to each of the above circuits as a DC power source voltage. Further, various kinds of AC signals input from the input antenna 400 are demodulated in the demodulation circuit 421. Subsequently, individual signals for demodulating the shaped waveform are supplied to the respective circuits.

In the output interface 403, a modulation circuit 423 and an amplifier 424 are provided. The respective signals input to the output interface 403 by the respective circuits are modulated in the modulation circuit 423 and amplified or buffer amplified, and then transmitted from the output antenna 401 to a terminal device such as R/W. The input antenna 425 of the R/W 414 receives the signal transmitted by the non-contact type thin film integrated circuit device 411, and demodulates the signal in the input interface 426, and transmits the demodulated signal supply controller 427 to the computer 419. And the data processing can be performed with or without the database 415, so that the unique information of the product can be identified.

Although the above computer 419 has a software that can handle the product information function, of course, it is also possible to use hardware for information processing. Therefore, compared with the work of reading the barcode one by one by the conventional method, the time and labor for the information processing and the error can be greatly reduced, thereby reducing the burden in the commodity management.

The various circuits shown in Figure 29 merely show a structure in accordance with the present invention. The various circuits mounted on the article 411 and the R/W 414 are not limited to the above circuits. Fig. 29 shows an example in which an antenna is used as a non-contact type. However, the non-contact type is not limited to this example. Light-emitting elements, optical sensors, and the like can be used to transmit and receive light data.

In FIG. 29, the input interface 402 and the output interface 403 both include a rectifying circuit 420, a demodulating circuit 421 or a modulating circuit 423, and a CPU 404 which are formed in the thin film integrated circuit device 410. Various memory and other analog circuits. Further, in the R/W 414, the output interface 417 and the input interface 426 may also be formed in the integrated circuit 416. However, the structure is merely an example, and the present invention is not limited to the structure. For example, the input interface 402 and the output interface 403 may each include an analog circuit such as a rectifying circuit 420, a demodulating circuit 421, and a modulating circuit 423 formed in an IC chip, while the CPU 404, various memories, and the like, etc. It can be formed in a thin film integrated circuit device formed using a TFT.

Fig. 29 shows an example in which a power supply voltage is supplied by a reader/writer as a terminal device. However, the invention is not limited to this structure. For example, not shown in the drawings, a solar cell can be provided in the non-contact type integrated circuit device. In addition, a very thin battery such as a lithium battery can also be inserted.

FIG. 30 is a perspective view illustrating the ID mark 200 in the case where the input antenna 400 and the output antenna 401 are respectively formed. Although the special manufacturing method of the ID mark 20 is the same as that in the embodiment mode 1, it has four end point regions connecting the thin film integrated circuit device 13 to the antenna. The configuration in the case where the input antenna 400 and the output antenna 401 are respectively formed is not limited thereto.

Now, the CPU structure in the thin film integrated circuit device will be briefly discussed. Figure 31 shows a block diagram of an integrated circuit including a CPU, a memory, and an interface for input and output. First, for the CPU 919, the step of reading an instruction from the program memory 906 in the main memory 905 is indispensable. Therefore, it is necessary to distinguish the address of the instruction by the address bus 917. In this case, the address management section 911 executes

a command to address the main memory 905. Information in the main memory 915 can be performed by controlling the bus 918.

When the address points to the program memory 906, the instructions stored in the address are output, and the output instructions are fetched to the instruction register 912 by the data bus 916 and the internal bus 915. Various registers or a set of registers 910 include memory elements for operation that can be used to store material and execution status in the CPU 919, and for performing various processing in the CPU 919.

Instructions placed in the instruction register 912 can be sent to the instruction decoder 913. The instruction decoder 913 first compiles the received instructions and converts them into control information that the control section 900 can understand, and the operation of the instruction control section 900. The instruction decoder 913 distinguishes the information track (scratchpad or memory) to be processed according to the instruction. The term 'compilation' refers to converting data (bits) of multiple input signals into special signals.

Instructions from the instruction decoder 913 to the control portion 900 can be performed using signals. The control section 900 has signal lines (control lines) for controlling the circuits, and various processes corresponding to the type of information can be performed, and various control signals have additional switching circuits. When the switch is turned on, the control signal can be output to the circuit.

In the case where the content of the instruction is related to arithmetic, the control section 900 outputs a control signal (pulse signal for reading data) for arithmetic processing to the processor 901. The arithmetic arithmetic register 902 can be divided into two registers 903 and 904 that process objects and processed objects. The tasks of various memories are as discussed above. In addition, when the CPU 919 communicates with an external device (e.g., R/W), the input and output interface 914 has a function of converting signals of different standards into signals that the CPU 919 can process.

Further, the work memory 907 is an area temporarily stored in the data for executing the program processing, and the data memory 908 is an area for storing the fixed data processed by the program. As the working memory 907, RAM (Random Access Memory) can be generally used, and has a function of a work area in data processing. In addition, the RAM can also function as a buffer in communication with the R/W. In order to store the input data in a predetermined address as a signal, an EEPROM can generally be used.

(Example 13)

In the present embodiment, an example of an IDF wafer structure in accordance with the present invention is discussed in more detail with reference to Figures 32A and 32B. 32A shows a schematic diagram of an IDF die 217 that includes a power supply circuit 214, an input and output circuit 215, an antenna circuit 216, a logic circuit 210, an amplifier 211, a clock generation circuit and decoder 212, a memory 213, and the like. The antenna circuit 216 has an antenna wire 201 and an antenna capacitor 202.

The IDF wafer 217 can operate without its own power source because the power supply can be provided by receiving electromagnetic waves 218 from the reader/writer 200. When the antenna circuit 216 receives the electromagnetic wave 218 from the reader/writer 200, the signal as the detection output signal is detected by the input/output circuit 215, and the input/output circuit 215 includes the first capacitor mechanism 203, the first two. The polar body 204, the third diode 207, the third capacitor mechanism 208, and the like. Amplifier 211 amplifies this signal to a sufficiently large amplitude and then separates it into a clock and instruction with data using clock generator and decoder 212. The transmitted instructions can be decoded by logic circuit 210 to respond to the data in memory 213 and to write the required information to the memory.

The response can be generated by the switching element 209 in accordance with the on/off of the output of the logic circuit 210. This changes the impedance of the antenna 216, thereby changing the reflectivity of the antenna circuit 216. The reader/writer 200 reads the information of the IDF wafer 217 by detecting changes in the emissivity of the antenna circuit 216.

The power supply power consumed by the various circuits in the IDF wafer 217 is provided by a DC power supply VDD generated by the electromagnetic waves 218 received by the detection and smoothing power supply circuit 214. The power circuit 214 includes a first capacitor mechanism 203, a first diode 204, a second diode 205, and a second capacitor mechanism 206, wherein the second capacitor mechanism 206 can be controlled to have a sufficiently large value to facilitate Power is supplied to each circuit.

Figure 32B shows antenna circuit 1308 and power supply circuit 1307 separated from the circuitry used in IDF wafer 1309. The antenna circuit 1308 has an antenna wiring 1301 and an antenna capacitor 1302. The power supply circuit 1307 has a first capacitor mechanism 1303, a first diode 1304, a second diode 1305, and a second capacitor mechanism 1306.

The operation without the battery can be one of the features of the IDF wafer 1309. As discussed above, the IDF wafer has a mechanism in which the electromagnetic waves oscillated by the reader/writer can be picked up by the antenna circuit 1308 and rectified by the power supply circuit 1307 to generate a DC power source; and incorporated in the ID chip. The circuit in operation can be operated by a DC power supply.

In the embodiment modes and embodiments, the non-contact type thin film integrated circuit device is mainly discussed. Of course, the thin film integrated circuit device according to the present invention can also be used as a contact type thin film integrated circuit device. For example, it may be a magnetic strip type or an IC module contact type wafer. In the case of a contact type IC, a structure without an antenna can be employed. Further, a combined structure of a magnetic stripe type or an IC module contact type thin film integrated circuit device and a non-contact type thin film integrated circuit device may be used.

The thin film integrated circuit device to which the IDF wafer is classified according to the present invention can be mounted on various commodities such as an ID mark, an ID card, and an ID tag. In addition, the thin film integrated circuit device can be used in banknotes, coins, credit cards, tickets, and securities. In particular, when a paper, a plate or a wrapper is applied to a product, the thin film integrated circuit device is very effective. These products can be manufactured with reference to the embodiment modes and examples. As discussed above, the present invention is widely applicable.

Although the present invention has been fully described by reference to the embodiments of the drawings, it should be understood that various changes and modifications are obvious to those skilled in the art. Therefore, all such changes and modifications are intended to be included within the scope of the invention as defined herein.

10. . . Base

11. . . antenna

12. . . Connection pad

13,13'. . . Thin film integrated circuit device

14. . . Printing

IPR2025-00645 Page 01699

twenty four. . . Fill layer

28. . . Filler

15. . . Bonding material layer

16. . Separation layer

20. . . ID tag

twenty three. . . TFT

21, 21a-21c. . . Connection wiring

twenty two. . . Anisotropic conductive film

18. . Cross wiring

19. . . Contact part

53. . . middle layer

26. . . Bonding material layer

17. . . coating

27. . Insulation

30a. . . First intermediate layer

30b. . . Second intermediate layer

31. . . Protective film

32. . . Internal substrate

37a. . . Upper card substrate

37b. . . Lower card base

41. . . ID card

54. . . Protective film

49. . . ID tag

46. . . Antenna integrated thin film integrated circuit device

48. . . Thin film integrated circuit device

47. . . antenna

57. . . Island semiconductor film

58. . . Gate insulating film

55. . . Protective film

56. . . Gate electrode

52. . . Cross wiring

51, 51a-51b . . wiring

59. . . Passivation film

53. . . Intermediate film

300. . . Marking paper supply mechanism

301. . . ACF supplier

302. . . IDF wafer bonding mechanism

303. . . Bonding material layer supply mechanism

308. . . Filler layer supply mechanism

304. . . Separation paper supply mechanism

305. . . Marking picking mechanism

118. . . Marking the motherboard

306. . . Marking separation mechanism

307. . . Collection agency

309. . . Substrate separation mechanism

IPR2025-00645 Page 01700

310. . . Cascading system

45. . . Laminated resin layer

61. . . Peeling layer

60. . . Base

62. . . Resist

70,72. . . p channel TFT

63. . . Resist

69,71. . . N-channel TFT

64. . . Impurity element

65. . . Impurity element

66. . . Resist

67. . . Impurity element

68. . . Impurity area

75. . . Insulating film

44. . . Resist

76. . . Side wall

77. . . Resist

78. . . Impurity element

79. . . Impurity area

73. . . CPU

74. . . Memory

81. . . Groove

82. . . Prominent part

83. . . Fixture

85. . . Opening

84. . . Bonding material

86. . . ClF_3 gas

100. . . Bell-shaped sintering furnace

101. . . Base

102. . . Heater

103. . . Exhaust pipe

88. . . Base used

89. . . Leveling film

90. . . IC chip

91. . . Oxide film

92. . . Thermal ruthenium oxide substrate

94. . . Buried oxide film

93. . . Lower c-Si layer

95. . . Upper c-Si layer

99. . . Base

97. . . Small vacuum tweezers

105. . . antenna

104. . . Foldable flexible substrate

106. . . Connection pad

IPR2025-00645 Page 01701

107. . . Thin film integrated circuit device (IDF wafer)

108. . . Connection end

105b. . Lower antenna

105a . . Upper antenna

109a, 109a'. . . Upper connection wiring

109b. . . Lower connection wiring

110. . . IDF chip

111. . . Alignment mark

112. . . Alignment mark

113. . . Bonding material

114. . . UV light

115. . . Source area

117. . . Bungee area

116. . . Channel area

119. . . box

120. . . ID tag

122. . . bill

127. . . film

128. . . Barrier

129. . . box

123. . . books

124. . . Plastic bottle

131. . . fruit

130. . . vegetables

132. . . commodity

133. . . R/W

134. . . Antenna section

135. . . Display section

136. . . Operation key

137. . . POS system

180. . . Mobile phone body

138. . . Personal account

172. . . commodity

181. . . Sensor section

183. . . Display section

139. . . Baggage

145. . . conveyor belt

140. . . Reader/writer

142. . . Electromagnetic wave

141. . . antenna

143. . . computer

144. . . database

411. . . Thin film integrated circuit device

414. . . Reader/writer

400. . . Antenna for input

IPR2025-00645 Page 01702

401. . . Antenna for output

402. . . Interface for input

403. . . Interface for output

412. . . Electromagnetic wave

418. . . antenna

409. . . Busbar

404. . . CPU

405. . . Auxiliary processor

406. . . ROM

407. . . RAM

410. . . Thin film integrated circuit device

408. . . Non-volatile memory

420. . . Rectifier circuit

421. . . Demodulation circuit

423. . . Modulation circuit

424. . . Amplifier

425. . . antenna

426. . . Interface for input

427. . . Controller

419. . . computer

415. . . database

417. . . Interface for output

416. . . Integrated circuit

200. . . ID tag

919. . . CPU

906. . . Program memory

905. . . Main memory

917. . . Address bus

911. . . Address management section

918. . . Control bus

912. . . Instruction register

916. . . Data bus

915. . . Internal bus

910. . . Register

913. . . Instruction decoder

900. . . Control section

901. . . processor

902. . . Arithmetic register

903,904 . . Register

914. . . Interface

907. . . Working memory

908. . . Data memory

217. . . IDF chip

214. . . Power circuit

215. . . Input and output circuits

IPR2025-00645 Page 01703

216. . . Antenna circuit

210. . . Logic circuit

211. . . Amplifier

212. . . Clock generation circuit and decoder

213. . . Memory

201. . . Antenna wiring

202. . . Antenna capacitor

218. . . Electromagnetic wave

200. . . Reader/writer

203. . . First capacitor mechanism

204. . . First diode

207. . . Third diode

208. . . Third capacitor mechanism

209. . . Switching element

205. . . Second diode

206. . . Second capacitor mechanism

1308. . . Antenna circuit

1307. . . Power supply circuit

1309. . . IDF chip

1301. . . Antenna wiring

1302. . . Antenna capacitor

1303. . . First capacitor mechanism

1304. . . First diode

1305. . . Second diode

1306. . . Second capacitor mechanism

1A and 1B are perspective views illustrating an ID mark structure according to the present invention; Figs. 2A and 2B are perspective views illustrating an ID mark structure according to the present invention; and Figs. 3A and 3B are perspective views illustrating an ID card structure according to the present invention; And 4B are perspective views illustrating the ID mark structure according to the present invention (using an isotropic conductive film); FIGS. 5A and 5B are perspective views illustrating the ID mark structure according to the present invention (using a layer of a non-conductive adhesive material); FIGS. 6A and 6B Is a perspective view (internal cross-wiring) illustrating the ID mark structure according to the present invention; FIGS. 7A to 7C are perspective views (using an internal substrate) illustrating the ID mark, ID card, and ID tag structure according to the present invention; FIGS. 8A and 8B are illustrations A perspective view of an ID tag and ID card structure according to the present invention (embedded antenna type); FIGS. 9A and 9B are schematic cross-sectional views of an ID tag and other embedded antenna type thin film integrated

circuit device according to the present invention, FIG. 10A and 10B is a diagram illustrating an ID mark and other production lines according to the present invention; FIGS. 11A and 11B are enlarged views showing a diagram and a finished product of an ID card and an ID tag and other production lines according to the present invention; 12A to 12E are diagrams for explaining a method of manufacturing a CPU and a memory in the thin film integrated circuit device used in the present invention; and Figs. 13A to 13D are views showing a CPU in the thin film integrated circuit device used in the present invention; FIG. 14A to FIG. 14C are diagrams illustrating a method of manufacturing a CPU and a memory in the thin film integrated circuit device used in the present invention; and FIGS. 15A to 15C are diagrams illustrating a thin film product used in the present invention FIG. 16A and FIG. 16B are diagrams illustrating a method of forming a sidewall; FIGS. 17A and 17B are diagrams illustrating a method of disassembling a thin film integrated circuit device (using a substrate to be used as a disk) Figure 18 is a schematic view of a low-pressure CVD system; Figures 19A to 19C are schematic views illustrating various substrates to be peeled off; Figures 20A to 20C are schematic views illustrating a folded antenna substrate, and Figures 21A to 21D are diagrams illustrating a thin film product in the case of a folded antenna substrate FIG. 22A to FIG. 22C are schematic diagrams illustrating a method of bonding an IDF wafer to a commercial substrate (selective ultraviolet light radiation); FIG. 23 is a view showing formation of a TFT. Diagram of the relationship between the direction of the pole/channel/drain region and the folding direction of the commercial substrate; FIGS. 24A to 24E are diagrams illustrating an example of an article according to the present invention; FIGS. 25A to 25D are diagrams illustrating bonding of an ID mark according to the present invention or the like FIG. 26A and FIG. 26B are diagrams showing an example of purchasing goods in a store; FIG. 27 is a diagram showing a relationship between a product manufacturer (manufacturer), a seller, and a customer; FIG. 28 is a view showing a safety proofreading FIG. 29 is a block diagram illustrating an ID mark structure according to the present invention; and FIG. 30 is a perspective view illustrating an ID mark structure according to the present invention (an antenna for input and an output for output) Fig. 31 is a block diagram showing the structure of a CPU in a thin film integrated circuit device; and Figs. 32A and 32B are circuit diagrams of a thin film integrated circuit device used in the present invention.

10. . . Base

11. . . antenna

12. . . Connection pad

twenty four. . . Fill layer

IPR2025-00645 Page 01704

28. . Filler

15. . . Bonding material layer

16. . . Separation layer

twenty three. . . TFT

twenty one. . . Connection wiring

twenty two. . . Anisotropic conductive film

18. . . Cross wiring

19. . . Contact part

17. . . coating

Patent Citations (17)

Publication number	Priority date	Publication date	Assignee	Title
US5378536A *	1991-04-08	1995-01-03	Minnesota Mining And Manufacturing Company	Repositionable adhesive tape
US6168829B1 *	1993-01-21	2001-01-02	Moore Business Forms, Inc.	Double faced tape with repositional adhesive
Family To Family Citations				
CA2032125A1	1990-02-22	1991-08-23	John A. Miller	Repositionable adhesive tape
JPH09214111A *	1996-01-30	1997-08-15	Matsushita Electric Ind Co Ltd	Electronic circuit board
CN1258252A	1997-05-27	2000-06-28	三菱树脂株式会社	Non-contact IC card and method for mfg. same
US6073856A *	1997-09-05	2000-06-13	Dai Nippon Printing Co., Ltd.	Noncontact IC device
JP2000332523A *	1999-05-24	2000-11-30	Hitachi Ltd	Radio tag, and its manufacture and arrangement
JP2001030403A	1999-07-16	2001-02-06	Three M Innovative Properties Co	Base material having multilayered structure and self- adhesive film
JP2001118041A	1999-10-18	2001-04-27	Denso Corp	Id tag
US6509217B1 *	1999-10-22	2003-01-21	Damoder Reddy	Inexpensive, reliable, planar RFID tag structure and method for making same
US6307517B1 *	2000-06-13	2001-10-23	Applied Wireless Identifications Group, Inc.	Metal compensated radio frequency identification reader
WO2008008785A1 *	2003-07-17	2005-01-27	Matsushita Electric Industrial Co., Ltd.	Thin film transistor and method for manufacturing same
US7566001B2 *	2003-08-29	2009-07-28	Semiconductor Energy Laboratory Co., Ltd.	IC card
US7405665B2 *	2003-12-19	2008-07-29	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device, RFID tag and label-like object
TWI457835B *	2004-02-04	2014-10-21	Semiconductor Energy Lab	An article carrying a thin film integrated circuit
US7472296B2 *	2004-02-20	2008-12-30	Semiconductor Energy Laboratory Co., Ltd.	Integrated circuit, semiconductor device and ID chip
WO2005121908A1 *	2004-06-14	2005-12-22	Semiconductor Energy Laboratory Co., Ltd.	Copy machine with copy control function, scanner and facsimile, and piece of paper and film each installed with semiconductor device

* Cited by examiner, † Cited by third party

Cited By (101)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7566001B2 *	2003-08-29	2009-07-28	Semiconductor Energy Laboratory Co., Ltd.	IC card
CN1910608B *	2004-01-23	2011-12-14	株式会社半导体能源研究所	ID label, ID card, and ID tag
TWI457835B *	2004-02-04	2014-10-21	Semiconductor Energy	An article carrying a thin film integrated circuit

IPR2025-00645 Page 01705

			Lab	
CN101010706B *	2004-09-03	2012-07-11	株式会社半导体能源研究所	Health data collecting system and semiconductor device
WO2006031824A2 *	2004-09-14	2006-03-23	Adasa, Inc.	Systems and methods for deployment and recycling of rfid tags, wireless sensors, and the containers attached thereto
TWI372413B *	2004-09-24	2012-09-11	Semiconductor Energy Lab	Semiconductor device and method for manufacturing the same, and electric appliance
JP3915927B2 *	2004-11-18	2007-05-16	セイコーエプソン株式会社	Electronic component and manufacturing method thereof
JP3915928B2 *	2004-11-24	2007-05-16	セイコーエプソン株式会社	Electronic component and manufacturing method thereof
CN101088158B *	2004-12-24	2010-06-23	株式会社半导体能源研究所	Semiconductor device
US7579224B2 *	2005-01-21	2009-08-25	Semiconductor Energy Laboratory Co , Ltd.	Method for manufacturing a thin film semiconductor device
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7307006B2 *	2005-02-28	2007-12-11	Semiconductor Energy Laboratory Co., Ltd.	Method of manufacturing semiconductor device
JP5186359B2 *	2005-03-26	2013-04-17	ブリバンターズ、インコーポレイテッド	Electronic financial transaction card and method
US7237724B2 *	2005-04-06	2007-07-03	Robert Singleton	Smart card and method for manufacturing a smart card
WO2006129578A1	2005-05-30	2006-12-07	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device and driving method thereof
US7605056B2 *	2005-05-31	2009-10-20	Semiconductor Energy Laboratory Co , Ltd.	Method of manufacturing a semiconductor device including separation by physical force
US20060272980A1 *	2005-06-06	2006-12-07	Montgomery Robert D	Interconnecting luggage system having optional features
US7510950B2 *	2005-06-30	2009-03-31	Semiconductor Energy Laboratory Co., Ltd.	Method for manufacturing semiconductor device
US7687327B2	2005-07-08	2010-03-30	Kovio, Inc,	Methods for manufacturing RFID tags and structures formed therefrom
US7607249B2 *	2005-07-15	2009-10-27	Innovatier Inc.	RFID bracelet and method for manufacturing a RFID bracelet
US7598867B2 *	2005-09-01	2009-10-06	Alien Technology Corporation	Techniques for folded tag antennas
TWI409934B *	2005-10-12	2013-09-21	Semiconductor Energy Lab	Semiconductor device
US7435625B2 *	2005-10-24	2008-10-14	Freescale Semiconductor, Inc.	Semiconductor device with reduced package cross-talk and loss
US7635014B2 *	2005-11-11	2009-12-22	Semiconductor Energy Laboratory Co., Ltd.	Method for pressure bonding and method for manufacturing semiconductor device
US7551448B2 *	2006-01-31	2009-06-23	Cryovac, Inc.	Electronic device having improved electrical connection
US20070183184A1 *	2006-02-03	2007-08-09	Semiconductor Energy Laboratory Ltd.	Apparatus and method for manufacturing semiconductor device
JP4640221B2	2006-03-10	2011-03-02	セイコーエプソン株式会社	Ink cartridge and printer
JP4661643B2	2006-03-13	2011-03-30	セイコーエプソン株式会社	Semiconductor device, ink cartridge, and electronic device
JP5057321B2 *	2006-03-14	2012-10-24	株式会社ジャパンディスプレイウェスト	Manufacturing method of display device
US7823217B2 *	2006-03-27	2010-11-09	Muhlbauer Ag	Method and device for producing RFID smart labels or smart label inlays
BRPI0710244A2 *	2006-04-10	2021-07-06	Innovatier, Inc.	ELECTRONIC INLAYS AND ELECTRONIC CARDS AND THEIR MANUFACTURING METHODS
US20070290048A1 *	2006-06-20	2007-12-20	Innovatier, Inc.	Embedded electronic device and method for manufacturing an embedded electronic device

IPR2025-00645 Page 01706

US20080007409A1 *	2006-06-21	2008-01-10	Ferry Kristel L.	Making and securing identification tags
CN102156901B *	2006-06-26	2013-05-08	株式会社半导体能源研究所	Paper including semiconductor device and manufacturing method of same
JP5204958B2 *	2006-06-26	2013-06-05	株式会社半導体エネルギー研究所	Method for manufacturing semiconductor device
EP1873692B1 *	2006-06-29	2011-12-21	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
DE102006030913A1	2006-06-29	2008-01-03	Inotec Barcode Security Gmbh	Decorative or exhibitive surface element with a lithographic imprint that is manufactured by means of in-mould labeling process, comprises a planar base structure, an identification element, and a first- and a second lateral surface
US8232621B2 *	2006-07-28	2012-07-31	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
US20080055824A1 *	2006-08-25	2008-03-06	Innovatier, Inc.	Battery powered device having a protective frame
US20080160397A1 *	2006-08-25	2008-07-03	Innovatier, Inc	Battery powered device having a protective frame
DE102006042329B4 *	2006-09-01	2008-08-21	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.	A method for selective plasma chemical dry etching of phosphosilicate glass formed on surfaces of silicon wafers
US7561107B2 *	2006-09-07	2009-07-14	Intelleflex Corporation	RFID device with microstrip antennas
US20080061979A1 *	2006-09-13	2008-03-13	Hause Curtis B	Traceable RFID enable data storage device
US20080065676A1 *	2006-09-13	2008-03-13	Hause Curtis B	System and method for tracing data storage devices
US20080122623A1 *	2006-09-13	2008-05-29	Hause Curtis B	System and method for tracing data storage devices
JP4870509B2 *	2006-09-27	2012-02-08	新光電気工業株式会社	Electronic equipment
US7797252B2	2006-10-20	2010-09-14	Target Brands, Inc.	Service plan product and associated system
KR20090086404A *	2006-11-07	2009-08-12	토판 폼즈 컴퍼니 리미티드	Window base material, card having module housed therein, and method for manufacturing card having module housed therein
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080198022A1 *	2007-02-21	2008-08-21	Imation Corp.	Inkjet printable RFID label and method of printing an inkjet printable RFID label
JP4957285B2 *	2007-02-22	2012-06-20	富士通株式会社	RFID tag, protective member, and method of manufacturing protective member
TW200845844A *	2007-03-23	2008-11-16	Innovatier Inc	A step card and method for making a step card
JP5268395B2 *	2007-03-26	2013-08-21	株式会社半導体エネルギー研究所	Method for manufacturing semiconductor device
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US7953433B2	2007-04-24	2011-05-31	Imation Corp.	Data storage device and data storage device tracing system
US20080282540A1 *	2007-05-14	2008-11-20	Innovatier, Inc.	Method for making advanced smart cards with integrated electronics using isotropic thermoset adhesive materials with high quality exterior surfaces
KR100798685B1 *	2007-05-31	2008-01-28	주식회사 제이디씨텍	A process of manufacture for liquid crystal display smart card
JP2009000942A *	2007-06-22	2009-01-08	Brother Ind Ltd	Tag tape, tag tape roll, radio tag circuit element cartridge, and tag label producing apparatus
TW200912761A *	2007-07-20	2009-03-16	Soon Huat Leonard Wee	A radio frequency transponder
JP5037286B2 *	2007-09-28	2012-09-26	富士通株式会社	RFID tag and method of manufacturing RFID tag
US20090096614A1 *	2007-10-15	2009-04-16	Innovatier, Inc.	Rfid power bracelet and method for manufacturing a rfid power bracelet
US8650097B2 *	2007-12-03	2014-02-11	Yu Yung Choi	System and method for streamlined registration of products over a communication network and for verification and management of information related thereto
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090181215A1 *	2008-01-15	2009-07-16	Innovatier, Inc.	Plastic card and method for making a plastic card

IPR2025-00645 Page 01707

US7744005B2 *	2008-01-16	2010-06-29	Taiwan Name Plate Co., Ltd.	Induction card with a printed antenna
US8016194B2	2008-03-06	2011-09-13	Imation Corp.	Mobile data storage device reader having both radiofrequency and barcode scanners
TW200949710A *	2008-05-16	2009-12-01	Unibase Technology Co Ltd	UHF Radio-frequency label
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US8350704B2	2008-10-03	2013-01-08	Neology, Inc.	Non-transferable radio frequency identification label or tag
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
KR101054448B1 *	2009-05-25	2011-08-04	주식회사 아그젝스	How to manufacture HF RFID antenna by direct printing method
DE102009038511A1 *	2009-08-25	2011-03-10	ASTRA Gesellschaft für Asset Management mbH & Co. KG	Folded and printed care label for textiles
US8238095B2 *	2009-08-31	2012-08-07	Ncr Corporation	Secure circuit board assembly
WO2011123553A2 *	2010-04-02	2011-10-06	Visa International Service Association	Crack embossing using diamond technology
TW201137762A *	2010-04-23	2011-11-01	Chung Shan Inst Of Science	System and method for determining whether an individual to be identified as a registered individual
CN102270407A *	2010-06-01	2011-12-07	罗嘉尔	Adhesive material with mark structure
WO2012094436A2 *	2011-01-04	2012-07-12	Tufts University/Trustees Of Tufts College	Electronic components on paper-based substrates
US8805193B2 *	2011-02-17	2014-08-12	Avery Dennison Corporation	Remotely powered optical output labels
EP2748771A1 *	2011-08-26	2014-07-02	Identive Group, Inc.	Card lamination
CN107634148B *	2011-11-14	2019-09-17	Lg化学株式会社	Bonding film
KR101272206B1 *	2012-01-13	2013-06-05	아로 주식회사	Manufacturing method of thin type nfc antenna using thermally curable resin composition
US9122968B2 *	2012-04-03	2015-09-01	X-Card Holdings, Llc	Information carrying card comprising a cross-linked polymer composition, and method of making the same
US9665814B2 *	2012-05-30	2017-05-30	Black Card Llc	Multi-layer metal-carbon transaction cards and associated methods
US9898694B2	2012-05-30	2018-02-20	Black Card Llc	Tri-layer transaction cards and associated methods
KR101177730B1 *	2012-05-30	2012-08-30	주식회사 나노엑	Wireless antenna for both radio frequency identification and wireless charging with electromagnetic waves absorber, and manufacturing method thereof
KR101409296B1	2012-09-07	2014-06-24	서울대학교산학협력단	Method of selective activation for magnetic nanoparticle and selectively activated magnetic nanoparticle
EP2994006B1 *	2013-05-09	2017-03-29	Gaming Partners International Usa Inc.	Secure value tokens
KR102086098B1 *	2013-07-03	2020-03-09	삼성디스플레이 주식회사	Display device
CN103440520B *	2013-08-15	2016-06-08	中电智能卡有限责任公司	Packaging process and the Pressure sensitive adhesive tape thereof of double-interface card stick up mechanism
KR102126276B1 *	2013-08-30	2020-06-25	삼성디스플레이 주식회사	Organic light emitting display
US10204297B2 *	2014-10-06	2019-02-12	Itire, Llc	Smart tag assembly for mounting on an object to be tracked
KR101589669B1 *	2014-04-29	2016-02-03	(주)샌스앤커넥트	Clothes tag manufacturing apparatus capable of nfc communicating and method thereof
WO2015174633A1 *	2014-05-15	2015-11-19	주식회사 아이티엠반도체	Antenna module package
KR101602832B1 *	2014-05-15	2016-03-11	주식회사 아이티엠반도체	Package of battery protection circuits having NFC antenna and battery pack including the same
KR101666160B1 *	2015-03-13	2016-10-13	코나씨 주식회사	a carbon fiber of decorations plastic card process

IPR2025-00645 Page 01708

US20160379943A1 *	2015-06-25	2016-12-29	Skyworks Solutions, Inc.	Method and apparatus for high performance passive-active circuit integration
DE102016004448A1 *	2016-04-12	2017-10-12	Giesecke+Devrient Mobile Security Gmbh	Location information of a coil
WO2017210305A1	2016-06-01	2017-12-07	Cpi Card Group - Colorado, Inc.	Ic chip card with integrated biometric sensor pads
WO2018035258A1 *	2016-08-16	2018-02-22	Cpi Card Group - Colorado, Inc.	Improved ic chip card
EP3779989A4 *	2018-04-04	2021-05-26	SONY Corporation	Cartridge memory, recording medium cartridge, and method for producing same

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
TWI457835B	2014-10-21	An article carrying a thin film integrated circuit
US8136735B2	2012-03-20	ID label, ID card, and ID tag
KR101207442B1	2012-12-03	Method for manufacturing thin film integrated circuit device, noncontact thin film integrated circuit device and method for manufacturing the same, and idtag and coin including the noncontact thin film integrated circuit device
US7271076B2	2007-09-18	Manufacturing method of thin film integrated circuit device and manufacturing method of non-contact type thin film integrated circuit device
CN100502013C	2009-06-17	Method for manufacturing thin-film semiconductor circuit, and element substrate
CN1922727B	2011-12-21	Manufacturing method of semiconductor device, integrated circuit card, ic tag, rfid, transponder, bill, negotiable securities, passport, electronic apparatus, bag, and clothing
KR101024958B1	2011-03-25	Ic card and booking account system using the ic card
TWI374486B	2012-10-11	Method for manufacturing integrated circuit
KR101476625B1	2014-12-26	Semiconductor device
JP4999757B2	2012-05-30	ID label, ID tag and ID card
KR101205195B1	2012-11-27	Semiconductor device
CN101395617A	2009-03-25	Semiconductor device and method for operating the same
JP5110766B2	2012-12-26	Method for manufacturing thin film integrated circuit device and method for manufacturing non-contact type thin film integrated circuit device
JP4912586B2	2012-04-11	Method for manufacturing thin film integrated circuit device
JP4761779B2	2011-08-31	ID labels, ID cards, ID tags, and articles
JP4776940B2	2011-09-21	Integrated circuit, semiconductor device, and wireless chip
JP5159178B2	2013-03-06	Semiconductor device
JP4727280B2	2011-07-20	Product management system

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2004027699		2004-02-04	

Legal Events

Date	Code	Title	Description
2014-10-21	GD4A	Issue of patent certificate for granted invention patent	

Data provided by IFI CLAIMS Patent Services

IPR2025-00645 Page 01709

About Send Feedback Public Datasets Terms Privacy Policy

IPR2025-00645 Page 01710

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/021,347	**01/10/2022 08:09:49 PM ET**	**18.115.001US9.10**

Title of Invention

MOBILE PHONE WITH MAGNETIC CARD EMULATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	2310	FILED BY	Katherine Campbell
PATENT CENTER #	60480316	FILING DATE	09/15/2020
CUSTOMER #	35781	FIRST NAMED INVENTOR	Siva G. Narendra
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Usman Mughal

Documents

TOTAL DOCUMENTS: 51

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
Campbardo_ITMI981564.pdf	3	Foreign Reference	83 KB
Carpier_FR2788646.pdf	11	Foreign Reference	139 KB
Christensen_DE60026768T2.pdf	6	Foreign Reference	98 KB
Combaluzier_WO2000014678.pdf	7	Foreign Reference	102 KB
Cowling_GB2316908.pdf	5	Foreign Reference	75 KB
Felt_AT399405T.pdf	9	Foreign Reference	127 KB

FukuokaShinichiro_JP3614157.pdf	10	Foreign Reference	205 KB
Fukushima_JP2523960.pdf	4	Foreign Reference	88 KB
Furuhashi_EP0720102.pdf	24	Foreign Reference	275 KB
Furukawa_Hideyuki_JP4086584.pdf	8	Foreign Reference	140 KB
Grasl_DE19928733.pdf	6	Foreign Reference	115 KB
Husemann_CA2337672.pdf	16	Foreign Reference	167 KB
Hutchison_KR20030072203A.pdf	12	Foreign Reference	155 KB
Ito_JP4053704.pdf	13	Foreign Reference	231 KB
Ito_JPH1097599.pdf	8	Foreign Reference	126 KB
Kaarle_CN1653751.pdf	14	Foreign Reference	166 KB
KangSangWook_KR101149887.pdf	10	Foreign Reference	436 KB
Katayama_JP3839288.pdf	8	Foreign Reference	135 KB
Kayanakis_FR2801709.pdf	8	Foreign Reference	129 KB
Kobayashi_EP0541818.pdf	10	Foreign Reference	155 KB
Kokubu_JP3180086.pdf	4	Foreign Reference	110 KB
Korshun_CH690048.pdf	9	Foreign Reference	131 KB
LeeByeongHoon_KR100604877.pdf	10	Foreign Reference	166 KB

MasuyamaHiroshi_JP4515793.pdf	11	Foreign Reference	182 KB
Minemura_JP2005202914.pdf	8	Foreign Reference	153 KB
Mizushima_Eiga_JP4322021.pdf	13	Foreign Reference	206 KB
Murakami_JP3641230.pdf	14	Foreign Reference	172 KB
Natsuno_JP2001167187.pdf	20	Foreign Reference	174 KB
Newcom_AUPP411098A0.pdf	6	Foreign Reference	114 KB
Nishizawa_CN1218276C.pdf	15	Foreign Reference	197 KB
NishizawaHirotaka_JP4412947.pdf	13	Foreign Reference	208 KB
OnTrack_IL119943.pdf	8	Foreign Reference	121 KB
Peek_WO1996026500.pdf	7	Foreign Reference	96 KB
Rancien_FR2868987.pdf	6	Foreign Reference	147 KB
Smets_MX2007000546.pdf	12	Foreign Reference	183 KB
TakagiYoshihiko_JP4624732B2.pdf	20	Foreign Reference	205 KB
Terho_FI99071C.pdf	29	Foreign Reference	286 KB
Vazvan_FI100137.pdf	12	Foreign Reference	172 KB
Wong_AU6159601A.pdf	3	Foreign Reference	78 KB
Amtmann_AU2002366416.pd	3	Foreign Reference	82 KB

f			
Arai_TWI457835.pdf	29	Foreign Reference	250 KB
Arakaki_AU5079498.pdf	5	Foreign Reference	82 KB
Breck_WO2001067355.pdf	60	Foreign Reference	457 KB
Burger_CA2388007.pdf	35	Foreign Reference	274 KB
Nagaoka_JP3180086B2.pdf	19	Foreign Reference	217 KB
Rienzo_AU4831500A.pdf	4	Foreign Reference	91 KB
Thomas_WO2003081519A2.pdf	38	Foreign Reference	285 KB
Bando_WO2003010939A1.pdf	5	Foreign Reference	112 KB
Fukuoka_Shinichiro_JP3614157B2.pdf	10	Foreign Reference	190 KB
Halpern_WO2002071311A3.pdf	6	Foreign Reference	103 KB
18P115001US9_10_IDS.pdf	13	Information Disclosure Statement (IDS) Form (SB08)	1032 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
Campbardo_ITMI981564.pdf	EE9E394A607EBC32625DE0517DF34083E625424886A65F3D6A50BE4C1DA9E04FBA057DA44ED3DFF72D2B2F7597FE92C67F0D4C141057A5560DA0D98990CE498B
Carpier_FR2788646.pdf	DDCEC7607CE66BE253CD9451968E778A6D1D5DC812A11D00

	C052CC1A644385703C23FDCBE037D617B58FD69B4381DBBB EC83564F2BA1E183245CEF735550FC9A
Christensen_DE60026768T2.pdf	09C387BE00436CCB65B4FF64AC1BBC8CF529DCE39080F9205 B185C3288CDC87716CD8C667214E57B89AD271A046091401F BE1FE39996E278D89B97FC8ABAF7F4
Combaluzier_WO2000014678.pdf	E2D65D4BC6B7AF64B72B2550286AC965E49B1BAE89DE9605 DDAC77F279E2ABEA2519F720006D203D837DE3A352B7C6382 B8BCC648DA52A1B44A51F557B8FB00F
Cowling_GB2316908.pdf	9850427E22C7BCF3830F1349061889B2436CC863ABA721AAC9 76A5472FB2735B103F69041BF38694B491DD32E3F6CB3B11E0 C96FF604332C9611197420F95684
Felt_AT399405T.pdf	0DCE1725BFE4634D9D390C95AA7075FB8E42C6E032DDA58B 8EC782C761B66827C7BE41B52506B5AF3E9DBE5466454E60E 4CAE964F6CBDCBB0CA94E7728562F2C
FukuokaShinichiro_JP3614157.pdf	15C74A908041A0175308DA575CD08A29B969CBEFDAED6708A 972A5959A2310B3AE11A7B43D084F8DE049A999CEC5B4A069 20D91869B91FA1D6C1EEEEE92E3555
Fukushima_JP2523960.pdf	6A1A244049057FE48368DBA9FD1568B835BE0D049B916944F1 BA02E7A1E11AC67600557E95E52929E5474FB16A7E31D4FF57 624A022DCBB06DF4A583A03F2B84
Furuhashi_EP0720102.pdf	648AECE8F352E865E3D505AA4542BCE24E56341D7EB64DFF0 88C54C55720D86FCBA6AF66B4CBD569366434496C955455DF 1536D5B560EFE1BCFED74464511A43
Furukawa_Hideyuki_JP4086584.pdf	98D1F154D48F4F3D8AA554E6034D4457F9BED500E3C627A5F 192B48B3872C8416726B6BA89F9012DB19DADC0DB20B6BBE1 A33B85CB8B6D157CBFB32E65F662F0
Grasl_DE19928733.pdf	ADCC23D2F80A6A099AA3FB2A7BC88DECA5B39F05AF25B00E C63314D99205B2F5C16CC05FEE2A801CAB4E6508281B7CDD 1DEC852CDE30E3E7A9DCB680B7864097
Husemann_CA2337672.pdf	FD6CF49A938B684F7F716FEDE1FA9A3479DE4110F71571DC1

	A8263BDA05BBA2E2CF2892E87A42C62316590861CA5ACCB1021DE6A6A4098BC4AC95D0145A65557
Hutchison_KR20030072203A.pdf	070BB512C3E735886ECDB92574ECDA68D35BC45633642F9809F0595C2617517CC7175C33AA83DB87CC4D0F01B70A404A639FFC8167B7EE1500BC11EF6ED6186F
Ito_JP4053704.pdf	150978D851A6BD7D8847C31E03B6AFDE6D782E82D2D7212AECE0967972ACBD506A797052FAC9D93C4150FB258A1B2C2ABB5FC8833D307FAEF588EF554660828F
Ito_JPH1097599.pdf	15A3F06C4EF43749D715142328C2C2E2F6B907812A0598B546F637C0B2F14C3C05BDF68AFCC6D77CAB26793B0C1E33C061F40934A230C15D27BB46CC9093AA5C
Kaarle_CN1653751.pdf	E96C2D5110750DF8B01D3375F25BCD9E39BA6D0AFA4B6A43C7971643FDC5C08FCD8F246D16404EE3AA1BBD8E1941DBD04EC15A192F9CA1A77DA343145E0E59B5
KangSangWook_KR101149887.pdf	4026CFC2716C291CF361FDA86E9C1A19B6E177D541B41F268245C90AF1D612CDB14DE053E6867454F39CF1F83B25CAFB5A896E5F6792D3432B0F3AFC0802E479
Katayama_JP3839288.pdf	5A9FB5B740393CE7382C65A405443E441EEF1615A702F78BE15D167288400C64499A31A1E0C47518BFF18EA2828B0705FC1F49727B2503B6089FFA8172A403B1
Kayanakis_FR2801709.pdf	7D45F9A4F3D0722B480E8D99F73E908C9E02DC9B4E4D4FDEBC2FFB07259B8D6E0EEDCF541359738020BD27D9544739B781D51E63B840C9B39BD324009F302887
Kobayashi_EP0541818.pdf	FA61310D03CCBDAC4AD6DF33E75F9CFD76768C28E43583612C7F0C0E57D1313AE7709EB607EE2CD7BD118490070C90F5ACBE93BECC023CD6C04E5E5B2C154039
Kokubu_JP3180086.pdf	10B70135DDA04792B814F9FABD1F8B09E7CB2B12B2B8483FBEC56F1BA568E86A2554F03DD435E4F222A277E4C2EAFA384BF0579012A3BA059D5B609B0DFB2EDB
Korshun_CH690048.pdf	B052CD213D92AB6B3306AD416C3226D6686B62F6754D2A111

	ABC6BD4441AA60C28D62C13C9DC7DA9FD3039250784B0C70029D007EE0C1623BBA76CE21C04A327
LeeByeongHoon_KR100604877.pdf	CCD6D071B6B37AFD08D1DEB56DAC16A549B0B83DEA3919E1EC98BE37F783E816BDD46D6251F9B85A7597CFE8E08C7A5CC9F27FABE51A385A49EF675E544A2ECB
MasuyamaHiroshi_JP4515793.pdf	A976A96DE7B4E8DD005E92249A0AFE854EF9051651A395DA38BD160A9246A619DE24EB718B37B6B9A1A55B0D340DD9F9BEF6A5E7E0918667CF29D5C1DF2173BD
Minemura_JP2005202914.pdf	826FFE15996772303D706313EE52CB2CAE82014E7115E5590480E5CAA82A69C099E982BCABE55ACB8E932D98658395EA41F36FB2EB9868334847D8DA393CD0D6
Mizushima_Eiga_JP4322021.pdf	9D33C440EDEED1BBD6CF718D9F3B457B72E46B5B01071B8E7DBFC6AEFEE3376016CCD99DEE7CD4A35FA88833041F6314E8F7BAEB1C06FEC148F1EA2520575DCD
Murakami_JP3641230.pdf	877FA08C2047DE5B618E667DCD1D728233B18A75D1263780CF2A836149CEC04DEC678DA48E23A7F13041942366D7839CDF1BC4A14A6EA01F1E179D057893BC37
Natsuno_JP2001167187.pdf	6E86B51E3F7226D3B6E97132D27F8308E12F133D453F49B82EA42043C03D721EF4F6C737BC5E615E58C76AC02C1EF44A8C4102C0773924595OC20E960A6891EE
Newcom_AUPP411098A0.pdf	A84EC446ED08FE93BBDCD98F7217DF3FEC440A48AD37656E2706637731B37373C52EBB062FAD2C753A0B79AC2D0217DE11FED9258E0930437B1BCF0D03C498D6
Nishizawa_CN1218276C.pdf	F0D4E802CEEE90992E88BD792EBAFA7F7DF827F9CD6B54AE2D2D9797F8569319D97A2F2476C6FAC36CB776EBB7A0BA041FB8F89DF1AF84B319277207D7E592F1
NishizawaHirotaka_JP4412947.pdf	57C682817A424516B15F74D8EAE3E3A0553077711D6CB175AC9F7B238C6254E2E8963E4F5120D9750B4C937B5D6E0937CF75327AF52448B0DC749FBA0F54A680
OnTrack_IL119943.pdf	44FA582B41F952AC6BEE35F7099D80E99C7FE81A2B0088DDA

	AA1ED46CE301E6F64E3E883E4392911B68930F8C7062717B91D704458BC11CD539A9154A008E6B5
Peek_WO1996026500.pdf	93D03E789563DC935DEE4CE7CEE1975149DA23FBAB276DED0E521E5970C960BC12506B82CA5E614CA0E4C067D3F8C6579BDED65A992949BBBAF98029D13DA1EB
Rancien_FR2868987.pdf	27AD99948B0E8EF1165A510ECCBF6FC1FC788677FDB615F69EF8A2D06E69DD37F08F73A63364E29BCAF8DEBF3AC0C97987AB0241E8FB0AB73855F42246DB0E69
Smets_MX2007000546.pdf	1F1A9E60C212CAEB3F3A3AA474F9495E2D8BB052E3F718A16E6040653D2794D402D57EE9BECC4B35A75295B848464C4867D30D5418E37C61D1E0CBC408910CC1
TakagiYoshihiko_JP4624732B2.pdf	5F72EABB6335E40FED296C37E41FC688251A91C6E4CA2C526E770F4016E4BFE54663F7253263FAA85D9A13DA1AD34449B0EAB21172FD13FEFEA7C92D7B3C97E1
Terho_FI99071C.pdf	2A4056FA199AB2EB317304E91F245A166DA3DA6FA039F12F858641ED1B9E5538AC2BB9570C1FF3EC9848BF2C58B69DB177B9CDE5B623BBB4E94B0719F7A50039
Vazvan_FI100137.pdf	B2B54EA7B10B455C9D2809F52717218CE6BFB94FB0C7BF4E18D5ECE79943E8E0373DC77D17C2E40A18B75DFB1513E434F2DD3AECD2C285F3ABC254A0AF45D630
Wong_AU6159601A.pdf	C48043C82A2C23CC8EE4B77449A242F8F1253412D5ADACA148A9A4A10D7F36867E513DC646B07BA44998C8FA484C23AA9E11F0A75A0237B227964D3EEBE9E92B
Amtmann_AU2002366416.pdf	AE3C508693D7017501EDD5EE949177625A88456E7E67B1C5F1D3519DAB6C570D37DCCA562B4CC75169C237CFEF5258EC852AD194A1073F4A4B3A630C70446743
Arai_TWI457835.pdf	61966DE35465493CAAA6300367B58380D4BE0A85FA453316A0D17556443CDAA53B1188D8EEBE817416BBC2D4EC094497788B6CDCCF3F0D24D3784B377DE2246AC
Arakaki_AU5079498.pdf	8D19906E4AE85225910AC3C62EEFAB0488CF567A555B508CD

	1558638DA7B1B39D37A8F51FA35931737A4653F760216CF4CD AE2ECB2E2AAE3919A37D3BBC3D6A6
Breck_WO2001067355.pdf	70D103C2359F7AD1083F68782EEE9AFD5887C41DEE82115AF C45D4D7B0E28F68B9497D7347D82704ADFA254CF06ACE3972 CBC544CA0A8BA761423C3D3B0C5471
Burger_CA2388007.pdf	980D54100D9229E3A4D035B0C5BA0A5DE601E0082C57425F8 CE3CC69FADE05BEEAD5D20C174F2AD91B05E9D0747546BA5 75B029E7E2FF4CBBE0A5DDEE55768A9
Nagaoka_JP3180086B2.pdf	902246859DE0C58E17E788FD121FF1815D90873B5F64F52CEB 464F8D9E3D3F1D502D13DD465E46768292FC02190EE8343EC D0D6BDA1619F42A33391357B0FCD1
Rienzo_AU4831500A.pdf	5CD35C7A3B0E9E229C871F2121F486D80167F5DE62BDDBD48 747A42A941B232DEC9459E6628608BA0B8A6378F4248480236 1DE5FDCB4445DF365C7EAB8C83C96
Thomas_WO2003081519A2.pdf	AC70DFEC0E01F0BE96779A53C226DF54ACDD3A6FD9C819D1 C58E899DEBE40C7ABA0A3AD6D05228ED7EACBC333096D74 B63585EDDDF25D89DF3D54C1397B2B22C
Bando_WO2003010939A1.pdf	F17D12E9234D1C4D0EEF1BC1A5FB7EBF8576CED27002EFA2 9D6C0EB57E383C03BD8EF8BC172B0AA678C6ECE9FC736F32 FE80E389B34A4B57CE704DB4118A685C
Fukuoka_Shinichiro_JP3614157B2.pdf	AFE627EDCCC45452D930C120FA9F52A528C20011A1B14EBC 1F30810728236EC13817FFE379B528246CD45A04B0D18152D6 E3765637F303D0338678B25ED00E07
Halpern_WO2002071311A3.pdf	91F11217A49C470032892B6F341177C7D12601A24135969ED41 F9055F859B7233706D973B905D3B807BCE393B940CFF8DE7C CC6534CE5C79A41C6794FD858B1C
18P115001US9_10_IDS.pdf	0BF22EBD7C64EC96EA44E9172C281270547579988 8A77EAF74 848F066508CF66C039B8812375203172A5940B712CA42BFA06 CCBF711314036FE81023CE9CB97D

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Patents 2002071311

Mobile phone communications system with increased functionality

Abstract

The invention relates to a mobile telephone and a smart card transaction system in combination, where the functionality of a mobile telephone is increased so that the phone can be used in a large range of transactions for which smart cards are normally used. The phone may also be provided with a slot to receive smart cards and re-charge them with funds for cashless transactions, by communicating with a bank account or the like.

Classifications

» G06Q20/32 Payment architectures, schemes or protocols characterised by the use of specific devices or networks using wireless devices

View 7 more classifications

WO2002071311A3

WIPO (PCT)

Download PDF Find Prior Art Similar

Other languages: French

Inventor: John W Halpern

Worldwide applications

2001 WO US EP AU

Application PCT/EP2001/002571 events

2001-03-07 Application filed by Halpern John Wolfgang

2001-03-07 Priority to PCT/EP2001/002571

2002-09-12 Publication of WO2002071311A2

2002-11-21 Publication of WO2002071311A3

2004-02-26 Publication of WO2002071311A8

Info: Patent citations (16), Non-patent citations (1), Cited by (39), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, PatentScope, Discuss

Patent Citations (16)

Publication number	Priority date	Publication date	Assignee	Title
EP0384829A1 *	1989-02-21	1990-08-29	France Telecom	Multicolour electroluminescent flat panel display having a memory effect
US5181025A *	1991-05-24	1993-01-19	The United States Of America As Represented By The Secretary Of The Air Force	Conformal telemetry system
JPH06268724A *	1993-03-15	1994-09-22	Hitachi Ltd	Folding type portable electronic equipment
US5553314A *	1994-04-12	1996-09-03	Motorola, Inc.	Method of configuring a communication unit using a wireless portable configuration device
WO1996033594A1 *	1995-04-18	1996-10-24	Cambridge Display Technology Limited	Electroluminescent device
GB2314179A *	1996-06-12	1997-12-17	John Quentin Phillipps	Display and input arrangements for portable electronic apparatus
EP0820178A2 *	1996-07-15	1998-01-21	Motorola Inc.	Contactless smartcard for use in cellular telephone
GB2321551A *	1996-03-22	1998-07-29	John Wolfgang Halpern	Reading smartcards
WO1998058509A1 *	1997-06-16	1998-12-23	Swisscom Ag	Chip card and method for communication between an external device and a chip card
GB2331889A *	1997-11-28	1999-06-02	Nec Corp	Cellular telephone having an additional earphone/microphone
GB2348521A *	1999-04-01	2000-10-04	John Wolfgang Halpern	Pocketsize carrier for information storage and information exchange
Family To Family Citations				
GB2275548B *	1993-03-04	1996-11-13	Landis & Gyr Energy Management	Smart card
US5497411A *	1994-03-14	1996-03-05	Pellerin; Joseph C. E.	Telecommunications card-access system
SE506506C2 *	1995-04-11	1997-12-22	Au System	Electronic transaction terminal, telecommunication system including an

				electronic transaction terminal, smart card as electronic transaction terminal and method of transferring electronic credits
JP3309898B2 *	1997-06-17	2002-07-29	日本電気株式会社	Power circuit
SE515327C2 *	1999-08-27	2001-07-16	Ericsson Telefon Ab L M	Device for carrying out secure transactions in a communication device

* Cited by examiner, † Cited by third party

Non-Patent Citations (1)

Title
PATENT ABSTRACTS OF JAPAN vol. 018, no. 675 (E - 1648) 20 December 1994 (1994-12-20) *

* Cited by examiner, † Cited by third party

Cited By (39)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US20040230489A1 *	2002-07-26	2004-11-18	Scott Goldthwaite	System and method for mobile payment and fulfillment of digital goods
US20040127256A1 *	2002-07-30	2004-07-01	Scott Goldthwaite	Mobile device equipped with a contactless smart card reader/writer
GB2396538B *	2002-12-20	2005-12-14	* Motorola, Inc	Wireless communication device,associated smartcard and method of operation therefor
JP4391134B2 *	2003-05-30	2009-12-24	株式会社日立製作所	Mobile terminal and its management device
KR100423401B1 *	2003-06-24	2004-03-18	(주) 엘지텔레콤	Account transfer/remittance system by mobile-phone and the method
US7337407B2 *	2003-06-24	2008-05-20	Lg Telecom, Ltd.	Method for providing banking services by use of mobile communication system
JP2005159607A *	2003-11-25	2005-06-16	Matsushita Electric Ind Co Ltd	Portable communication apparatus
DE602004020684D1	2004-03-19	2009-05-28	Nokia Corp	ND METHOD FOR IMPROVING TERMINAL OPERATION
FR2870067B1	2004-05-05	2006-06-16	Radiotelephone Sfr	METHOD OF RECHARGING A SUBSCRIPTION CARD BY WIRELESS EQUIPMENT
WO2005119607A2 *	2004-06-03	2005-12-15	Tyfone, Inc.	System and method for securing financial transactions
US7715888B2 *	2004-07-29	2010-05-11	Kyocera Corporation	Portable electronic device
WO2006018906A1 *	2004-08-16	2006-02-23	Matsushita Electric Industrial Co., Ltd.	Portable terminal
JP2006072115A *	2004-09-03	2006-03-16	Fuji Photo Film Co Ltd	Image display device
US20110071949A1 *	2004-09-20	2011-03-24	Andrew Petrov	Secure pin entry device for mobile phones
US20060064391A1 *	2004-09-20	2006-03-23	Andrew Petrov	System and method for a secure transaction module
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
JP4188340B2 *	2005-05-10	2008-11-26	ソニー・エリクソン・モバイルコミュニケーションズ株式会社	Mobile terminal and function restriction method
US20070145135A1 *	2005-12-28	2007-06-28	Fabrice Jogand-Coulomb	Methods used in a nested memory system with near field communications capability
US20070145152A1 *	2005-12-28	2007-06-28	Fabrice Jogand-Coulomb	Nested memory system with near field communications capability
US7991156B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US8220633B1 *	2007-07-27	2014-09-02	United Services Automobile Association (Usaa)	System and methods related to an available balance debit/credit card
US8228020B2 *	2007-12-11	2012-10-09	Lg Electronics Inc	Digital broadcasting receiver and a data processing method
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices

IPR2025-00645 Page 01722

US10002384B1 *	2007-12-20	2018-06-19	Jpmorgan Chase Bank, N.A.	Automated card notification system and method
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100102123A1 *	2008-10-28	2010-04-29	First Data Corporation	Systems, Methods, and Apparatus for Facilitating Access to Medical Information
US8550361B2 *	2008-10-28	2013-10-08	First Data Corporation	Systems, methods, and apparatus to facilitate locating a user of a transaction device
US20100102131A1 *	2008-10-28	2010-04-29	First Data Corporation	Systems and Methods for Disabling a Contactless Transaction Device
US10803515B2 *	2008-10-31	2020-10-13	First Data Corporation	Systems, methods, and apparatus for using a contactless transaction device reader with a computing system
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US20110010283A1 *	2009-07-09	2011-01-13	Eddie Williams	E-card
EP2369543A1 *	2010-02-26	2011-09-28	Deutsche Telekom AG	Mobile electronic device with authentication function for using transaction-based services and system comprising same
TWI537851B *	2011-05-04	2016-06-11	jian-gang Yang	Mobile transaction method and hand-held electronic device
US9659291B2	2011-05-04	2017-05-23	Chien-Kang Yang	Method for processing a payment
US10509991B1	2019-03-18	2019-12-17	Capital One Services, Llc	Detection of images in relation to targets based on colorspace transformation techniques and utilizing infrared light
US10467445B1 *	2019-03-28	2019-11-05	Capital One Services, Llc	Devices and methods for contactless card alignment with a foldable mobile device

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
WO2002071311A3	2004-02-26	Mobile phone communications system with increased functionality
TW364245B	1999-07-11	Wireless transaction and information system
WO2005020028A3	2005-07-14	Intelligent transaction router and process for handling multi-product point of sale transactions
WO2001065494A3	2001-12-20	System, and method for prepaid anonymous and pseudonymous credit card type transactions
SE0004820D0	2000-12-22	Procedure for increasing security when paying by credit and debit card
WO2006019997A3	2007-04-12	Method and system for conducting contactless payment card transactions
WO2007030480A3	2007-06-21	System and method for secured account numbers in proximity devices
ES2143790T3	2000-05-16	Method to securely debit an electronic payment method
WO2005004070A3	2005-03-03	System and method for conducting secure electronic transactions
WO2006031626A3	2007-04-26	Purchase notication alert forwarding system and method for preventing fraud
EP0933733A3	2003-10-29	Method and system of contactless interfacing for smart card banking
TW200636592A	2006-10-16	Electronic transaction card
WO2007033071A3	2007-12-13	Calling card with intergrated banking functions
AU2002356470A1	2003-06-10	Credit card payment by mobile phone
AU3042801A	2001-08-07	Banking system with enhanced identification of financial accounts
WO2006052815A3	2006-10-26	Purchase card system and method therefor
EP1544819A3	2006-03-01	Wireless banking system and wireless banking method using mobile phone
WO2005086593A3	2006-07-06	Inter-operable, multi-operator, multi-bank, multi-merchant mobile payment method and a system therefor
WO2004049093A3	2005-06-30	Scheme for spreading and facilitating remote e-services
NO320649B1	2006-01-09	Mobile radio terminal equipped with extra reader for smart card

IPR2025-00645 Page 01723

TNSN07308A1	2008-12-31	Electronic system and method for recharging credit cards
WO2003092348A3	2003-12-11	The operational method and system of the telecommunication device for the electronic cash
AU2002344068A1	2003-06-10	Prepaid card information issuing system, call rate settlement system, communication rate settlement system, and expense settlement system
WO2002049322A3	2002-09-06	Mobile communication unit
WO2002086676A3	2004-02-26	System and method for using a prepaid card

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
PCT/EP2001/002571	2001-03-07	2001-03-07	Mobile phone communications system with increased functionality

Applications Claiming Priority (4)

Application	Filing date	Title
AU2001239280A	2001-03-07	Mobile phone communications system with increased functionality
EP01913849A	2001-03-07	Mobile phone communications system with increased functionality
PCT/EP2001/002571	2001-03-07	Mobile phone communications system with increased functionality
US10/469,616	2001-03-07	Mobile phone communications system with increased functionality

Legal Events

Date	Code	Title	Description
2002-09-12	AL	Designated countries for regional patents	**Kind code of ref document**: A2 **Designated state(s)**: GH GM KE LS MW MZ SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
2002-09-12	AK	Designated states	**Kind code of ref document**: A2 **Designated state(s)**: AE AG AL AM AT AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ CZ DE DE DK DK DM DZ EE EE ES FI 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 SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
2002-11-06	121	Ep: the epo has been informed by wipo that ep was designated in this application	
2002-11-21	AL	Designated countries for regional patents	**Kind code of ref**

IPR2025-00645 Page 01724

			document: A3 **Designated state(s)**: GH GM KE LS MW MZ SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
2002-11-21	AK	Designated states	**Kind code of ref document**: A3 **Designated state(s)**: AE AG AL AM AT AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ CZ DE DE DK DK DM DZ EE EE ES FI 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 SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
2003-02-06	DFPE	Request for preliminary examination filed prior to expiration of 19th month from priority date (pct application filed before 20040101)	
2003-09-02	WWE	Wipo information: entry into national phase	**Ref document number**: 2001913849 **Country of ref document**: EP
2003-09-04	WWE	Wipo information: entry into national phase	**Ref document number**: 10469616 **Country of ref document**: US
2003-12-03	WWP	Wipo information: published in national office	**Ref document number**: 2001913849 **Country of ref document**: EP
2004-01-22	REG	Reference to national code	**Ref country code**: DE **Ref legal event code**: 8642
2004-02-26	CR1	Correction of entry in section i	**Free format text**: IN PCT GAZETTE 37/2002 DUE TO A TECHNICAL PROBLEMAT THE TIME OF INTERNATIONAL PUBLICATION, SOME INFORMATION WAS MISSING UNDER (81). THE MISSING INFORMATION NOW APPEARS IN THE CORRECTED VERSION

IPR2025-00645 Page 01725

2004-02-26	CFP	Corrected version of a pamphlet front page	
2004-12-10	NENP	Non-entry into the national phase	Ref country code: JP

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents JP2523960

Document editing device

JP2523960B2
Japan

Find Prior Art Similar

Other languages: Japanese

Inventor: [redacted]

Worldwide applications

1990 JP

Application JP2218924A events

1990-08-22 Application filed by [redacted]
1990-08-22 Priority to JP2218924A
1992-04-03 Publication of JPH04102112A
1996-08-14 Application granted
1996-08-14 Publication of JP2523960B2
2010-08-22 Anticipated expiration
Status Expired - Lifetime

Info: Patent citations (1), Cited by (5), Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (1)

Hide Dependent

(57) [Claims]

1. 1. A memory card interface circuit capable of accessing a memory card in at least an input device for inputting desired characters, a display device for displaying input / editing results, and a document editing device having a built-in battery. An insertion port that can share a connection terminal that can connect a power supply interface circuit that can supply power from a connection terminal and a battery, and has a battery detection device that can detect that a battery is inserted in this insertion port,

   The document editing apparatus is configured to charge the built-in battery through the power supply interface when it is detected that a battery is inserted into the insertion port.

Description

DETAILED DESCRIPTION OF THE INVENTION [Industrial field of application] The present invention relates to, for example, a Japanese word processor,
The present invention relates to a document editing device having functions such as document input, editing, and printing.

[Conventional technology]

In recent years, there are notebook type and notebook type that are lightweight and compact and easy to carry in Japanese word processors and personal computers.

[Problems to be Solved by the Invention]

Book-type and notebook-type Japanese word processors and personal computers have built-in batteries for easy use on the train or anywhere. For Japanese word processors and personal computers, an external storage device such as a floppy disk drive and a liquid crystal backlight are becoming indispensable, so the Japanese word processor,
Currently, the battery built into a personal computer can normally be used for only a few hours. Further, when a battery having a power source capacity that can be used for a long time is used, the volume and weight increase, which causes a problem that it is inconvenient to carry.

An object of the present invention is to provide a document editing apparatus which can be used for a long time and has a small volume and small weight.

[Means for solving the problem]

IPR2025-00645 Page 01727

According to the present invention, at least a desired character is input device,
A document editing device having a display device for displaying input / edit results, wherein a connection terminal capable of connecting a memory card interface circuit capable of accessing a memory card and a power source interface circuit capable of supplying power from a battery are connected. Provided with an insertion port capable of sharing possible connection terminals, and having a battery detection device capable of detecting that a battery has been inserted into this insertion port, when it is detected that a battery has been inserted into this insertion port, This can be achieved by configuring the battery to be charged via the power interface.

[Action]

A battery such as a sealed lead battery that can be made thin can be inserted into the slot of the memory card so that both power supply and memory card insertion can be performed, and the volume of the Japanese word processor and personal computer itself is small or lightweight. Also, it is possible to extend the usage time by using the battery inserted from the memory card insertion slot together with the Japanese word processor and the battery built in the personal computer, or by allowing the user to carry a battery that can be inserted from the memory card insertion slot. can do.

[Example]

An embodiment of the present invention will be described in detail below with reference to the drawings.

FIG. 1 is a view showing the appearance of a document editing device such as a Japanese word processor. 1 is a display device, 2 is an input device, 4 is a printing device, 12 is a main body, and a power supply is required for backup. A RAM (Random Access Mem) that can store data such as a card-type sealed lead-acid battery 18 in the same form as a memory card used at any time or a ROM (Read Only Memory) card that contains a program or documents
ory) indicates the slot into which the card can be inserted. Although only one of the memory card and the card-type lead-sealed battery can be inserted into the insertion slot 12 in this embodiment, a plurality of insertion slots can be provided to insert, for example, two memory cards or the memory card 1.
It is also possible to insert a sheet and a card type sealed lead battery 18. In addition, even when the insertion slot 12 is only one, when the card-type sealed lead battery 18 is inserted, the power interface circuit 16
By providing a built-in battery charging circuit 44 for charging the built-in battery 42 to the internal battery 42, the built-in battery 42 is
it can be charged without using the power supply 46 or AC adapter 45, and when using a memory card, a card-type sealed lead battery 18
Even if you can't insert into the insertion slot 12, you can use it only with the built-in battery 42. Further, when the card-type sealed lead battery 18 is inserted into the insertion port 12, it can be used for a long time as compared with the case where the built-in battery 42 alone is driven. Further, the card-type sealed lead battery 18 is smaller and lighter than the AC adapter 45 like the memory card, so that it does not cause any trouble for a plurality of users to carry around. Reference numeral 15 denotes a power switch of the main body. Even if the power switch 15 is turned off, codes such as characters input from the input device 2 and document data of edited results are backed up.

FIG. 2 is a block diagram of a document editing device such as a Japanese word processor. Reference numeral 2 is an input device such as a keyboard or a tablet for inputting a desired character or operation mode. Enter the operation command code.

The control device 3 temporarily stores the code such as characters input from the input device 2 and the document data of the edited result, and sends the pixel data to the display device 1 for display, and the output device 4,
External storage device 5, memory card interface circuit 14
And control. Further, if the card-type sealed lead-acid battery detection circuit 27 detects that the card-type sealed lead-acid battery 18 is inserted into the insertion slot 12, it can be seen that the card-type sealed lead-acid battery 18 is attached to the display device 1. Display patterns. By displaying the pattern, it is easy for the user to make a mistake as a memory card and a card-type sealed lead battery.
You can prevent 18 from being pulled out. Further, when the card-type sealed lead battery 18 is inserted in the insertion slot 12, the codes such as characters input from the input device 2 and the edited document data are backed up even when the power switch 15 of the main body is turned off. .

The output device 4 is a printer that outputs, as a hard copy, a document edited by operating the input device 2. An external storage device 5 stores edited documents, image data, and the like, and is, for example, a 5-inch or 3.5-inch floppy disk device. The memory card interface circuit 14 includes an address bus for accessing the ROM and RAM in the memory card when the memory card is inserted into the insertion slot 12, a data bus, and a control bus for controlling reading and writing. It is possible to read and write the data of the memory card of the control device 3 by connecting to the. The power supply interface circuit 16 allows the document data of the card-type seal lead battery 18 to be inserted into the insertion port 12 even if the power switch 15 of the main body is turned off, or the card-type seal lead battery 18 can be inserted electrically or mechanically. The card type sealed lead battery 18 is detected in the controller 3 by detecting that it is inserted in
If it is inserted into the card 12, or if the card-type sealed lead battery 18, the AC power supply 46 or the AC adapter 45 is connected, the built-in battery 42 is charged.
8. A circuit that allows the built-in battery 42 to be used effectively when the AC power supply 46 or the AC adapter 45 is not connected.

FIG. 6 is a diagram showing an internal block of the power supply interface circuit. The card-type sealed lead battery detection device 27 is a device that electrically or mechanically detects that the card-type sealed lead battery 18 is inserted into the insertion port 12. Built-in battery 42 is a card-type sealed lead battery 18, AC power supply 46 or AC adapter
Even when the 45 is not connected, it is usually about 3 even with the built-in battery 42.
The main body can be used for about a time, and the backup of the memory in the main body can be backed up for several years. Built-in battery charging circuit 44 is a card type sealed lead battery 18, AC power supply 46
Alternatively, if the AC adapter 45 is connected, the built-in battery 42 is charged, and the card-type sealed lead battery 18, AC power supply 46 or AC
The built-in battery 42 is used effectively when the adapter 45 is not connected.

FIG. 3 is a view showing the outer shape of the card-type sealed lead battery 18. The connector 19 is fitted with the mating connector of the insertion port 12 and connected to the power supply interface circuit 16. The external shape is the same as that of the memory card.

FIG. 4 is a view showing the inside of the card-type sealed lead battery 18. The separator 21 is sandwiched between the cathode plate 20 and the anode plate 22 and immersed in an electrolytic solution, and the cathode 26 connected from the cathode plate 20 and the anode 24 connected from the anode plate 22 have a connector structure and are inserted. Mates with the mating connector at port 12. twenty five
is a dummy connector that fits with the mating connector of the insertion port 12 but is not connected in terms of signals. On the other hand, in the case of a memory card, the connector parts corresponding to the anode 24 and the cathode 26 of the card type seal battery are not connected in terms of signals, and the connector corresponding to the dummy connector 25 is connected to the address bus, the data bus and the control signal.

Fig. 5 is a circuit block diagram of the memory card, and 37 is RA.
M card access interface device or a memory card connector that connects to a system such as a personal type Japanese word processor, 38 is a RAM part that is a storage element, for example, 2 32K bytes memory LSI, 64K bytes storage capacity have. 39 is an address decoder section for selecting a memory LSI from the address signal sent from the connector section 37 and generating a control signal for writing and reading, 40 is a battery for holding the stored contents, 41 is a power supply control section, and a memory card Controls the memory card power system by switching between the drive power supplied from the system such as the interface circuit

14 and the power supply for the battery 40, and detects the voltage drop of the battery 40 to detect the life of the battery 40. It controls the function of checking. In this embodiment, the memory card is a RAM card, but it may be a ROM card.

〔The invention's effect〕

According to the present invention, for example, in a document editing device such as a Japanese word processor, a battery such as a sealed lead battery is formed in a form that can be inserted into a memory card slot, and an insertion port that can be used for both power supply and memory card insertion. By providing it, the volume of the Japanese word processor itself can be made small and lightweight. Further, since it is possible to detect that the battery is inserted and used, it is possible to prevent the document, etc., which has been created by bending the battery carelessly, from being wasted. Further, the life of the battery is extended, the document can be created for a long time by using the battery, and the workability can be improved.

[Brief description of drawings]

FIG. 1 is a diagram showing the appearance of a document editing device such as a Japanese word processor, FIG. 2 is a block diagram of a document editing device such as a Japanese word processor, and FIG. 3 is a card type. FIG. 4 is a diagram showing the outer shape of the sealed lead-acid battery 18, FIG. 4 is a diagram showing the internal structure of the card-type sealed lead-acid battery 18, FIG. 5 is a diagram showing the circuit block of the memory card, and FIG. 6 is the inside of the power supply interface circuit. It is a figure which shows a block. DESCRIPTION OF SYMBOLS 1 ... Display device, 2 ... Input device, 14 ... Memory card interface circuit, 16 ... Power supply interface circuit, 27 ...
Battery detection device.

Front page continuation (72) Inventor Shigeru Matsuoka 1-1-1, Higashitaga-cho, Hitachi-shi, Ibaraki Hitachi Ltd. Taga factory (56) Reference JP-A-3-244013 (JP, A)

Patent Citations (1)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
JP2973212B2 *	1990-02-22	1999-11-08	株式会社ソーテック	Removable hard disk drive and battery replacement structure for portable computer expansion

* Cited by examiner, † Cited by third party

Cited By (5)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
JP2011057738A *	2009-09-04	2011-03-24	Ube Industries Ltd	Method for producing polymer composition containing fine carbon fiber opened and dispersed

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US5845144A	1998-12-01	Information processing apparatus with internal printer
US4497036A	1985-01-29	Portable computer
US7197588B2	2007-03-27	Removable personal digital assistant in a dual personal computer/personal digital assistant computer architecture
US4667299A	1987-05-19	Portable computer
US7426595B2	2008-09-16	Desktop holder and portable terminal system
US6389383B1	2002-05-21	Function extending apparatus, electronic apparatus and electronic system
EP0638912B1	2000-03-08	Recording and/or reproducing system and data backup system
EP0145206A2	1985-06-19	Intelligence display arrangement
EP0811186A1	1997-12-10	Modular pcmcia card
US20070120525A1	2007-05-31	Electronic device with auxiliary unit that is usable detached from main unit of electronic device
US6728811B1	2004-04-27	Portable information terminal

IPR2025-00645 Page 01729

JP2523960B2	1996-08-14	Document editing device
JP3631469B2	2005-03-23	Electronics
EP0517508A1	1992-12-09	Storage controller for a personal computer
CA2063558C	2000-08-15	Portable low power computer
JP2001101356A	2001-04-13	Memory card adapter with displaying function
JP2001028836A	2001-01-30	Card adaptor with built-in battery and charging device with adaptor function
JPH09128114A	1997-05-16	Computer system and card type interface device to be applied to the computer system
JPH08115399A	1996-05-07	Memory card
JP2916225B2	1999-07-05	Information output device
JPH11102233A	1999-04-13	Portable information card input device
JP3117405U	2006-01-05	Multimedia connection reader
JP2001506780A	2001-05-22	Apparatus and method for adapting computer peripherals
JP2000099206A	2000-04-07	External unit for computer
KR200241676Y1	2001-10-12	Card adapter, main station removably coupled with the card adapter, and universal card reader/writer

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2218924A	1990-08-22	1990-08-22	Document editing device

Applications Claiming Priority (1)

Application	Filing date	Title
JP2218924A	1990-08-22	Document editing device

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents KR20030072203

Interface between modem and subscriber interface module

Abstract

The circuitry for interfacing the modem of the wireless communication device with a subscriber interface module (SIM) 122 includes a modem controller 302, a universal asynchronous receiver / transmitter (UART) 312 connected to the modem controller, and a control signal provided to the programmable clock circuit. 352 and programmable clock circuits 314, 316 for generating a UART clock and a SIM clock independently of each other based on the common clock 350, a reset circuit 320 for generating a SIM reset signal, and powering on and off the SIM. And a power control circuit 308 for controlling, all of which reside on the integrated circuit chip 301. This circuit also includes a bus interface circuit 214 that interfaces the modem to the SIM using a common data line 212.

Classifications

- H04M1/725 Cordless telephones

View 1 more classifications

KR20030072203A

South Korea

Download PDF Find Prior Art Similar

Other languages: Korean

Inventor: 제임스 영이, 4세 어치슨, 스티븐 아이, 수탄카요

Worldwide applications

2001 ~~KR~~ CA US CN JP EP ES AU WO

Application KR10200027009959A events

2000-02-04 Priority to US18022800P

2000-02-04 Priority to US60/180,228

2001-02-02 Application filed by 퀄콤 인코포레이티드

2003-09-13 Publication of KR20030072203A

Info: Patent citations (10), Cited by (43), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (17)

Hide Dependent

1. A wireless communication device for a subscriber interface module (SIM) comprising an input / output (I / O) port 206 for transmitting and receiving serial data and a clock input 208 for receiving a subscriber interface module (SIM) clock. As circuit 130 for interfacing modem 120 of (WCD).

   Modem controller 302;

   A transmitter 334 for selectively transmitting data to the SIM I / O port via a common data line 212 and a receiver 336 for receiving data from the SIM I / O port, and connected to the modem controller. Universal asynchronous transceiver (UART) 312; And

   Programmable clock circuits 314, 316 that generate a SIM clock and a UART clock based on a common clock 350 and generate the SIM clock and UART clock independently of each other in response to clock control signals 352, 354 or 356 from the modem controller. Wherein the common clock (350) is provided to the programmable clock circuit (314, 316).

2. 2. The circuit of claim 1 wherein the modem controller, the UART and the programmable clock circuit are each configured on the same integrated circuit (IC) chip (301).

3. 2. The circuit of claim 1, wherein the programmable clock circuit selectively enables and disables the SIM clock independently of the UART clock in response to the SIM clock enable / disable control signal (356).

4. The circuit of claim 1, wherein the programmable clock circuit is:

   A first programmable divider (316) for generating a SIM clock based on the common clock and in accordance with a first frequency control signal (354) from the modem controller; And

   And a second programmable divider (314) for generating a UART clock based on the common clock and in accordance with a second frequency control signal (352) from the modem controller.

5. The method of claim 1,

   One of a UART transmitter and a SIM I / O port sends consecutive data bytes to the UART receiver via the common data line, the modem controller configures the UART to operate in byte mode,

   In the byte mode the UART receiver collects consecutive data bytes and the modem controller reads data bytes from the UART.

6. The method of claim 1,

   One of the UART transmitter and the SIM I / O port transmits consecutive data bits to the UART receiver over a common data line at a predetermined baud rate, and the modem controller configures the UART to operate in sample mode,

IPR2025-00645 Page 01731

in the sample mode, the UART receiver repeatedly samples the signal state of the common data line at a sample rate that is a predetermined multiple baud rate to collect sample data bytes, and the modem controller reads the sample data bytes and the UART Circuitry for detecting an error condition associated with the SIM based on the sample data bytes collected by the receiver.

7. 2. The SIM of claim 1, wherein the SIM comprises a reset input 210 for receiving a SIM reset signal, wherein the circuit also induces a SIM reset signal in response to a SIM reset control signal 360 from the modem controller. Circuitry further comprising a reset circuit (320) for selectively declaring and declaring.

8. The method of claim 1,

The SIM I / O port consists of an open-drain I / O port, the common data line is connected between the SIM I / O port and a UART receiver, and the circuit is connected to the input and the common connected to the UART transmitter. Further comprising a bus interface (I / F) circuit 214 having an output connected to the data line,

The bus I / F circuit is:

Provide a high impedance to the common data line when the UART transmitter applies a first logic level to an input of the bus I / F interface circuit,

The UART transmitter is connected to a second input of the bus I / F interface circuit

And provide low impedance to the common data line when applying a direct level.

9. The method of claim 8,

A power supply rail of the WCD used to power the bus I / F circuit and a power input of the bus I / F circuit and connected to the power input of the bus I / F circuit in response to a switch control signal. A power switch 244 for selectively connecting and disconnecting the power supply rail; And

Switch control in which the modem controller can selectively power bus I / F circuitry and remove power from bus I / F circuitry by inducing the switch control signal in response to control signal 332 from the modem controller. And further comprising a circuit (310).

10. The method of claim 9,

A power supply rail of the WCD used to power the SIM and a power input of the SIM and selectively connect and disconnect the WCD power supply rail to the power input of the SIM in response to a second switch control signal. Second power switch 232; And

A second switch control circuit that allows the modem controller to selectively power and remove power from the SIM by inducing the second switch control signal in response to a second control signal 330 from the modem controller (308, further comprising.

11. The method of claim 1,

A power switch connected between the power supply rail of the WCD used to power the SIM and the power input of the SIM and selectively connecting and disconnecting the WCD power supply rail to the power input of the SIM in response to a switch control signal (232); And

Further comprising a switch control circuitry 308 capable of selectively powering the SIM and removing power from the SIM by inducing a switch control signal in response to the control signal 330 from the modem controller. Characterized by a circuit.

12. 2. The modem of claim 1 further comprising an internal timer 318 for generating an interrupt 306 in the modem controller, wherein the generation is based on a clock 350 received by the internal timer and from the modem controller. And after a programmable delay time in accordance with the delay control signal (358).

13. An input / output (I / O) port 206 for transmitting and receiving serial data, a clock input 208 for receiving a subscriber interface module (SIM) clock, and a reset input 210 for receiving the SIM reset signal. As a circuit 130a on an integrated circuit (IC) chip 301 for interfacing a modem 120 of a wireless communication device (WCD) 104 to a subscriber interface module (SIM) comprising.

Modem controller 302;

A transmitter 334 for selectively transmitting data to the SIM I / O port via a common data line 212 and a receiver 336 for receiving data from the SIM I / O port, and connected to the modem controller. Universal asynchronous transceiver (UART) 312;

Programmable clock circuits 314 and 316 for generating a SIM clock and a UART clock based on a common clock 350 and for generating a SIM clock and a UART clock independently of each other in response to a clock control signal 352 from the modem controller. The common clock 350 is provided to the programmable clock circuit; And

A reset circuit (320) for selectively declaring and undeclaring a SIM reset signal in response to a SIM reset control signal (360) from the modem controller.

14. Modem 120 of wireless communication device (WCD) 104, which is a subscriber interface module (SIM) that includes an input / output (I / O) port 206 that transmits and receives serial data and has an open-drain configuration. As circuit 130 for interfacing with:

Modem controller 302;

A transmitter 334 for selectively transmitting data to the SIM I / O port via a common data line 212 and a receiver 336 for receiving data from the SIM I / O port, and connected to the modem controller. Universal asynchronous transceiver (UART) 312;

A bus interface (I / F) circuit 214 having an input connected to the UART transmitter and an output connected to the common data line and converting the UART transmitter into an open-drain configuration compatible with the SIM I / O port. ;

A power supply rail of the WCD and a power supply input of the bus I / F circuit and selectively connect and disconnect the power input of the bus I / F circuit and the WCD power supply rail in response to a switch control signal. Switch 244; And

A switch capable of selectively powering the bus I / F circuitry and removing power from the bus I / F circuitry by inducing a switch control signal in response to a control signal 332 from the modem controller A circuit comprising a control circuit 310.

15. The method of claim 14,

A power supply rail of the WCD used to power the SIM and a power input of the SIM and selectively connect and disconnect the WCD power supply rail to the power input of the SIM in response to a second switch control signal. Second switch 332; And

A second switch control circuit that allows the modem controller to selectively power and remove power from the SIM by inducing the second switch control signal in response to a second control signal 339 from the modem controller (308, further comprising.

16. A method of interfacing a modem 120 of a wireless communication device (WCD) 104 to a subscriber interface module (SIM), the modem comprising a modem controller 302 connected to a universal asynchronous transceiver (UART) 312. The UART includes a transmitter 334 for selectively transmitting continuous data to the SIM over a common data line 212 at one or more predetermined baud rates and a receiver 336 for receiving continuous data from the SIM, wherein the UART The receiver can be operated in either a byte mode in which the UART receiver collects consecutive data bytes transmitted at a predetermined baud rate or in a sample mode in which the UART receiver samples the state of a common data line at a sample rate exceeding a predetermined baud rate. In the method of construction,

(a) configuring the UART to operate in the sample mode (502);

(b) sending (504) a byte to the SIM over the common line using the UART transmitter;

(c) collecting sample bytes indicating whether an error associated with the SIM has occurred by repeatedly sampling the state of a common line during an error signal window occurring after the byte has been transmitted in step (b);

(d) determining (606) whether an error associated with the SIM has occurred based on the sample byte; And

(e) resending (614) the byte to the SIM when an error occurrence associated with the SIM is determined.

17. The method of claim 16,

(f) counting (620,622) the number of sample bytes to determine a time when a predetermined guard time has elapsed since the byte was transmitted in step (b); And

(g) repeating step (b) when the predetermined guard time has elapsed.

Description

Interface between modem and subscriber interface module (INTERFACE BETWEEN MODEM AND SUBSCRIBER INTERFACE MODULE)

The subscriber identification module (SIM) is, for example, a smart card used in connection with a wireless communication device (WCD) such as a cellular radiotelephone. Typical SIMs include small computer systems having a controller and a memory. The SIM memory contains information associated with the subscriber / user of the WCD, including, for example, a subscriber / user identifier, a phonebook identifying a stored telephone number bank, an encryption sequence for secure data communication over the air, and the like. Typically, the subscriber can install the SIM on the WCD or remove the SIM from the WCD. The SIM can be removed from the first WCD and installed on the second WCD, thereby enabling the user the ability to transfer male or female "identification" between WCDs.

Conventional SIMs provide a relatively simple electrical interface that includes a SIM I / O port for transmitting serial data to and receiving serial data from another device (WCD), a SIM clock input for receiving a clock, and a reset signal. It includes a reset input for receiving. However, functional interfacing with conventional SIMs (e.g., interaction with SIMs and accessing data from SIMs) can be complicated because the SIM has a processor, and several standards that require a relatively sophisticated way to communicate with a SIM (For example, the Global System for Mobile Communications (GSM) standard) can be complicated by the existence. Therefore, the functional interface with the SIM by the functional SIM interface is much more complicated than when reading data from memory, for example. Instead, the SIM and the requesting device (e.g., WCD) connected to the SIM actually exchange commands and responses in a back and forth manner. A more complex problem is that some SIMs are not compatible with commonly accepted SIM interface standards (eg GSM).

Accordingly, there is a need to provide an interface for electrically and functionally interfacing the WCD to the SIM, whereby the WCD can control and access the information contained in the SIM. There is also a need for a SIM that is compatible with commonly accepted SIM interface standards and an interface capable of interfacing SIMs and WCDs that are not compatible with these standards.

Moreover, there is a need to reduce power consumption, component count, size and cost of WCDs. Thus, it is desirable to reduce all these aspects of the WCD, including an interface for interfacing the WCD to the SIM.

The present invention relates to a wireless communication device, in particular a wireless communication device comprising a subscriber identity module.

1 is a block diagram of a typical WCD in which the present invention may be practiced.

2A is a block diagram external to the SIM interface of FIG. 1 in accordance with an embodiment of the present invention.

2B is a circuit diagram of the bus interface circuit of FIG. 2A in accordance with the present invention.

3 is a block diagram of the interior of the SIM interface of FIG. 1 in accordance with an embodiment of the present invention.

4 is a continuous timing diagram of (a) to (g) corresponding to the SIM interface signal or clock of FIG.

5 is a flow diagram of a method associated with transferring data bytes from a modem to the SIM of FIG. 1 in accordance with an embodiment of the present invention.

6 is a flowchart of a method corresponding to a receive interrupt service routine according to an embodiment of the present invention.

7 is a block diagram of an exemplary computer system in which some of the invention may be practiced.

summary

The present invention provides a method and circuit for interfacing a WCD's modem to a SIM. The SIM provides an input / output (I / O) port for transmitting and receiving continuous data, a clock input and a reset signal for receiving a SIM clock. It includes a reset input for receiving. In one embodiment, the present invention includes circuitry for interfacing a modem to a SIM. This circuit includes a modem controller and a universal asynchronous transceiver (UART) attached to the modem controller. The UART includes a transmitter and a receiver for transmitting data to and receiving data from the SIM I / O port through a common data line. The circuit also includes a

programmable clock circuit for generating a SIM clock and a UART clock based on a common clock provided to the programmable clock circuit. The programmable clock circuit generates the SIM clock and the UART clock independently of each other in response to a clock control signal from the modem controller.

According to the present invention, the modem controller, the UART and the programmable clock circuit can each be included in the same integrated circuit (IC) chip.

In accordance with another aspect of the present disclosure, the programmable clock circuitry can selectively enable and disable the SIM clock independently of the UART clock in response to the SIM clock enable / disable control signal.

According to another aspect of the invention, a modem controller places a UART to operate in byte mode, and the UART receiver collects consecutive data bytes from the UART transmitter or SIM I / O when transmitted at the programmable baud rate.

According to another aspect of the present invention, the modem controller configures the UART to operate in sample mode, and the UART receiver repeatedly samples the signal state of the common data line to collect the same data bytes at different programmable baud rates. The modem controller also reads the sample data bytes and detects an error condition associated with the SIM based on the sample data bytes collected by the UART receiver.

According to another aspect of the invention, the circuit extracts, optionally declares and undeclares a SIM reset signal in response to a SIM reset control signal from a modem controller.

The SIM I / O port consists of an open-drain I / O port and a common data line connected between the SIM I / O port and the UART receiver. According to another aspect of the invention, the circuit also includes a bus I / F circuit having an input connected to a UART transmitter and an output connected to a common data line. Bus I / F circuitry provides high impedance to common data lines when the transmitter applies a first logic level to the input of the open-drain interface circuit and is common when the transmitter applies a second logic level to the input of the open-drain interface circuit. Provide a low impedance to the signal on the data line.

According to another aspect of the invention, the circuit comprises a first power switch connected between the power supply rail of the WCD and the power input of the bus I / F circuit used to power the bus I / F circuit. The first power switch selectively connects and disconnects the WCD power supply rail to the power input of the bus I / F circuit in response to the first switch control signal. The circuit also includes a first switch control circuit that extracts a first switch control signal in response to the first control signal from the modem controller, whereby the modem controller selectively powers the SIM and removes power from the SIM. can do.

According to another aspect of the invention, the circuit comprises a second power switch connected between the power supply rail of the WCD used to power the SIM and the power input of the SIM. The second power switch selectively connects and disconnects the WCD power supply rail for the SIM power input in response to the second switch control signal. The circuit also extracts a second switch control signal in response to the second control signal from the modem controller, whereby the modem controller can power the SIM and selectively remove power from the SIM.

According to another aspect of the present invention, the circuit generates an interrupt for the modem controller after a programmable delay time based on a clock received by the interval timer and a delay control signal from the modem controller.

In another embodiment, the present invention includes a method of interfacing a modem to a SIM. The method configures the UART to operate in sample mode and includes sending bytes from the common line to the SIM using a UART transmitter. The method also includes repeatedly sampling the state of the common line during the error signal window generation after the byte has been transmitted, collecting sample bytes indicating whether an error associated with the SIM has occurred. The method also includes determining whether an error associated with the SIM has occurred based on the sample byte and resending the byte to the SIM when it is determined that an error associated with the SIM has occurred.

Characteristics and Benefits

The present invention provides an interface comprising a method and circuitry for electrically and functionally interfacing a WCD to a SIM, whereby the WCD can control and access information contained in the SIM. This interface is sufficiently flexible to allow SIM and WCD to interface with a SIM that is compatible with the commonly accepted SIM interface standard and with a SIM that is not compatible with the standard

The interface includes multiple interface circuits implemented on a single integrated circuit chip, which reduces the component count, size and power requirements of the WCD.

The interface reuses the circuitry and features of the modem of the WCD, including the modem controller, instead of adding a dedicated controller to implement and control the interface, thereby reducing the number of parts of the WCD and conserving the power of the WCD.

For example, the interface provides a data connection between the modem and the SIM via the modem UART. The interfaces extract and control the UART clock and SIM clock independently of each other. The interface also extracts and controls the SIM reset signal independently of the SIM and UART clocks. As a result, the interface has availability for initializing and / or resetting the logic of the SIM, detecting error conditions sent by the SIM, detecting when the SIM is installed in the WCD, removed from the WCD, and so forth.

The interface includes a bus interface circuit connected between the modem and the SIM, thereby allowing the modem and the SIM to share a common data line used to communicate data between the two devices. The interface may repeatedly sample the common data line in sample mode to detect an error condition associated with the SIM. Optionally, the interface may sample the common data line in byte mode, thus collecting data bytes or characters communicating on the common data line.

The interface can selectively power bus interface circuits and remove power from them, thus conserving power in the WCD and protecting the SIM and modem when the SIM is not in use.

The interface can optionally power and remove power from the SIM, thus conserving power in the WCD.

The invention is described in detail below with reference to the drawings.

Environment

1 is a block diagram of a WCD 104 that may be practiced with the present invention. WCD 104 includes cellular wireless telephones, satellite wireless telephones, PCMCIA cards integrated into a computer, and the like. WCD 104 includes a transmit / receive antenna 106 and a signal processing module 108 connected to antenna 106. WCD 104 may be connected to computer 110 by data link 112.

The signal processing module 108 installs (plugs in) and removes (unplugs) radio frequency (RF) reception (Rx) and transmission (Tx) sections 116, the modem 120, and the signal processing module 108 from it. A conventional SIM 122). Modem 120 includes a demodulator / decoder section and an encoder / modulator section both coupled to RF Rx / Tx section 116. Modem 120 also includes a modem controller for controlling the modem and SIM 122 as described below. Typical SIM 122 includes a small computer system having a controller and a memory. The SIM memory includes, for example, information associated with subscriber / user identifiers, phonebooks identifying stored phone number banks, messages, and encryption sequences for secure public data communication. The invention can be used with a SIM which is

compatible with the following standards: ISO / IEC 7816, TIA / EIA IS-820, GSM 11.11 and gsm 11.12. However, the present invention is not limited to the use of SIMs, and therefore SIMs which are not exactly compatible with the above standards may be used.

Signal processing module 108 includes a SIM interface (I / F) 130 (shown in FIG. 1) configured and operative in accordance with the principles of the present invention for interfacing modem 120 to SIM 122. do. SIM I / F 130 includes an internal SIM I / F 130a inside modem 120. SIM I / F 130 also includes an external SIM I / F 130b external to modem 120. Modem 120 may control and access information contained in SIM 122 via SIM I / F 130 in a manner described below.

A brief overview of the operation of the WCD 104 is provided. In the receiving direction, the antenna 106 of the WCD 104 receives the RF signal 140 transmitted from another wireless communication device (not shown), such as a base station, mobile station, or the like. RF signal 140 may be compatible with any number of communication protocols, including, for example, code division multiple access (CDMA) communication protocols. RF signal 140 may also carry information formatted according to a data protocol such as TCP / IP (Transaction Control Protocol / Internet Protocol).

Antenna 106 provides RF signal 140 to RF Rx / Tx section 116. The RF section 116 frequency downconverts the received RF signal and provides a frequency downconverted signal, such as an intermediate frequency (IF) or baseband signal, to the demodulator / decoder of the modem 102. The demodulator / decoder section demodulates and then decodes the down-converted signal to produce demodulated and decoded signals usable, for example, in WCD 104 or computer 110.

In the transmission direction, the modulator / encoder section of the modem 120 encodes and modulates the data to be transmitted wirelessly to the wireless device, and provides a baseband or IF signal encoded and modulated into the RF Rx / Tx section 116. The RF Rx / Tx section 116 frequency upconverts the baseband or IF signal to produce an RF transmission signal. The RF Rx / Tx section 116 provides the antenna 106 with an RF transmit signal to be transmitted wirelessly by the antenna.

External SIM I / F (130b)

2A is a block diagram of an external SIM I / F 130b in accordance with an embodiment of the present invention. In FIG. 2A, external SIM I / F 130b is shown associated with both modem 120 and conventional SIM 122. A typical SIM 122 is a SIM input / output (I / O) port 206, a SIM clock input 208 and a SIM reset input that send serial data bits to and receive serial data bits from the modem 120. And 210.

The SIM I / O port 206 is connected to a receive port ("RX") of the modem 120 via a common data line 212 connected between the SIM I / O port and the modem RX port. Can be sent). Modem 120 includes a transmission port (denoted as "TX") that transmits a data signal comprising consecutive data bits to SIM I / O port 206. The modem TX port sends a data signal to the I / O port 206 through a bus I / F circuit 214 having an input connected to the modem TX port and an output connected to the common data line 212. The modem TX port first sends a data signal to the bus I / F circuit input and in response the bus I / F circuit output sends a data signal to the SIM I / O 206 via the common data line 212. Therefore, modem 120 transmits continuous data to and receives continuous data from SIM I / O port 206 via common data line 212. In the present invention, modem 120 and SIM I / O port 206 may safely share common data line 212 due to bus I / F circuitry 214 as described below.

Modem 120 extracts the SIM clock ("SIM_CLK") from the modem output labeled "CLK" in FIG. 2A and transmits the SIM clock to SIM input 208 via clock line 220. The SIM clock drives logic in the SIM 122. The modem 120 may selectively enable and disable the SIM clock to control the SIM 122.

Modem 120 extracts the SIM reset signal ("SIM_RST") from the modem output labeled "RST" in FIG. 2A and transmits the SIM reset signal to SIM reset input 210 via reset line 222. The SIM reset signal can be used to reset the SIM 122. Modem 120 may optionally declare and undeclare SIM reset signals to control SIM 122.

The first power supply rail 230 (indicated by "SIM VDD") that is external to the modem 120 supplies power to the power supply input of the SIM 122 via the SIM power switch 232. The power switch 232 may selectively power and remove power from the SIM 122 in response to the SIM power control signal provided to the switch 232 via the line 234. Modem 120 extracts the SIM power control signal from the first power enable output (denoted as "PWR EN1") of modem 12, thereby allowing the modem to conserve power when SIM 122 is not used. The SIM 122 can be selectively powered on and powered off. A typical switching circuit for the power switch 232 includes a FET transistor having a source-drain path connected between the power supply rail 230 and the power supply input of the SIM 122 and a gate electrode connected to the line 234. do.

The second external power supply rail 240 (denoted "Bus VDD") supplies power to the power supply input of the bus I / F circuit 124 via the bus power switch 244. The power supply rails 230 and 240 may be the same or different power supply rails. The power switch 244 may power the bus I / F circuit 214 or remove power from the bus power control signal provided to the switch 244 via the line 248. Modem 120 extracts the bus power control signal from the second power enable output (denoted as "PWR EN2") of modem 120, whereby the modem protects the SIM and modem circuit of the present invention and conserves power. The bus I / F circuitry 214 may optionally be powered on and off. The power switch 244 may include a switch circuit similar to the switch 234 circuit as described above.

As mentioned above, the external SIM I / F 130b is a power switch (e.g., required to carry the above-described interface signals (e.g., SIM_CLK, SIM_RST, data signals and power control signals) between the modem 120 and the SIM 122). 232, 244, bus I / F circuitry 214, and multiple signal lines 234, 248, 212, 220, 222, and the like.

Bus I / F Circuit

As mentioned above, the modem 120 and the SIM 122 share a common line 212. SIM I / O port 206 is configured as an open-drain output. Open-drain outputs are known. Therefore, common line 212 attached to SIM I / O port 206 is referred to as an open-drain bus. Bus I / F circuitry 214 connects to common line 212 (open-drain bus) at the desired voltage level without damaging one of the modems 120 or one of the SIMs 122 sharing a common line. Provide an inducible mechanism.

In the present invention, the modem transmit and receive ports TX and RX each have a dedicated function. Modem transmit port TX includes drive circuitry that actively leads the attached line to either a high or low voltage level (corresponding to a logic high "1" or logic low "0" binary value). The modem receive port RX can sense (sample) the voltage level on the common line 212 and interpret this level as either a logic high "1" or a logic low "0" binary value. In general, an RX port cannot sense the level (state) of a TX port unless a physical connection exists between the RX and TX ports.

Because the TX port drive circuitry actively induces the attached line, other devices attached and inducing the same line in a manner competing with the TX port cause damage to the TX port drive circuitry and / or cause unnecessary current draw. For example, connecting the SIM I / O port 206 directly to the modem TX port may cause the modem when the SIM I / O port 206 is driven to a low logic level, such as providing a low resistance path to ground. The TX port results in a state that is driven to a high logic level. Since the potential difference is between ground through the low resistance path, the SIM I / O port 206 can reduce the high current from the modem TX port under the conditions described above. As a result, either the modem 106 or the SIM 122 can be damaged.

In order to securely interface both the modem TX and RX ports to the SIM I / O port 206, the bus I / F 214 is configured in an open-drain bus configuration that is compatible with the SIM I / O port 206. Adapt. Bus I / F 204 operates as follows:

1) When the modem TX port is driving logic high at the input to bus I / F circuitry 214, the output of bus I / F circuitry provides a high impedance to common line 212, and thus to a common line. The connected external device may "pull up" the voltage on the common line 212 to a logic high level or "pull down" to a logic low level; and

2) When the modem TX port is driving logic low at the input to bus I / F circuitry 214, the output of bus I / F circuitry 214 is dependent on the signal on common line 212 (e.g., SIM I). / O port 206) to provide a low impedance path, so that the voltage on common line 212 is driven to a logic low level.

2B is a circuit diagram of the bus I / F circuit 260 corresponding to the bus I / F circuit 214. in FIG. 2B, reference level "RX" (eg, "R4") represents a resistance and reference level "QX" (eg "Q1") represents a transistor. The bus I / F circuit 260 includes a first NPN transistor 262 (Q2) and a second NPN transistor 264 (Q4) connected in series thereto. Each transistor 262, 264 is configured as an open collector inverter. As described above, the output terminal 266 (connected to the common line 212) of the bus I / F circuit 260 is connected to the input terminal 270 (connected to the modem TX port) of the bus I / F circuit. Provides either high impedance or low impedance paths for signals on common lines.

For simplicity, two inverter stages corresponding to transistors 262 and 264 are shown in FIG. 2A. But the inverter stage need not be ideal. For example, the first inverter stage may be a logic inverter that is performed in any type of logic such as, for example, TTL or CMOS. In addition, the second inverter stage may be an N-channel enhanced MOSFET. in addition, the use of two inverter stages is not necessary. Any circuit that meets the input / output requirements described above may be used.

Internal circuit

3 is a block diagram of an internal SIM IF 130a (in contact with SIM I / F 130b) in accordance with an embodiment of the present invention. In a preferred embodiment, the plurality of circuits associated with the internal SIM IF 130a are configured on a single integrated circuit chip 301 inside the modem 120 (as described above), thus reducing the number of parts of the WCD 104 and Reduced in size

Modem controller

Internal SIM I / F 130a includes a modem controller 302 (central processing unit (CPU)) coupled to data bus 304. Data bus 304 is associated with an address bus and data read and write signals (not shown) as is known to those skilled in the art. Modem controller 302 is preferably a 32-bit controller (32-bit reduction command set controller), and data bus 3040 is preferably a 32-bit bus.

Modem controller 302 may write data and / or commands (control signals) to other circuit elements (described below) coupled to data bus 304. The modem controller 302 may read data from other circuit elements at appropriate times. The modem controller 302 accesses (eg, writes and / or reads) various other devices connected to the data bus 304 using memory mapped access techniques, I / O port access techniques or other access techniques known to those skilled in the art.)can do.

Modem controller 302 may receive one or more interrupt signals 306 as described below, each associated with a different interrupt state from various circuit elements connected to data bus 304. The specific mechanism associated with interrupt reception is known.

The modem controller 302 controls the circuitry and functions of the modem 104, but the modem 104 such as demodulation / decoding, encoding / modulation, and data transmission within the modem 104 and between an external device such as the computer 110 and the modem.) Is not directly related to interfacing to SIM 122. The present invention reuses the modem controller 302 as a SIM interface controller. This can simply prevent adding another controller to control the SIM interface, thereby reducing the power consumption, cost and component count of the WCD 104 while maintaining a flexible and powerful SIM interface.

Internal SIM I / F 130a may also include SIM power control circuit 308, bus power control circuit 310, UART 312, UART clock circuit 314, SIM clock circuit 316, internal timer 318. And a SIM reset circuit 320, each of which is connected to a data bus 304.

Power control

The SIM power control circuit 308 derives the SIM power control signal (FIG. 2A) in response to the SIM power control signal 330 (command 330) received from the modem controller 302, and thus the modem controller 302 May power-on and power-off the SIM 122.

Similarly, bus power control circuit 310 derives a bus power control signal (FIG. 2A) in response to bus power control signal 332 received from modem controller 302, thereby allowing modem controller 302 to provide a bus. I / F circuitry 214 may be powered on and powered off. The control circuits 308, 310 may be latched to the latch data value "0" or "1" provided to the data bus 304.

in alternative embodiments, one or both of power switches 232 and 244 and corresponding control circuits 308 and 310 are removed. For example, in alternative embodiments, the switch 232 and power rail 230 shown in FIG. 2A may be omitted. In this embodiment, the switch 244 selectively supplies power to the bus I / F circuit 214 and the SIM 122. By omitting the switch 232, this embodiment advantageously reduces the number of parts of the WCD 104.

One or more bus I / F circuits 214 and switches 244 and 232 may also be configured on the integrated circuit 301, thus forming part of the internal I / F 130a instead of the external circuit 130b.

Universal Asynchronous Transceiver (UART)

UART 312 includes a UART transmitter 334 (corresponding to TX portion of modem 120) and UART receiver 336 (corresponding to RX portion of modem 120). The modem controller 302 sends a UART control signal 338 to the UART 312 to configure and control the UART receiver and transmitters 334 and 336. For example, the modem controller 302 configures the baud rate, the number of bits (or bytes) of the character frame, the number of stop bits, and the parity (even or odd) used by the UART 312. UART 312 provides one or more interrupt signals 306 to modem controller 302 depending on the state of UART transmitter 334 and / or receiver 336.

In the transmission direction for the modem 120, the modem controller 302 may write one or more data bytes 340 to the UART transmitter 334 to be sent to the SIM I / O 206. In response, the UART transmitter 334 transmits data bytes in the form of consecutive data bits to the SIM I / O 206 via the bus I / F circuitry 214 as described above.

In the receiving direction, the UART receiver 336 can repeatedly sample the signal state (ie, logic level) of the common line 212 to collect sample bytes according to the signal state of the common line. The modem controller 302 may then read the sample byte collected by the UART receiver 336 (indicated by sample byte 3442 in FIG. 3) from the UART receiver. The UART 312 provides an interrupt signal 306 to the modem controller 302, which receives data bytes sent by the SIM I / O port 206 or the UART transmitter 334 in the manner described below. Received (and the corresponding sample byte collected).

UART 312 receives UART clock 344 extracted or generated by UART clock circuit 314. UART 312 may transmit and receive continuous data at different baud rates determined by UART clock 344 and in accordance with the baud rate control signal 338 received from modem controller 302.

UART receiver 336 may operate in one of two modes, including byte mode and sample mode, in accordance with mode control command 338 received from modem controller 302. When commanded in byte mode, the UART receiver 336 receives and collects consecutive data bytes sent by the SIM I / O port 206. In order to do this, the UART receiver 336 is configured at a sample rate that matches the baud rate at which the SIM I / O port 206 (or UART transmitter 334) transmits consecutive data bits on the common data line 212. Sample received consecutive data bits. Typically, the UART samples each received consecutive data bit only once or twice in byte mode.

However, when commanded in sample mode, the UART receiver 336 repeatedly samples the common data line 212 at a sample rate that is several times greater than the baud rate when the SIM I / O port 206 transmits consecutive data bits. . For example, the UART receiver 336 can sample the common line 212 at 16X current baud rate,

such that the UART receiver can determine a single consecutive bit time (SIM I / O port 206 or UART transmitter 334). The common line is sampled 16 times during the consecutive bits transmitted by. In this example, UART receiver 336 collects 16 sample bytes for each successive bit sent by SIM I / O port 206

The UART receiver 336 can sample the common line 212 in either sample or byte mode while the SIM I / O port 206 or the UART transmitter 334 is sending data to the common line 212. Thus, the UART receiver 336 can operate in a wrap-around manner, whereby the receiver can sample and collect data transmitted by the UART transmitter 334. In addition, the UART receiver 336 can sample the common line 212 when neither the SIM I / O port 206 nor the UART transmitter 334 are transmitting data on the common line 212.

Clock and timing

Internal SIM I / F 130a receives common clock 350 from an external clock source 352, such as a crystal oscillator. Typical frequency of common clock 350 includes 19.2, 19.68, 19.8 MHz. Programmable UART clock circuit 314, programmable SIM clock circuit 316 and programmable internal timer 318 each receive a common clock 350 at a separate input.

UART clock circuit 314 extracts UART clock 344 based on common clock 350 and in accordance with UART clock control signal 352 received from modem controller 302. UART clock circuit 314 may be a programmable divider that divides the frequency of common clock 350 by the N value in accordance with UART clock control signal 352, thereby generating UART clock 344 at the controlled frequency.

Similarly, the SIM clock circuit 316 extracts the SIM clock signal based on the common clock 350 and in accordance with the first SIM clock (frequency) control signal 354 received from the modem controller 302. The SIM clock circuit 316 may be a programmable divider that divides the frequency of the common clock 350 by the M value in accordance with the SIM clock control signal 354, thereby generating a SIM clock at the controlled frequency. The SIM clock frequency 314 can also selectively enable and disable the SIM clock in response to a second SIM clock control (enable / disable) signal 356 received from the modem controller 302. SIM clock circuit 316 applies a static logic low ("0") or logic high ("1") to reset line 220 in response to a SIM clock disable signal received from modem controller 302. .

Internal timer 318 derives a programmable delay time based on common clock 350 and in accordance with timer control signal 358 received from modem controller 302. Internal timer 3180 may include a counter and / or a programmable divider to count clock cycles of common clock 350. In operation, the modem controller 302 programs the internal timer 318 according to the delay time. After the delay has elapsed, the internal timer 318 provides a timeout interrupt 306 to the modem controller 302, whereby the modem controller 302 tracks the timing associated with controlling the SIM 122. Can be maintained.

reset

The SIM reset control circuit 320 induces a SIM reset signal in response to the SIM reset control signal 360 received from the modem controller 302, whereby the modem controller 302 can reset the SIM 122. . The SIM reset control signal 320 can be latched to latch the provided data value "0" or "1".

Signal and Clock Timing Diagrams

4 is a continuous timing diagram (a) through (g) of a signal associated with the interface circuit of the present invention. Timing diagram (a) shows consecutive data bytes 402 applied to common data line 212 by either SIM I / O port 206 or modem transmitter 334. The contiguous data byte 402 contains a chronological sequence of contiguous logic bits (associated with logic "1" or logic "0" values or states, respectively). The contiguous data byte 402 comprises a start bit " ST " (logic " 0 "), eight data bits D0 to D7, parity bit " P " and one or more stop bits " SP " (logic " 1 "). include. The format of the contiguous data bytes 402 shown in the timing diagram (a) is merely an example. For example, other formats are possible, including different numbers of stop bits.

When the SIM 122 transmits or receives a sequence of data bytes (eg, data byte 402) to or from the modem 12, the SIM refers to the SIM error window 4040 following the stop bit of the sequence of data bytes. Error state for a time 404. The SIM 122 can generate an error state by pulsing-low the logic state of the common line 212 to a logic " 0 " to generate a narrow SIM error pulse 406. Each SIM error pulse 406 associated with the error window 404 is substantially shorter than each data bit D0-D8.

Timing diagram (b) is a timeline 408 showing when the UART receiver 336 samples the common data line 212 while in sample mode. Each sample strobe 410, 412 represents a sampling occurrence resulting in sample bytes collected by the UART receiver 336. While in sample mode, the UART receiver 334 may detect the occurrence of a narrow SIM error pulse 406 due to the relatively high sample rate associated with the sample strobe 412. In this manner, the modem controller 302 may detect one or more bit errors, parity errors, and fault status of the SIM 122.

Timing diagram c is a UART interrupt timeline 416 that corresponds to when the UART transmitter 334 transmits consecutive data bytes 402. After sending the data byte 402, the UART transmitter 334 declares an interrupt 418 (corresponding to the interrupt signal 306) to the modem controller 302.

Timing diagram d is a timeline showing consecutive consecutive data bytes 422a and 422b transmitted by UART transmitter 334 (or SIM I / O port 206). The modem controller 302 gives a predetermined guard time between the data bytes 422a and 422b. According to the GSM 11.11 standard, the guard time 424 may be greater than the maximum number of predetermined stop bits associated with each data byte 422a, 422b. Therefore, the guard time can be given by the modem controller 302 using the internal timer 318.

The timing diagram e is an example of the UART clock 344.

The timing diagram f is an example of the SIM clock SIM_CLK shown in relation to the UART clock 344. The modem controller 302 may control the SIM clock independently and asynchronously with the UART clock 344. For example, as shown in waveform diagram f, SIM_CLK is the initial full clock cycle 430, the initial portion of the second clock cycle 432, the intermediate corresponding to when SIM_CLK is disabled by the modem controller 302. The logic low portion 434 and the modem controller 302 include subsequent clock cycles 436 that correspond when the SIM_CLK is enabled again.

Since the SIM clock can be disabled while the UART is operating along the sample common line 212, the modem controller 302 can detect an inappropriate bus condition of the common line 212. This inadequate state includes a common line 212 that "sticks" high or low because the SIM 122 has been improperly operated, removed from the WCD 104 or recently installed.

The timing diagram g is an example of the SIM reset signal SIM_RST. In a typical SIM reset / initialization sequence following GSM 11.11, the modem controller 302 disables SIM_CLK, transitions the SIM_RST from logic high to logic low, and back to logic high and then enables SIM_CLK. The modem controller 302 uses an internal timer 320 to timing the asynchronous sequencing of the clock and signal described above.

Way

Byte transfer

5 is a flowchart of a control method 500 (indicated as "byte transfer" in FIG. 5) associated with transferring (ie, transmitting) data bytes from modem 102 to SIM I / O port 206 in accordance with the present invention. to be. In a first step 502, the modem controller 302 commands the UART receiver 336 in sample mode.

IPR2025-00645 Page 01737

in a next step 504, the modem controller 302 sends a data byte to the UART transmitter 334 and instructs the UART to send the data byte. In response, the UART transmitter 334 sends the data byte as a data byte contiguous to the SIM I / O port 206 over the common line 212 while the UART transmitter 336 repeatedly samples the common line 212. Send it.

After the UART transmitter 334 transmits the data byte, and after the UART receiver 336 receives the sample byte in the wrap-around manner described above, the UART receiver receives a signal indicating receipt of the data byte to the modem controller 302. Provide an interrupt 306. The interrupt is associated with a received interrupt status or value such as interrupt status = "Tx byte" ("transmit byte") or interrupt status = "process guard time". In this case, the reception interrupt state = " Tx bytes " because the UART transmitter 334 knows that it has sent a data byte.

The receive interrupt initiates next step 506. In step 506, the modem controller 302 uses an interrupt service routine (abbreviated as "Rx ISR") to service the receive interrupt. The Rx ISR activates certain processing or method steps depending on the state associated with the receive interrupt. In this case, the Rx ISR activates the method steps according to the Rx ISR state = " Tx bytes " The detailed method corresponding to Rx ISR is described below.

In a next step 508, the modem controller 302 waits for another sample byte from the UART receiver 334.

Interrupt service routines

6 is a flowchart of a method 600 corresponding to the Rx ISR described above. Method 600 may be represented in FIG. 6 as "Rx ISR" and may be performed at modem controller 302. Method 600 (ie, Rx ISR) is initiated by a receive interrupt from UART 312.

In an initial decision step 602, the following is determined.

Rx ISR status = "Tx Bytes" (described above in accordance with Method 500), or

Rx ISR Status = "Processing Guard Time"

When Rx ISR status = " Tx bytes " (at step 506 described above), flow control proceeds to next step 604. In step 604, while the data byte is being transmitted (e.g., during step 504 described above), all sample bytes collected by the UART receiver 334 are skipped, such that the SIM error signal window (e.g., the timing diagram of FIG. Only the sample bytes collected during the error signal window 404 described in connection with a) remain.

In a next decision step 606, sample bytes collected during the error signal window are checked to determine if an error signal is indicated. If no error signal is indicated in step 606, flow control proceeds to next step 608. In step 608, a status signal is set to indicate that the data byte (as described in steps 504 and 604) was transmitted successfully.

In a next step 610, the Rx ISR state is set to " process guard time. &Quot;

In a next step 612, the process waits for another sample byte.

Method steps 604-614 are run in step 506 described in connection with method 500.

On the other hand, when an error signal is indicated in step 606, the flow proceeds to the next step 614. In step 614, the status signal is set to " retransmission ", thereby indicating that the data byte needs to be retransmitted. The flow then proceeds to step 616.

Returning to the initial decision step 602, when the Rx ISR state = " process guard time ", the flow proceeds to the next step 620. In step 620, the number of received (collected) sample bytes is counted.

In a next decision step 622, it is determined whether the number of received sample bytes is equal to or greater than the number of samples corresponding to the guard time. If an insufficient number of sample bytes have been collected, the flow proceeds to the next step 624, where more sample bytes are received.

When a sufficient number of bytes have been collected, the flow proceeds to the next step 626. In step 626, the UART 312 is reset and the UART receiver 336 is released from the sample mode.

In a next decision step 628, the status signal is checked to determine if the status signal = "retransmission byte". If the status signal is not equal to the "retransmission byte", flow proceeds to next step 630. At step 630, the next data byte may be sent using method 500, for example.

On the other hand, when the status signal = "retransmission byte", the flow proceeds to the next step 632. In step 632, the last data byte transmitted is retransmitted using method 500, for example.

Computer systems

The method of the present invention is performed using a controller (eg, modem controller 302) operating in a computer based system environment. Although communication hardware may be used to carry out the invention, a general purpose computer system may be used. The invention may preferably be carried out in combination with software performed by the modem controller 302 and interface circuitry. As a result, the present invention can be implemented with a computer system or other processing system.

An example of computer system 700 is shown in FIG. 7. In the present invention, the methods and processes described above, such as methods 500 and 600, are performed on computer system 700. Computer system 700 includes one or more processors, such as processor 704 (eg, corresponding to modem controller 302). The processor 704 is connected to the communication infrastructure 706 (eg, a bus or network that may include the data bus 304 described with reference to FIG. 3). Various software implementations are described in terms of typical computer systems. After reading this description, those skilled in the art will understand how to perform the invention using other computers and / or computer architectures.

Computer system 700 also includes main memory 708, preferably random access memory (RAM), and may also include second memory 710. The second memory 710 may include, for example, a removable storage device 714 representing a hard disk drive 712 and / or a floppy disk drive, a magnetic tape drive and an optical disk drive. Removable storage device 714 reads from and / or writes to removable unit 718 in a known manner. Removable storage unit 718 represents a floppy disk, magnetic tape, optical disk, and the like, which are read and written by removable storage device 714. Removable storage unit 718 includes a computer usable storage medium having stored thereon computer software and / or data.

Alternatively, the second memory 710 may include similar other means for causing a computer program or other instructions to be loaded into the computer system 700. Such means may include, for example, removable storage unit 722 and interface 720. The means transmits a program cartridge and cartridge interface (used in a video game device), a removable memory chip (EPROM or PROM) and a corresponding socket and data and software from the removable storage unit 722 to the computer system 700. Other interfaces 72 and removable storage units 722 may be included.

IPR2025-00645 Page 01738

Computer system 700 may also include a communication interface 724. Communication interface 724 allows software and hardware to be transferred between computer system 700 and external devices. The communication interface 724 may include a modem, a network interface (such as an Ethernet card), a communication port, a PCMCIA slot, a card, and the like. Data and software transmitted over communication interface 724 are in the form of signals 728, which may be electrical, electromagnetic, optical, or other signals that may be received by communication interface 724. This signal 728 is provided to the communication interface 724 via the communication path 726. The communication path 726 carries a signal 728 and can be performed using wire or cable, fiber optics, telephone lines, cellular telephone links, RF links, and other communication channels.

As used herein, the terms "computer program medium" and "computer usable medium" may be a hard disk and signal 728 installed in removable storage drive 714, hard disk drive 712, and signal 728. Such computer program products are means for providing software to computer system 700.

Computer programs (computer control logic) are stored in main memory 708 and / or second memory 710. The computer program may be received via the communication interface 724. When such a computer program is performed, the computer program enables the computer system 700 to carry out the present invention. In particular, when the computer program is executed, the computer program allows the processor 704 to perform the processes of the present invention. Thus, such a computer program represents a controller of the computer system 700. By way of example, in a preferred embodiment of the present invention, the processing performed by the modem controller 302 may be performed by computer control logic. Where the present invention is performed using software, the software may be stored in a computer program product and computer system 700 using removable storage drive 714, hard drive 712, or communication interface 724. Can be loaded into.

conclusion

While various embodiments of the present invention have been described, it is not limited to the described description. Therefore, the scope of the present invention should not be limited to the above-described exemplary embodiments, but only by the following claims.

The present invention has been described in terms of functional blocks, which illustrate performing certain functions and relationships. The boundaries of these functional blocks have been defined for convenience of description. Other boundaries may be defined if certain functions and relationships are performed properly. Therefore, any other boundary is within the scope of the present invention. Those skilled in the art will appreciate that such functional blocks may be performed by discrete components, application specific integrated circuits, processors that perform appropriate software, and combinations thereof. Therefore, the scope of the present invention is not limited to the above-described typical implementation, but only by the following claims

Patent Citations (10)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
FI894320 *	1991-06-26	1993-09-27	Nokia Mobile Phones Ltd	GENERING AV EN KLOCKFREKVENS I ETT SMART CARD GRAENSSNITT
FR2683342B1	1991-10-31	1994-01-07	Gemplus Card International	INTERFACE CIRCUIT FOR INTEGRATED CIRCUIT BOARD.
US5920850A *	1994-11-04	1999-07-06	Pitney Bowes Inc.	Metering system with automatic resettable time lockout
FR2739242B1 *	1995-09-25	1997-10-24	Gemplus Card Int	MODEM EQUIPPED WITH A CHIP CARD READER
FR2755566B1 *	1996-11-04	1998-12-11	Alsthom Cge Alcatel	RADIO MODEM EQUIPPED WITH A MEMORY CARD READER
FR2767011B1 *	1997-08-04	1999-09-24	Alsthom Cge Alcatel	METHOD FOR ADAPTING THE FUNCTIONING OF A SUBSCRIBER IDENTIFICATION MODULE TO AN INTERFACE (S) OF A MOBILE RADIO COMMUNICATION TERMINAL, CORRESPONDING SUBSCRIBER IDENTIFICATION MODULE AND MOBILE TERMINAL
FR2772535B1 *	1997-12-11	2000-12-15	Micropross	COMMUNICATION INTERFACE WITH A SYNCHRONOUS CHIP CARD AND DEVICE PROVIDED WITH SUCH AN INTERFACE
GB2335568B *	1998-03-18	2003-04-09	Nec Technologies	Network operator controlled locking and unlocking mechanism for mobile phones
JPH11340868A *	1998-05-29	1999-12-10	Kyocera Corp	Portable telephone set
JP2002532921A *	1998-12-08	2002-10-02	アライドシグナルインコーポレイテッド	Simplified provisioning process and multiple subscriber interface for installation of multiple cellular and / or mobile communications satellite services

* Cited by examiner, † Cited by third party

Cited By (43)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				

IPR2025-00645 Page 01739

FR2800228B1 *	1999-10-26	2002-02-08	Wavecom Sa	SYSTEM AND METHOD FOR CONTROLLING THIRD PARTY EQUIPMENT THROUGH A SIM CARD THROUGH A RADIO COMMUNICATION MODULE, CORRESPONDING RADIO COMMUNICATION MODULE AND THIRD PARTY EQUIPMENT
EP1304607A1 *	2000-05-26	2003-04-23	Cegetel Groupe	Method for interactive exchange between a subscriber identification module co-operating with a terminal in a radiotelephone, and a local device
US7822878B2 *	2000-02-17	2010-10-26	Siemens Industry, Inc.	Device, system, and method for the automatic configuration of a network communications device
JP2002359660A *	2001-03-28	2002-12-13	Sony Computer Entertainment Inc	Data communication apparatus and method, data communication system, recording medium for recording data communication program recorded thereon, and the data communication program
US6895518B2 *	2001-05-31	2005-05-17	Koninklijke Philips Electronics N.V.	Power and frequency adjustable UART device
US20030037191A1 *	2001-08-13	2003-02-20	Robert Baranowski	Wireless module
US6909659B2 *	2001-08-30	2005-06-21	Micron Technology, Inc.	Zero power chip standby mode
US7898894B2 *	2002-02-25	2011-03-01	Hewlett-Packard Development Company, L.P.	Power saving in multi-processor device
US6898349B2 *	2002-05-17	2005-10-25	Abocom Systems, Inc.	Wireless computer peripheral interface with the capability of identification
US7395447B2 *	2002-09-16	2008-07-01	Silicon Labs Cp, Inc.	Precision oscillator for an asynchronous transmission system
US6917658B2 *	2002-09-16	2005-07-12	Silicon Labs Cp, Inc	Clock recovery method for bursty communications
WO2004036492A2 *	2002-10-16	2004-04-29	Sci-Tel Ltd.	Smart card network interface device
CA2427389A1 *	2002-12-24	2004-06-24	Research In Motion Limited	Methods and apparatus for controlling power to electrical circuitry of a wireless communication device having a subscriber identity module (sim) interface
US7313177B2 *	2003-05-10	2007-12-25	Hewlett-Packard Development Company, L.P.	Reset scheme for I/O pads in a source synchronous system
DE50306423D1 *	2003-09-09	2007-03-15	Siemens Ag	CIRCUIT ARRANGEMENT AS AN INTERFACE BETWEEN SIM CARD AND GSM MODEM
US20060293082A1 *	2003-09-10	2006-12-28	Neuhaus Hans J	Extension of the sim card in gsm devices
US7610061B2 *	2003-09-20	2009-10-27	Samsung Electronics Co., Ltd.	Communication device and method having a common platform
DE10357824A1 *	2003-12-09	2005-07-14	Kuka Roboter Gmbh	Method and device for operating cooperating different devices
KR20050098142A *	2004-04-06	2005-10-11	삼성전자주식회사	Electronic device for communicating with host through serial communication interface
TWM266644U *	2004-10-22	2005-06-01	Uniwill Comp Corp	Wireless conversion device
US7707441B2 *	2004-10-22	2010-04-27	Broadcom Corporation	Method and system for reducing power consumption of handsets through UART auto flow control
US20060104227A1 *	2004-11-15	2006-05-18	Chia-En Chuang	Data communication methods and systems
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US8913634B2 *	2005-04-01	2014-12-16	Freescale Semiconductor, Inc.	Method and apparatus facilitating multi mode interfaces
CN101263704A *	2005-09-08	2008-09-10	日本电气株式会社	Mobile communication terminal and mobile communication method
US7288962B2 *	2006-02-08	2007-10-30	Kyocera Wireless Corp.	Level shifting multiplexing circuit for connecting a two conductor full duplex bus to a bidirectional single conductor bus
TWI324865B *	2006-03-31	2010-05-11	Hon Hai Prec	Power management system and method for network device

IPR2025-00645 Page 01740

			Ind Co Ltd	
US7711373B2 *	2006-05-11	2010-05-04	Nokia Corporation	Multiradio control interface
US20080035729A1 *	2006-08-09	2008-02-14	Wei-Jung Lin	Multiple Card Reading Modules Apparatus
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
EP2114027A1 *	2008-04-30	2009-11-04	Gemplus	Method of detecting TV off event on a mobile terminal
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US8489837B1 *	2009-06-12	2013-07-16	Netlist, Inc.	Systems and methods for handshaking with a memory module
TWI449356B *	2010-02-05	2014-08-11	Htc Corp	Detachable wireless communication module and method for using the same
CN101859395A *	2010-05-14	2010-10-13	中兴通讯股份有限公司	Information transmission realization method and system, main control equipment and intelligent card
US8817856B2 *	2010-05-27	2014-08-26	Lg Electronics Inc.	Method and apparatus for controlling suspend mode in dual modem device
KR101679430B1 *	2010-09-30	2016-11-25	삼성전자주식회사	Method and apparatus for detecting of sim card inserting in a portable terminal
US8615227B2 *	2011-12-12	2013-12-24	Broadcom Corporation	Enhanced discontinuous mode operation with shared radio frequency resources
CN103581157A *	2012-08-10	2014-02-12	中兴通讯股份有限公司	Embedded device and control method for carrying out data communication based on same
US8745301B2 *	2012-10-29	2014-06-03	Qualcomm Incorporated	High voltage dedicated charging port
US8760123B2	2012-10-29	2014-06-24	Qualcomm Incorporated	High voltage dedicated charging port
WO2017049317A1 *	2015-09-18	2017-03-23	Able Device, Inc.	Secure data link for subscriber identification module (sim)-based processor
CN107613098B *	2017-08-24	2020-09-04	Oppo广东移动通信有限公司	Mobile terminal, download mode switching circuit thereof and download mode switching method thereof

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
KR20030072203A	2003-09-13	Interface between modem and subscriber interface module
US7975921B2	2011-07-12	NFC reader having a passive operating mode with low electrical consumption
JP2004348235A	2004-12-09	Portable electronic device and portable terminal device
JP4544263B2	2010-09-15	Communication system and memory card
WO2005043275A2	2005-05-12	Fpga boot-up over a network
US6728795B1	2004-04-27	DMA channel for high-speed asynchronous data transfer
KR100450765B1	2004-10-02	Wireless communication medium and method for operation thereof
WO2014153935A1	2014-10-02	Storage card and method for storing data
CN100356359C	2007-12-19	Connector between processor and user recognition card
JP5007382B2	2012-08-22	Communication device having SIM interface compatible with wireless separation
US6209058B1	2001-03-27	Expansion card
US9792467B2	2017-10-17	Wireless card reader and method for storing data
US20150052264A1	2015-02-19	Wireless expansion card and method for data storage
CN104573773B	2017-09-29	A kind of smart card reader method
US20020013148A1	2002-01-31	Telephone set identifying method, telephone set type identifying apparatus, processing apparatus and storage medium
US6888217B2	2005-04-26	Data transfer control circuitry including FIFO buffers

IPR2025-00645 Page 01741

CN104700127B	2017-11-07	A kind of IC-card data transmission method
KR100537903B1	2005-12-20	Information processing device without supply of independent voltage source
JP2000227951A	2000-08-15	Method for managing electronic circuit
KR19990037579U	1999-10-15	Smart card interface
US7693554B2	2010-04-06	Method for operating a data storage medium
JP2005303596A	2005-10-27	Control method of infrared ray communication module
KR960027503A	1996-07-22	IC card and magnetic card combined mobile wireless payphone
CN101262517A	2008-09-10	A wireless communication module

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
US18022800P	2000-02-04	2000-02-04	*US Provisional Application*
US60/180,228		2000-02-04	

Legal Events

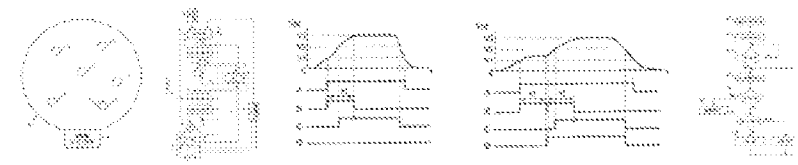
Date	Code	Title	Description
2006-02-03	WITN	Application deemed withdrawn, e g. because no request for examination was filed or no examination fee was paid	

Data provided by IFI CLAIMS Patent Services

Patents 3614157

RFID tag and method for adjusting resonance frequency in RFID tag

Images (10)



Classifications

G06K19/0726 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e.g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips the record carrier comprising an arrangement for non-contact communication, e.g. wireless communication circuits on transponder cards, non-contact smart cards or RFIDs the arrangement including a circuit for tuning the resonance frequency of an antenna on the record carrier

View 3 more classifications

JP3614157B2
Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: 裏…郎 福岡

Worldwide applications

2002 JP 2003 EP DE AT US CN

Application JP2002221841A events

2002-07-30 Application filed by オムロン株式会社
2002-07-30 Priority to JP2002221841A
2004-02-26 Publication of JP2004062665A
2005-01-26 Application granted
2005-01-26 Publication of JP3614157B2
Status Expired - Fee Related
2022-07-30 Anticipated expiration

Info: Patent citations (8), Cited by (65), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (4) Hide Dependent

1. An RFID tag,
A switching circuit for turning on and off an inductance forming a resonance circuit and a plurality of resonance capacitors or at least one connection of the plurality of resonance capacitors;
A constant voltage circuit for smoothing a power signal supplied from the interrogator (reader / writer) through the resonance circuit and outputting a constant voltage;
Voltage detecting means for detecting the smoothed voltage;
Voltage monitoring means for monitoring the degree of rise of the smoothed voltage;
A resonance capacitance switching command means for commanding on / off of the switching circuit in response to an output of the voltage monitoring means when a predetermined increase cannot be obtained;
The voltage monitoring means is
A first voltage detection circuit that outputs a detection output when the output from the constant voltage circuit reaches a first voltage, and a timer circuit that receives the output of the first voltage detection circuit and outputs a timer signal for a predetermined period When,
A second voltage detection circuit for outputting a detection output when the output of the constant voltage circuit reaches a second voltage higher than the first voltage;
While the timer circuit outputs the timer signal, when the output from the second voltage detection circuit is not obtained, the switching circuit is driven to reduce the capacitance value of the resonance capacitor, while the timer signal the operation before Symbol switching circuit after the output has exceeded the predetermined time,
RFID tag, characterized in that to return the resonant circuit to an initial state.

2. The resonance capacitor has a fixed capacitor and at least one adjustment capacitor When the resonance frequency increases, the resonance capacitor is disconnected, and the capacitance value of the resonance capacitor is reduced. 2. The RFID tag according to claim 1, wherein the RFID tag is controlled so as to approach a resonance frequency defined by.

3. When there are a plurality of adjustment capacitors, the voltage monitoring unit sequentially disconnects the adjustment capacitors every predetermined period, all the adjustment capacitors are disconnected, and the second voltage higher than the first voltage. 2. The RFID tag according to claim 1, wherein when the voltage cannot be reached, the resonance circuit is returned to the initial state.

4. At least one on-off of the above connection of the inductance and a plurality of resonance capacity or the plurality of resonance capacities to form a resonant circuit carried out by the switching circuit,
The constant voltage circuit outputs a constant voltage by smoothing the power signal given from the interrogator (reader / writer) via the resonance circuit,
A voltage detection means detects the smoothed voltage,
The voltage monitoring means monitors the degree of increase in the smoothed voltage,
When the predetermined increase cannot be obtained, the switching of the switching circuit is commanded by the resonance capacitance switching command means in response to the output of the voltage monitoring means,

IPR2025-00645 Page 01743

In the voltage monitoring means, when the output from the constant voltage circuit reaches the first voltage, the first voltage detection circuit outputs a detection output, and the timer circuit receives the output of the first voltage detection circuit. A timer signal for a predetermined period is output, and when the output of the constant voltage circuit reaches a second voltage higher than the first voltage, the detection output is output by the second voltage detection circuit, and the timer circuit outputs the timer signal. When the output from the second voltage detection circuit is not obtained during the output, the switching circuit is driven to reduce the capacitance value of the resonance capacitor, while the output of the timer signal has passed a predetermined period the operation before Symbol switching circuit after adjustment method of the resonance frequency in the RFID tag, characterized in that to return the resonant circuit to an initial state.

Description

[0001]
BACKGROUND OF THE INVENTION
The present invention relates to an RFID tag andMethod for adjusting resonance frequency in RFID tagAbout.
[0002]
[Prior art]
FIG. 1 shows a system overview of an RFID tag and an RFID interrogator using the RFID tag. In FIG. 1, reference numeral 1 denotes an RFID tag. The interrogator 2 (reader / writer) has a detection area 3 having a predetermined spread. That is, in this system, there may be a plurality of tags 1, 1.
[0003]
[Problems to be solved by the invention]
RF for books, envelopes, casino chips, etc.IDWhen the tag 1 is mounted, if the tags 1 overlap each other, there is a problem that the communication performance is remarkably lowered and the interrogator (reader / writer) 2 cannot be accessed successfully. In these applications, RFIDTag 1 stacked, orRFIDWith tag 1RFIDThere is a case where the interval between the tags 1 is set very close.
[0004]
In that state, L (inductance of the resonance coil) of both tags 1 is mutually coupled, and the mutual inductorNTend to form, and the inherent inductance of the tag 1 tends to increase in conjunction with the mutual inductance.
[0005]
This meansRFIDSince the resonance capacitor existing in the tag 1 has a constant value, the resonance frequency is lower than the state where there is no mutual coupling (the expected resonance frequency and the frequency specified by the interrogator). Means.
[0006]
On the other hand, from the interrogator (reader / writer) 2 sideRFIDOscillation is performed at the same frequency as the resonance frequency of tag 1 (expected resonance frequency). This meansRFIDResonance point decreased due to overlap of tag 1 etc.RFIDFrom the viewpoint of the tag 1, this means that a magnetic field whose resonance has shifted is supplied from the interrogator (reader / writer) 2 side antenna, and the supplied energy is reduced accordingly As a result, the communication distance is reduced.
[0007]
RFIDin order to eliminate the decrease in communication distance due to the overlapping of the tags 1, JP 2000-151480 A discloses an identification method when a plurality of tags are superimposed. This is where the built-in tagNAlthough a configuration is described in which the resonance frequency can be changed by switching the switch, a method of adjusting the built-in capacitor for each tag among a plurality of superimposed tags to adjust to the desired frequency States. The resonance frequency of other tags is changed sequentially after the communication with one tag is completed.
[0008]
In the case of this method, it is possible to match the resonance frequency of one tag with the resonance frequency emitted by the interrogator, but the resonance frequency of the other tag deviates from the resonance frequency emitted by the interrogator. Therefore, a general collision prevention procedure (for example, JIS6323-3 ISO / IEC15693-3) is not used, and the interrogator and the tag perform one-to-one communication.
[0009]
In addition, there is no method for determining the order between multiple tags (from which tag the resonance frequency is adjusted), and it is difficult to ensure stable operation as a realistic system, and difficult to realize. There is a problem.
[0010]
The present invention has been made to solve such a problem, and an object of the present invention is to effectively use a collision prevention related function called anti-collision, which has a simple configuration and can realize a stable system operation.Method for adjusting resonance frequency in RFID tagIs to provide.
[0011]
[Means for Solving the Problems]
RFIDThe following is a brief description of the problems that occur with tag superposition. That is, RFIDThe coil inductance L of the tag causes mutual inductance due to overlapping with other tags, and the L value is increased accordingly. Therefore, by reducing the value of C for resonance corresponding to the increment of L, the resonance frequency is always kept constant, thereby solving problems such as insufficient rise in power supply voltage. In addition, the configuration consists of a plurality of resonance capacitors, and by separating this resonance capacitor configured under certain conditions, the capacitor value is reduced, and the decrease in resonance frequency caused by the increase in mutual inductance is corrected. To do.
[0012]
In order to solve the above problems, an RFID tag according to the present invention includes an inductance forming a resonance circuit and a plurality of resonance capacitors, or at least one of the plurality of resonance capacitors.ConnectedA switching circuit for performing on / off, a constant voltage circuit for smoothing a power signal supplied from an interrogator (reader / writer) via the resonance circuit and outputting a constant voltage, and for detecting the smoothed voltage Voltage detecting means, voltage monitoring means for monitoring the degree of rise of the smoothed voltage, and resonance for commanding on / off of the switching circuit in response to the output of the voltage monitoring means when a predetermined increase cannot be obtained. Capacity switching command means, and the voltage monitoring means outputs a detection output when the output from the constant voltage circuit reaches a first voltage, and the first voltage detection circuit. A timer circuit that receives the output of the circuit and outputs a timer signal for a predetermined period, and a second circuit that outputs a detection output when the output of the constant voltage circuit reaches a second voltage higher than the first voltage. And when the output from the second voltage detection circuit cannot be obtained while the timer circuit outputs the timer signal, the switching circuit is driven to set the capacitance value of the resonance capacitor. While the output of the timer signal has passed a predetermined periodPreviousThe resonance circuit is returned to the initial state by the operation of the switching circuit
[0013]
Further, the resonance capacitor according to the present invention has a fixed capacitor and at least one adjustment capacitor, and when the resonance frequency increases, the adjustment capacitor is disconnected and the capacitance value of the resonance capacitor is reduced. Control is performed so as to approach the resonance frequency defined by the interrogator.
[0014]
Further, the voltage monitoring means according to the present invention, when there are a plurality of adjustment capacitors, sequentially disconnect the adjustment

IPR2025-00645 Page 01744

capacitors every predetermined period, all the adjustment capacitors are disconnected, andHigher than the first voltageThe resonance circuit is returned to the initial state when the second voltage cannot be reached.

[0015]

Furthermore, the method for adjusting the resonance frequency in the RFID tag according to the present invention includes an inductance forming a resonance circuit and a plurality of resonance capacitors, or at least one of the plurality of resonance capacitors.ConnectedON / OFF is performed by a switching circuit, the power signal supplied from the interrogator (reader / writer) through the resonance circuit is smoothed and the constant voltage circuit outputs a constant voltage, and the voltage detection means detects the smoothed voltage. Then, the voltage monitoring means monitors the degree of rise of the smoothed voltage, and when a predetermined increase cannot be obtained, the switching of the switching circuit is commanded by the resonance capacitance switching command means in response to the output of the voltage monitoring means. In the voltage monitoring means, when the output from the constant voltage circuit reaches the first voltage, the first voltage detection circuit outputs a detection output, and receives the output of the first voltage detection circuit to receive a timer. The circuit outputs a timer signal for a predetermined period, and when the output of the constant voltage circuit reaches a second voltage higher than the first voltage, the second voltage detection circuit outputs a detection output. While the timer circuit outputs the timer signal, when the output from the second voltage detection circuit cannot be obtained, the switching circuit is driven to reduce the capacitance value of the resonance capacitor, while the timer signal After the output has passed a predetermined periodPreviousThe resonance circuit is returned to the initial state by the operation of the switching circuit.

[0016]

ThisThe invention ofit is possible to switch the resonance capacity of the resonance circuit and stably update the data of the resonance frequency with the interrogator (reader / writer).

[0017]

DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the present invention will be described below with reference to the accompanying drawings. 2 is a block diagram of the main part of one embodiment of the RFID tag according to the present invention, FIG. 3 is a waveform diagram of the RFID tag according to the present invention, FIG. 4 is another waveform diagram of the RFID tag according to the present invention, FIG. FIG. 2 is an operation flowchart of one embodiment of an RFID tag according to the present invention. In FIG. 2, voltage detection means 8 and 11 are voltage monitoring means, latch circuit 15 is resonance capacitance switch command means, control circuit 12, UID storage means 16 and data modulator / demodulator 17 are anti-collision information output means, respectively. Constitute.

[0018]

The RFID tag 1 includes a parallel resonance circuit 4 including a coil L, a resonance capacitor C1, and an adjustment capacitor C2. Since the initial state of the switching circuit SW1 made of a semiconductor such as a CMOS-FET is ON, the adjustment capacitor C2 and the resonance capacitor C1 are connected in parallel and included in the resonance circuit 4 in the initial state. The resonance circuit 4 resonates when entering a high-frequency magnetic field (corresponding to the detection area 3 in FIG. 1) provided by the antenna of the interrogator (reader / writer) 2, and the resonance output is applied to the rectifier circuit 5.

[0019]

As a result, the rectifying circuit 5 outputs a direct current component (rectification result) corresponding to the degree of coupling between the RFID tag 1 and the interrogator (reader / writer) 2 antenna. This DC component is smoothed by the smoothing capacitor 6 and stabilized by the constant voltage circuit 7. However, the output of the constant voltage circuit 7 is stabilized after a predetermined time has elapsed since the RFID tag 1 entered the detection area 3, and the output Vcc of the constant voltage circuit 7 at the beginning of the entry is not stable. This is important for the present invention and will be described in detail below.

[0020]

On the other hand, various commands received from the interrogator (reader / writer) 2 via the coil L are demodulated by the data modulator / demodulator 17, and the demodulated commands are supplied to the control circuit 12 for processing. The control circuit 12 collates the UID included in the command with the UID of the UID storage means 16, and outputs the UID to the data modulator / demodulator 17 if they match, and the data modulator / demodulator 17 modulates the UID. The UID is transmitted to the interrogator (reader / writer) 2 through the coil L.

[0021]

When the control circuit 12 receives the data call request or data write request received from the interrogator (reader / writer) 2 via the coil L --- data modulator / demodulator 17, the control circuit 12 reads the requested data from the UID storage means 16. Output or write the requested data to the UID storage means 16.

[0022]

When receiving a command response prohibition request from the interrogator (reader / writer) 2, the control circuit 12 sets the prohibit mode and prohibits the response to the command as long as power is supplied thereafter.

[0023]

If it demonstrates using the waveform of FIG. 3, the constant voltage output Vcc will be 0 initially. As the RFID tag 1 enters the detection area 3, Vcc increases. When the voltage V1 is reached, the voltage V1 is detected by the first voltage detection circuit 8, and the voltage detection circuit 8 raises the detection output A.

[0024]

This output A is applied to the timer circuit 10 via an exclusive OR circuit 9. This timer circuit 10 is triggered by the rising or falling of its input. In this case, as shown by the signal waveform B in FIG. 3, the timer circuit 10 outputs a timed signal B for a predetermined timer time t1.

[0025]

When the constant voltage output Vcc reaches a higher voltage V2 during the timer time t1, the voltage V2 is detected by the second voltage detection circuit 11, and the detection output C rises. thisDetection outputC is applied to the reset terminal 13 of the control circuit 12. When the detection output C applied to the reset terminal 13 rises, the control circuit 12 can perform an original operation such as access to the interrogator (reader / writer) 2 or the like. In other words, thisDetection outputWhen C is at a low level, the control circuit 12 is held in a reset state, and at least its output section is immobilized so that no unnecessary signal is output. The above shows the case where the RFID tag 1 enters the detection area 3 of the interrogator (reader / writer) 2 and operates normally.

[0026]

Next, the case where it cannot be said that it is normal compared with FIG. 3 is demonstrated using the waveform of FIG. The power supply voltage Vcc in FIG. 4 does not rise smoothly compared to the waveform diagram 3. As described above, as described above, there are various cases where a plurality of RFID tags 1 are overlapped with each other and are located relatively far from the interrogator (reader / writer) 2.

[0027]

This unusual state is shown in FIG. 4, and in the operational flow diagram of FIG.Sit corresponds to 5 or later. That is, when the RFID tags 1 overlap each other, the power supply voltage Vcc cannot reach the voltage V2 even after the timer time t1 has elapsed after reaching the voltage V1. That is, the output C of the voltage detection circuit 11 that detects the voltage V2 remains at a low level.

[0028]

On the other hand, when the timer time t1 elapses in this state, the timer circuit 10fallsoutputSignal waveformB falls, and this fall is applied to the clock terminal CK of the latch circuit 15 via the OR circuit 14, and the output D of the latch circuit 15 is inverted. Thus, when the output of the latch circuit 15 is inverted, the output (inverted D) connected to the switching circuit SW1 is inverted from high to low, and the switching circuit SW1 is turned off.

[0029]

As a result, the adjustment capacitor C2 is disconnected from the resonance circuit 4, the resonance frequency of the resonance circuit 4 increases, and approaches the resonance frequency defined by the interrogator (reader / writer) 2. As a result, the power supply voltage Vcc rises as shown in FIG. When the power supply voltage Vcc reaches the operating voltage V2 of the circuit, the output C of the voltage detecting circuit 11 changes from low to high as described in the previous example, and the

IPR2025-00645 Page 01745

control circuit 12 enters the operating state. As a result, the corresponding RFID tag 1 can be accessed with the interrogator (reader / writer) 2.

[0030]

The above is an effective compensation operation in the case where the RFID tag 1 is superimposed and there is mutual interference. However, this compensation operation sometimes becomes a problem. That is, in the case of an application in which the RFID tag 1 moves and enters the communication area 3, even when the RFID tag 1 is alone, the operation is performed when the distance from the interrogator (reader / writer) 2 is long. It does not reach the level of the possible voltage V2, but reaches the voltage V1 that triggers the timer circuit 10.

[0031]

In this case, when the adjustment capacitor C2 is switched, the above-described compensation operation causes the resonance frequency of the RFID tag 1 to deviate from the desired resonance frequency, greatly reducing the communication distance of the corresponding single RFID tag 1. It will be.

[0032]

To improve this, the operation when the timer circuit 10 times up again is shown in the signal B of the waveform in FIG. That is, when the power supply voltage Vcc does not reach the voltage V2 at the second timer time t1, the timer circuit 10Autoutput Signal waveformWhile B falls, the voltage detection circuit 11Detection The output C is at a low level unlike the previous example. For this reason, the output of the OR circuit 14 falls. As a result, the state of the latch circuit 15 in which the output of the OR circuit 14 is applied to the clock terminal CK is reversed again, the switching circuit SW1 is turned on, the adjustment capacitor C2 is connected, and the resonance circuit 4 Return to state.

[0033]

As a result, since the distance from the interrogator (reader / writer) 2 is initially far, the power supply voltage Vcc is changed to the operating voltage V2.InThe RFID tag 1 that could not be reached also moves the interrogator (reader / writer) 2inAs the distance approaches, the power supply voltage Vcc increases. When the power supply voltage Vcc rises and reaches the voltage V2, the voltage V2 is detected by the voltage detection circuit 11, and the control circuit 12 is set to an accessible state in which communication with the interrogator (reader / writer) 2 is possible.

[0034]

Thus, for example, as shown in a part of FIG. 1, even when the RFID tags 1 and 1 are overlapped and superimposed, each resonance frequency is defined by the interrogator (reader / writer) 2. The access state can be set close to the frequency, the power supply voltage Vcc is secured, and signals can be transmitted and received between each RFID tag 1 and the interrogator (reader / writer) 2 relatively easily. Can do.

[0035]

Next, an anti-collision (multiple responder recognition) technique for distinguishing each RFID tag will be described. Here, an embodiment will be described based on Japanese Industrial Standard (JIS) X6323-3 (ISO / IEC 15693-3) "IC Card without External Terminal—Nearby Type—Part 3: Collision Prevention and Transmission Protocol". Therefore, in order to further understand this embodiment, the above-mentioned standard published by the Japanese Standards Association is helpful.

[0036]

In the anti-collision algorithm adopted here, an inventory of a plurality of responders (RFID tags 1, 1, 1,...) Existing in the communication area 3 of the interrogator (reader / writer) 2 is used as a UID. It is extracted based on (unique number of tag).

[0037]

The interrogator (reader / writer) 2 can detect the presence of a plurality of responders (RFID tags) (the RFID tag itself as a responder)Interrogator (Reader / Writer)The existence of another responder can be known only from the information from 2), and the subject of the algorithm execution is the reader / writer 2.

[0038]

FIG. 6 shows a UID (tag unique number) that is information for identifying each RFID tag. In this embodiment, the UID is composed of 64 bits as shown in FIG. 6, and the binary display character length of the number of time slots is set as an area. Here, since the number of time slots is 16, the area is divided in units of 4 bits, and the UID is divided into 16 areas. This UID uniquely sets each RFID tag by 14 areas and 56 bits of the IC manufacturer code 4 area and the serial number 10 area in areas A, B, C, and D. The UID of the control circuit 12 of the RFID tag 1 Written and kept inside.

[0039]

Next, the anti-collision sequence will be described with reference to the operation flowchart shown in FIG. The operation flowchart shown in FIG. 7 shows the contents of a program stored and executed in the interrogator (reader / writer) 2. Here, a typical anti-collision sequence when the number of time slots is 16 will be described.

[0040]

First, in step S11, an area (mask data area) that stores interrogator mask-related data is initialized. In this initialization, the mask length data is set to 0, the mask value data is set to a predetermined value, and the area position data indicating the position where the UID (unique data) stored in the RFID tag is operated is also set to 0.

[0041]

When you are ready to issue a command,SAt 12, the reader / writer 2 sends an inventory command. As a result, an inventory command is transmitted to the plurality of RFID tags 1. Since each RFID tag 1 has a mask length of 0, UIA response is independently returned to the interrogator (reader / writer) 2 at its own time slot timing determined in the area 0 of D. Therefore, in many cases, each UID returns a response alone to the interrogator (reader / writer) 2 due to the access between the two, but the response may collide with some of the RFID tags 1.

[0042]

Correspondingly, the stepsS13NA signal on the RFID tag 1 side in response to the Bentley command is detected to detect the time slot position where the collision occurred. The detected time slot position is stored in the collision slot buffer 18 shown in FIG. This is to distinguish the RFID tag 1 that has collided, as will be described later. The collision slot buffer 18 is formed in the interrogator (reader / writer) 2.

[0043]

If there is no collision, the next stepSWhen the presence of the tag is detected normally at 14, the UID data of the corresponding RFID tag 1 is stored and held in the detection UID buffer 19 shown in FIG. This detection UID buffer 19 is also formed in the interrogator (reader / writer) 2. In this way, the time slot data and the UID data that have collided are accumulated in the buffers 18 and 19 of the interrogator (reader / writer) 2.

[0044]

Next, if there is a tag that was successfully detected, this is the stepSThe next control is executed in step S16. StepSIn 16, the interrogator (reader / writer) 2 refers to the contents of the detection UID buffer 19 described above, specifies the corresponding (having UID) tag by specifying its UID, and accesses the tag. That is, necessary data / information exchange is completed.

[0045]

After this access is complete,SIn 17, a command for setting a state in which no response is returned to the inventory command called STAY QUIET command is transmitted to the corresponding RFID tag 1, and the operation as a tag is stopped. (However, when the power is reset, the state returns to the response state.) As a result, the access to the corresponding RFID tag 1 at this timing is terminated, which is equivalent to the fact that the corresponding RFID tag 1 does not exist (is not in stock). Transition to the state.

[0046]

Then stepS18 to search for any other RFID tag 1 detected,S15, if another RFID tag 1 is detected, the above stepsSThe process corresponding to each RFID tag 1 is repeated by repeating steps 16 and thereafter. When processing of the RFID tag 1 detected normally is completed, the stepSThe determination result at 15 is No, and the control is stepSMoved to 20.

[0047]

StepSAt 20, it is determined whether or not there is a collided RFID tag 1 by looking at the contents of the collision slot buffer 18. When it is detected that there is a

IPR2025-00645 Page 01746

collision.SThe determination of 20 is Yes and the step.SAfter 21, a process for distinguishing the collided tags using the UID is executed.

[0048]

le first step.SIn 21, the first time slot position data among the time slots in which the collision has occurred is taken in as mask related data. In this embodiment, as described above, there are 16 time slots. Now, it is assumed that a collision has occurred at two locations of time slot 1 and time slot 4. In this example, "1", that is, binary data (0001) is stored as the first time slot position data. In addition, (0001) is stored / stored as mask value data.

[0049]

Next steps.S22, the initial value is 0 (step.S11 is added to the mask length. As a result, the mask length is set to 4 bits. Also, +1 is added to the area position, and as a result, UID area 1 (see FIG. 6) is selected as position data for designating the next time slot.

[0050]

In this way, when the condition to execute the next inventory command is met, control.S12 is moved to. The inventory command to be executed next is different from the previous contents, and is updated with "mask length is 4", "mask value is 0001", and "UID area position is 1". In this way, the updated inventory command is executed. In this case where there is a tag that has collided, a value (0001) that has once collided is entered as a mask, so there are always a plurality of RFID tags. However, since the "UID area position" that specifies the timing at which the RFID tag 1 returns a response is different from the previous time, the possibility of collision again becomes low. However, it cannot be said that there is nothing in principle.

[0051]

Anyway, when the inventory command is performed again like this, the same step as the previous step is performed accordingly.SRepeat steps 15, 16, 17, and 18. As a result, access to the interrogator (reader / writer) 2 is completed for the RFID tag 1 detected normally, and the collision state is.stateAs a result, the number of RFID tags 1 that cannot be accessed decreases gradually. However, in principle, it is not completely eliminated. Therefore, if the collision tag remains after this second inventory command execution, again step.SControl is transferred to 20, and the determination result is Yes. And then step.SThe process of updating the inventory commands 21 and 22 is executed again, and the third inventory command is stepped accordingly.S12 is executed.

[0052]

Thereafter, when this process of updating such a mask position is repeated and there is no colliding slot, it is a step.SThe determination result determined at 20 is No, and the control is now a step.S23. As a result, this time, the control to return the area position is a step.S24, 25, and steps.SThe process of repeating 19 is performed. This is to cover a dropout when a collision occurs in a plurality of slots at the same area position. A series of processing is performed, and when the area position returns to 0, the anti-collision sequence is completed. By repeating the process in this manner, it is possible to substantially eliminate the remaining RFID tag 1 that cannot be accessed due to a collision.

[0053]

Next, the simple collision handling algorithm shown in FIG. 10 will be described. The operation flow diagram shown in FIG. 10 is a simplified version of the anti-collision algorithm shown in FIG.SAt 31, a read command with a simple collision prevention function is executed. In this case, a command having a code indicating the order of the unique ID of the tag to start the collision prevention slot and a code indicating the location of data to be read from the tag is issued as the command. As a result, step.SAs indicated by 12 and 13, the collided time slot, the normally detected UID, and the desired read data are stored and held.

[0054]

Step if there is a collision.SThe determination result of 35 is Yes, and step again.SA read command 31 with a simple collision prevention function is executed. In this case, this step.SIn 31, instead of executing the fine algorithm shown in the flowchart of FIG. 7, the next command is executed with a simple algorithm. That is, the next command is executed by simply moving the slot start position to the next position.

[0055]

In this way, when the slot start position is simply moved, it is not possible to completely eliminate the occurrence of a collision with the same RFID tag 1 again. However, as described above, the RFID tag 1 is given a unique UID at least with 56 bits of the IC manufacturer code and serial number, and the slot start position is simply and easily moved as described above. Even if the executed command is executed, each RFID tag 1 can be almost identified by repeating it several times from the second time, and there is no problem or malfunction in a normal application.

[0056]

This has been confirmed by experiments and experiences of the inventors. The merit of adopting such a simple collision prevention algorithm is that the system configuration is simplified and maintenance is facilitated, and the access speed between the RFID tag 1 and the interrogator (reader / writer) 2 is increased. As a result, in an application in which the RFID tag 1 and the interrogator (reader / writer) 2 move relative to each other, the reliability of signal exchange is improved, which is advantageous in ensuring the reliability of the system. . In such a case, the simplified collision prevention algorithm can be positively adopted by selecting application conditions.

[0057]

In the above-described embodiment, as shown in the circuit diagram of FIG. 2, there is one adjustment capacitor C2. By providing a plurality of adjustment capacitors C2, finer adjustment is possible. However, as a result of various experiments conducted by the inventors, a single adjustment capacitor is almost sufficient when the anti-collision function is used.

[0058]

【The invention's effect】

As described above, according to the present invention, an anti-collision function is mounted on the RFID tag, and a switching circuit for switching on and off the resonance capacitor is provided. For this reason, if a certain level of power supply voltage / operating voltage on the RFID tag side is obtained, identification of each RFID tag can be surely performed by the anti-collision function. For this reason, even if the change in the resonance frequency is set relatively rough, a stable operation can be secured, and the practicality that the reliability of the entire system can be easily improved is extremely high.

[Brief description of the drawings]

FIG. 1 is a system overview of an RFID tag and an RFID interrogator using the RFID tag.

FIG. 2 is a block diagram of a main part of an embodiment of an RFID tag according to the present invention.

FIG. 3 is a waveform diagram of an RFID tag according to the present invention.

FIG. 4 is another waveform diagram of the RFID tag according to the present invention.

FIG. 5 is an operation flowchart of one embodiment of an RFID tag according to the present invention.

6 is a UID (tag unique number) information diagram for identifying an RFID tag according to the present invention. FIG.

FIG. 7 is an operation flowchart of the anti-collision sequence according to the present invention.

FIG. 8 is an area storage diagram of a collision slot buffer according to the present invention.

FIG. 9 is a UID data storage diagram of a detection UID buffer according to the present invention.

FIG. 10 is an operation flowchart of the simple collision handling algorithm according to the present invention.

[Explanation of symbols]

1 RFID tag

2 Interrogator (reader / writer)

3 Detection area

4 Resonant circuit

5 Rectifier circuit

IPR2025-00645 Page 01747

6 Smoothing capacitor
7 Constant voltage circuit
8,11 Voltage detection circuit
9 Exclusive OR (Exclusive OR) circuit
10 Timer circuit
12 Control circuit
13 Reset terminal
14 OR circuit
15 Latch circuit
16 UID storage means
17 Data modulator / demodulator
18 Collision slot buffer
19 Detection UID buffer
C1 Capacitor for resonance
C2 Adjustment capacitor
SW1 switching circuit

Patent Citations (8)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US5111186A *	1990-11-29	1992-05-05	Sensormatic Electronics Corporation	LC-type electronic article surveillance tag with voltage dependent capacitor
US5446447A *	1994-02-16	1995-08-29	Motorola, Inc.	RF tagging system including RF tags with variable frequency resonant circuits
US5602538A *	1994-07-27	1997-02-11	Texas Instruments Incorporated	Apparatus and method for identifying multiple transponders
GB9813371DD *	1998-06-22	1998-08-19	Powell George L	Anti-collision tag apparatus and system
JP2000151480A *	1998-11-11	2000-05-30	Mitsubishi Materials Corp	Identification system for superposed tags
US6354493B1 *	1999-12-23	2002-03-12	Sensormatic Electronics Corporation	System and method for finding a specific RFID tagged article located in a plurality of RFID tagged articles
US6377203B1 *	2000-02-01	2002-04-23	3M Innovative Properties Company	Collision arbitration method and apparatus for reading multiple radio frequency identification tags
AT393437T *	2000-08-15	2008-05-15	Omron Tateisi Electronics Co	CONTACTLESS COMMUNICATION MEDIUM AND SYSTEM

* Cited by examiner, † Cited by third party

Cited By (65)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US6841981B2 *	2002-04-09	2005-01-11	Mstar Semiconductor, Inc.	Radio frequency data communication device in CMOS process
JP3874007B2 *	2004-01-27	2007-01-31	オムロン株式会社	Read / write processing apparatus and read / write processing method for RFID tag
US7132946B2 *	2004-04-08	2006-11-07	3M Innovative Properties Company	Variable frequency radio frequency identification (RFID) tags
JP4191088B2 *	2004-05-14	2008-12-03	株式会社デンソー	Electronic equipment
WO2006011207A1 *	2004-07-29	2006-02-02	Mitsubishi Denki Kabushiki Kaisha	Radio tag read system, radio tag read device, and radio tag
KR100624688B1 *	2004-08-09	2006-09-19	삼성전자주식회사	Apparatus and method for wireless communication in image forming system
PT1794665E *	2004-09-29	2008-06-18	Swisscom Ag	Method and system for inputting user instructions of a user controllable telecommunications device
US7385499B2	2004-10-12	2008-04-15	Aristocrat Technologies, Inc.	Method and apparatus for synchronization of proximate RFID readers in a gaming environment
US7316352B1	2004-12-23	2008-01-08	Storage Technology Corporation	System and method for locked code on a radio frequency identification tag
CN100373392C *	2005-01-11	2008-03-05	盛群半导体股份有限公司	Power supply processing interface in passive radio frequency identification system

IPR2025-00645 Page 01748

JP4873868B2 *	2005-02-09	2012-02-08	ルネサスエレクトロニクス株式会社	Passive RFID semiconductor device, IC tag, IC tag control method, and communication method
DE102005005812A1	2005-02-09	2006-08-17	Atmel Germany Gmbh	Circuit arrangement and method for supplying power to a transponder
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
KR101111722B1 *	2005-04-25	2012-03-19	엘지전자 주식회사	Reader control system
DE102005020101A1 *	2005-04-29	2007-01-25	Giesecke & Devrient Gmbh	Portable data carrier and method for operating a portable data carrier
JP2008543156A *	2005-05-23	2008-11-27	エヌエックスピー ビー ヴィ	Electronic communication system, in particular authentication control system and corresponding method
US8295851B2	2005-08-03	2012-10-23	Michael Edward Finnegan	Realtime, interactive and geographically defined computerized personal matching systems and methods
US8880047B2 *	2005-08-03	2014-11-04	Jeffrey C. Konicek	Realtime, location-based cell phone enhancements, uses, and applications
CN101248440B *	2005-08-25	2010-06-23	Nxp股份有限公司	Method and RFID reader for evaluating a data stream signal in respect of data and/or collision
JP2007064765A *	2005-08-30	2007-03-15	Fujitsu Ltd	Rfid tag device, rfid reader writer device and distance measuring system
US20070115098A1 *	2005-11-18	2007-05-24	Wj Communications, Inc.	Rfid system including tags having low rf scattering mode
US7933577B2 *	2005-11-29	2011-04-26	Electronics And Telecommunications Research Institute	Method and apparatus for sharing portable terminal in CDMA system and mobile RFID system
US7417496B2	2005-12-06	2008-08-26	Electronics And Telecommunications Research Institute	Demodulator circuit of RFID system
CN101346728B *	2005-12-21	2012-04-11	皇家飞利浦电子股份有限公司	Collaborating RFID devices
KR100680501B1	2006-03-08	2007-02-08	엘지이노텍 주식회사	Radio frequency identification system of dual phase locked loop type
US7439860B2 *	2006-03-22	2008-10-21	Assa Abloy Ab	Auto-tuned RFID reader antenna
KR101338815B1 *	2006-06-09	2014-04-23	가부시키가이샤 한도오따이 에네루기 켄큐쇼	Semiconductor device
KR100728306B1	2006-06-19	2007-06-13	학교법인 포항공과대학교	A anti-collision method of tag in rfid
US20090280753A1 *	2006-06-21	2009-11-12	Nxp B.V.	Method of Checking the Integrity of an Antenna Arrangement, Transmitter, Receiver and Transceiver
CN101246538A *	2007-02-14	2008-08-20	日电（中国）有限公司	Radio frequency recognition system and method
AU2008215173B2 *	2007-02-16	2013-05-02	Orica Explosives Technology Pty Ltd	Method of communication at a blast site, and corresponding blasting apparatus
US8354917B2 *	2007-02-21	2013-01-15	Impinj, Inc.	RFID tag chips and tags complying with only a limited number of remaining commands and methods
WO2008105477A1	2007-02-27	2008-09-04	Kyocera Corporation	Portable electronic device and magnetic antenna circuit
EP1973069B1	2007-03-22	2013-01-02	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
DE102007027610A1	2007-06-12	2008-12-24	Atmel Germany Gmbh	Transponder, method for operating a transponder
US7796039B2 *	2007-06-28	2010-09-14	International Business Machines Corporation	Quick and accurate detection and reporting of component failures using RFID
JP4488040B2	2007-07-26	2010-06-23	Ｔｄｋ株式会社	Radio communication transmitter / receiver, RFID system, and radio communication transmitter / receiver reception method
CN101098348B *	2007-07-27	2010-06-09	北京华大恒泰科技有限责任公司	Method for reading data of reader-writer in radio frequency recognition system, and method for sending data of label
JP5019381B2 *	2007-10-09	2012-09-05	東芝テック株式会社	Wireless tag reader and method
JP4974171B2 *	2007-12-07	2012-07-11	ソニーモバイルコミュニケーションズ株式会社	Non-contact wireless communication device, method for adjusting resonance frequency of non-contact wireless communication antenna, and portable terminal device
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices

IPR2025-00645 Page 01749

US7793237B2 *	2007-12-17	2010-09-07	International Business Machines Corporation	System, structure and method of providing dynamic optimization of integrated circuits using a non-contact method of selection, and a design structure
JP5364270B2 *	2008-01-22	2013-12-11	株式会社東芝	Charger
US8391817B2	2008-06-27	2013-03-05	Nxp B.V.	Method of and system for tuning an antenna
CN101338892B *	2008-07-29	2011-12-14	宁波瑞奥光电技术有限公司	Safety processing method of RFID system for door lock
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
WO2010032573A1 *	2008-09-17	2010-03-25	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
CN102282574B *	2008-12-15	2015-06-03	卡德赖博私人有限公司	An RFID tag
US10402710B1	2009-02-03	2019-09-03	Impinj, Inc.	RFID tags with public and private inventory states
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
DE102009013962A1	2009-03-20	2010-10-14	Texas Instruments Deutschland Gmbh	Power level indicator
CN101630374B *	2009-08-26	2012-05-23	北京商约纳电子有限公司	SIM card with radio frequency identification function and power-saving method thereof
US20110084814A1 *	2009-10-08	2011-04-14	Checkpoint Systems, Inc.	Security tag utilizing rfid reflectivity mode power rationing
US10049317B1	2010-02-01	2018-08-14	Impinj, Inc.	RFID tags with public and private inventory states
US8917160B2 *	2011-03-21	2014-12-23	Sony Corporation	RFID module
FR2987904B1 *	2012-03-07	2014-03-21	Commissariat Energie Atomique	DEVICE FOR EVALUATING THE DISTANCE BETWEEN AN RFID LABEL AND AN INTERFACE
GB2508380A *	2012-11-29	2014-06-04	Ibm	Remote control of electrical appliances
CN103884873A *	2014-03-20	2014-06-25	上海华力微电子有限公司	Structure for preventing occurrence of resonance in reliability test
US9275529B1	2014-06-09	2016-03-01	Tyco Fire And Security Gmbh	Enhanced signal amplitude in acoustic-magnetomechanical EAS marker
CN106203543B *	2015-02-11	2019-03-29	天地融科技股份有限公司	A kind of switching device
US10134252B1	2017-05-22	2018-11-20	Tyco Fire & Security Gmbh	Dual-sided security marker
CN107895131B *	2017-11-06	2021-08-13	厦门印天电子科技有限公司	RFID label checking method in accordance with ISO15693 protocol
US10637444B1 *	2018-12-21	2020-04-28	Northrop Grumman Systems Corporation	Near field RFID probe with tunning

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP3614157B2	2005-01-26	RFID tag and method for adjusting resonance frequency in RFID tag
EP2667328B1	2019-07-31	Multi-mode RFID tag architecture
CN100501758C	2009-06-17	Communication method for reader and tag in RFID system
US7274284B2	2007-09-25	Method for RF card detection in a contactless system
JP4983017B2	2012-07-25	Information access system and method for accessing information in a contactless information storage device
JP4685926B2	2011-05-18	Improved transponder
EP2537121B1	2016-04-13	Multiple antenna reading system suitable for use with contactless transaction devices
WO2010014435A1	2010-02-04	Self tuning rfid

JP2004248310A	2004-09-02	Data processing method for rfid tag and interrogator (reader/writer)
US20070257775A1	2007-11-08	Identification system and identification method
JP4466678B2	2010-05-26	RFID tag and method for adjusting resonance frequency in RFID tag
JP3607585B2	2005-01-05	Non-contact response device
EP1892645B1	2013-09-04	Smart card
TW201701195A	2017-01-01	Dual frequency HF-UHF identification device, in particular of the passive type
JP4426820B2	2010-03-03	Non-contact IC card
KR101633240B1	2016-06-23	Method of configuring two wireless devices for mutual communication
JP2002525932A	2002-08-13	Electrostatic radio frequency identification system with contactless programming function
JP2007094885A	2007-04-12	Radio tag reader/writer, and radio tag read/write method
JP2011048600A	2011-03-10	Reader/writer device
JP2004252602A	2004-09-09	Non-contact data carrier
KR100662050B1	2006-12-27	Anti-collision method for rfid readers
KR101500188B1	2015-03-09	Method and apparatus for sensing collision tag in rfid system
JP4135278B2	2008-08-20	ID tag
JP2007049527A	2007-02-22	Radio ic tag reader and moving-body reading system
JP2011107894A	2011-06-02	Rfid system and anti-collision processing method

Priority And Related Applications

Child Applications (1)

Application	Priority date	Filing date	Relation	Title
JP2004083655A	2004-03-22	2004-03-22	Division	Data processing method for rfid tag and interrogator (reader/writer)

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2002221841A	2002-07-30	2002-07-30	RFID tag and method for adjusting resonance frequency in RFID tag

Applications Claiming Priority (6)

Application	Filing date	Title
JP2002221841A	2002-07-30	RFID tag and method for adjusting resonance frequency in RFID tag
AT03254399T	2003-07-11	RFID TAG WITH TIMER SWITCHING
EP03254399A	2003-07-11	RFID-tag with tuning means
DE60308113T	2003-07-11	RFID tag with tuning circuit
US10/627,872	2003-07-28	RFID tag and method for processing RFID data
CNB031331467A	2003-07-29	RFID -tag, RFID-tag and interrogator (reader/writer) data processing method

Legal Events

Date	Code	Title	Description
2004-01-09	A975	Report on accelerated examination	**Free format text:** JAPANESE INTERMEDIATE CODE: A971005 **Effective date:** 20040108
2004-01-21	A131	Notification of reasons for refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A131

IPR2025-00645 Page 01751

			Effective date: 20040120
2004-03-23	A521	Written amendment	Free format text: JAPANESE INTERMEDIATE CODE: A523 Effective date: 20040322
2004-05-07	A131	Notification of reasons for refusal	Free format text: JAPANESE INTERMEDIATE CODE: A131 Effective date: 20040506
2004-06-22	A521	Written amendment	Free format text: JAPANESE INTERMEDIATE CODE: A523 Effective date: 20040621
2004-10-05	TRDD	Decision of grant or rejection written	
2004-10-13	A01	Written decision to grant a patent or to grant a registration (utility model)	Free format text: JAPANESE INTERMEDIATE CODE: A01 Effective date: 20041012
2004-11-11	A61	First payment of annual fees (during grant procedure)	Free format text: JAPANESE INTERMEDIATE CODE: A61 Effective date: 20041025
2004-11-12	R150	Certificate of patent or registration of utility model	Free format text: JAPANESE INTERMEDIATE CODE: R150
2007-10-18	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20071112 Year of fee payment: 3
2007-10-23	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20081112 Year of fee payment: 4
2008-10-23	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20081112 Year of fee payment: 4
2008-10-28	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20091112 Year of fee payment: 5
2009-10-27	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20101112 Year of fee payment: 6
2010-10-21	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20101112 Year of fee payment: 6
2010-10-26	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20111112 Year of fee payment: 7
2011-10-18	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20121112 Year of fee payment: 8
2012-10-16	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20121112 Year of fee payment: 8
2012-10-23	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20131112 Year of fee payment: 9
2014-11-12	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

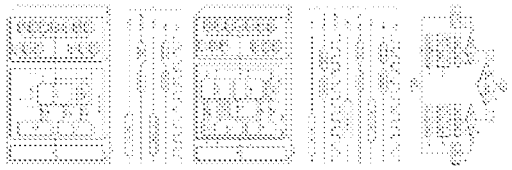
Patents KR101149887

Multi-channel memory card and control method thereof

Abstract

The memory card disclosed herein activates one or more data transmission / reception channels in response to a command input from the host, and independently performs data transmission / reception with the host through each data transmission / reception channel activated. As a result, a plurality of instructions can be processed at one time using one memory card, thereby improving data processing efficiency.

Images (5)



Classifications

G05B19/00 Electric permutation locks; Circuits therefor ; Mechanical aspects of electronic locks; Mechanical keys therefor

View 8 more classifications

KR101149887B1

South Korea

Download PDF Find Prior Art Similar

Other languages: Korean

Inventor: 강상욱, 김상범

Worldwide applications

2004 KR 2005 US JP DE 2011 US

Application KR1020040022571A events

2004-04-01 Application filed by 삼성전자주식회사

2004-04-01 Priority to KR1020040022571A

2005-10-07 Publication of KR20050097300A

2012-06-11 Application granted

2012-06-11 Publication of KR101149887B1

Info: Patent citations (27), Cited by (15), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (25)

Hide Dependent

1. A memory card having a plurality of data transmission / reception channels; And

   And a host for selectively activating the data transmission / reception channel provided in the memory card and providing a plurality of commands and data to the activated data transmission / reception channel.

   2. The memory card of claim 1, wherein the memory card is

      A plurality of input pins for receiving the plurality of commands and data provided from the host, a power supply voltage, a ground voltage, and a clock signal;

      An interface unit for dividing the plurality of commands by the channels; And

      A plurality of memory card controllers multi-accessed with the host through the plurality of channels to perform the command for each channel;

      Among the plurality of input pins, the pins receiving the command and the clock signal are dynamically allocated according to the number of channels.

      And the interface unit divides the command by the channel according to which of the pins allocated to receive the command is input.

3. delete

   4. The method of claim 2,

      And a number of command pins equal to the number of activated channels are assigned to the input pins.

   5. The method of claim 4, wherein

      The command pin is assigned from among the plurality of input pins, or has an additional pin on the memory card in addition to the input pins, characterized in that used as the command pin.

   6. The method of claim 2,

      The input pins include a first clock input pin for receiving the clock signal,

      When at least two channels are activated in the memory card, at least one of the input pins in addition to the first clock input pin is a second clock input pin so that data transmission / reception operation for each channel can be controlled independently. Memory card system, characterized in that additionally assigned.

   7. The method of claim 6,

      And an additional pin on the memory card in addition to the input pins, the memory card system being used as the second clock input pin.

IPR2025-00645 Page 01753

8. delete

9. delete

10. delete

11. delete

12. delete

13. delete

14. delete

15. delete

16. delete

17. delete

18. delete

19. In the control method of the memory card for performing a plurality of commands input from the host through a plurality of data transmission and reception channels:

Determining whether to use a multi-channel;

Performing the command through a single channel if the multi-channel is not used as a result of the determination;

Determining the number of channels when the multi-channel is used as a result of the determination;

Allocating a command line for each of the channels according to the determined number of channels;

Determining data rates for the channels; And

And performing a command for each channel at the determined data rate.

20. The method of claim 19,

The step of assigning the command line, the control method of the memory card, characterized in that for assigning the same number of command lines as the determined number of channels.

21. The method of claim 19,

The plurality of commands may be input through a command pin allocated among a plurality of input pins defined in the memory card, or may be input using a pin additionally provided in the memory card in addition to the input pins as the command pin. The control method of the memory card.

22. The method of claim 21,

The input pins include a first clock input pin,

The allocating of the command line may include removing at least one of the input pins in addition to the first clock input pin so that the data transmission / reception operation for each channel can be independently controlled when the determined channel is two or more. And assigning it to the second clock input pin.

23. delete

24. delete

25. delete

Description

Multi-channel memory card and control method thereof

1 is a block diagram of a two channel memory card according to a preferred embodiment of the present invention;

2 is a timing diagram for explaining a two-channel multi-access operation of the memory card shown in FIG. 1;

3 is a block diagram of a three channel memory card according to a preferred embodiment of the present invention;

4 is a timing diagram for explaining a three-channel multi-access operation of the memory card shown in FIG. And

5 is a flowchart illustrating a control method of a multi-channel memory card according to an exemplary embodiment of the present invention.

* Description of the symbols for the main parts of the drawings *

100, 200: memory card 120: input pin

130, 230: memory controller 140, 240: interface unit

150, 160, 250-270: control unit 180, 280: memory core

The present invention relates to a memory card having a flash memory, and more particularly, to a memory card capable of simultaneously performing at least two functions.

With the proliferation of portable digital devices such as digital cameras, MP3 players, color mobile phones, and personal digital assistants (PDAs), memory such as multimedia cards (hereinafter referred to as MMC cards) and SD cards (Secure Digital Cards) The demand for cards is growing rapidly. Memory cards are stamp-sized storage devices that cannot be erased without a power supply, and are becoming a necessity for information life due to their small size and abundant storage capacity.

According to the "MultiMediaCard Specification Version 4.0" published in February 2004, the MMC card has a 1-bit command line and an 8-bit data line, and writes data in bytes according to the command input from the host (Performs a write or read operation. However, according to the specification, only one function can be performed in one MMC card, and it is impossible to perform another function while one function is being performed. In addition, according to the MMC card specification currently used, even if two or more MMC cards are connected to an application, only one card that can transmit and receive data with the host is possible. Therefore, even if a plurality of MMC cards are connected, a plurality of functions are not provided. It cannot be done at the same time.

In addition, the MMC card requires several times longer than a normal write / read operation to perform a secured function. If the normal MMC operation is supported during this period, the security function may not be guaranteed. In case of not supporting normal MMC operation, there is a problem of waiting until all security functions are performed. This problem applies to SD cards as well as MMC cards.

Accordingly, an object of the present invention is to solve the above-mentioned problems, and to provide a multi-channel memory card having a plurality of data transmission / reception channels and a control method thereof.

SUMMARY OF THE INVENTION The present invention has been made in an effort to provide a multi-channel memory card and a control method capable of simultaneously performing a function other than a function being performed while a memory card performs a certain function.

An object of the present invention is to provide a multi-channel memory card and a control method capable of providing a multi-access function through a multi-channel while being compatible with a memory card specification.

In order to achieve the above object, the memory card system according to the present invention selectively activates a memory card having a plurality of data transmission / reception channels and the data transmission / reception channel provided in the memory card, and activates the activated data transmission / reception channel. It characterized in that it comprises a host for generating a plurality of commands.

In order to achieve the above object, the memory card according to the present invention comprises a plurality of input pins that receive one or more commands from a host, and one or more data transmission / reception channels in response to the command to activate data with the host. And a memory card control device which performs transmission and reception and stores the data transmission and reception result in a memory core.

In order to achieve the above object, the control method of the memory card according to the present invention comprises the steps of: (a) determining whether to use a multi-channel; (b) if the multi-channel is not used as a result of the determination in step (a), performing the command through a single channel; (c) checking the number of channels when using the multi-channel as a result of the determination in step (a); (d) allocating a command line and a data line for each channel; (e) determining data rates for the channels; And (f) performing a command for each channel at the data rate determined in step (e).

In a preferred embodiment, the plurality of input pins are pins defined according to the specification of the memory card, and have at least two ground pins and a plurality of input pins, and the memory card has two channels. One of the ground pins is used as a command pin that accepts a command, and when the memory card has three channels, one of the ground pins and one of the plurality of input pins respectively provide a command. The command pin is used as an accepting command pin, and the other one of the plurality of input pins is used as a clock input pin for receiving a clock signal required to execute the command

(Example)

Hereinafter, exemplary embodiments of the present invention will be described in detail with reference to FIGS. 1 to 5.

The novel memory card of the present invention activates one or more data transmission / reception channels in response to a command input from the host, and performs data transmission / reception with the host through each activated data transmission / reception channel. As a result, a plurality of instructions can be processed at one time by one memory card, and the data processing efficiency is greatly improved.

1 is a block diagram of a two-channel memory card 100 according to a preferred embodiment of the present invention, Figure 2 is a timing diagram for explaining the two-channel multi-access operation of the memory card 100 shown in FIG. .

First, referring to FIG. 1, the memory card 100 includes a plurality of input pins 120, a memory controller 130, and a memory core 180.

The plurality of input pins 120 are defined according to a specification of a memory card, for example, "MultiMediaCard Specification Version 4.0", and one or more instructions from the host through each of the pins 101-113 defined according to the specification. Accept data with The memory controller 130 activates one or two data transmission / reception channels in response to a command input from the input pins 120, and performs data transmission / reception with the host through the activated channel. The memory core 180 is configured of a flash memory to store data transmission / reception results performed by the memory controller 130.

The memory card 100 having such a configuration may also perform data transmission and reception through one channel according to a communication method defined in the memory card specification, and through two channels while being compatible with the existing memory card specification. Data transmission and reception may be performed simultaneously. As a result, while supporting all existing memory card specifications, it is possible to provide a multi-access function through multi-channels, thereby improving communication efficiency of the memory card 100. Here, the channel refers to a data transmission / reception channel which is composed of one command line and one or more data lines and performs an operation such as writing / reading satisfying a memory card specification.

First, the configuration of the input pins according to the memory card specification (for example, the MMC card specification) and the configuration of the input pins 120 according to the present invention will be described below.

IPR2025-00645 Page 01755

Pin #	MMC Mode(ver 4.0)			SPI Mode			2-Channel MMC Mode		
	Name	Type	Description	Name	Type	Description	Name	Type	Description
1	DAT3	I/O/PP	Data	CS	I	Chip select	DAT3	I/O/PP	Data
2	CMD	IO	Command/ Response	DI	I	Data In	CMD0	IO	Command1/ Response1
3	VSS1	S	Ground	VSS1	S	Ground	VSS	S	Ground
4	VDD	S	Power	VDD	S	Power	VDD	S	Power
5	CLK	I	Clock	CLK	I	Clock	CLK	I	Clock
6	VSS2	S	Ground	VSS2	S	Ground	CMD1	IO	Command2/ Response2
7	DAT0	I/O/PP	Data	DO	O	Data Out	DAT0	I/O/PP	Data
8	DAT1	I/O/PP	Data	Not used			DAT1	I/O/PP	Data
9	DAT2	I/O/PP	Data	Not used			DAT2	I/O/PP	Data
10	DAT4	I/O/PP	Data	Not used			DAT4	I/O/PP	Data
11	DAT5	I/O/PP	Data	Not used			DAT5	I/O/PP	Data
12	DAT6	I/O/PP	Data	Not used			DAT6	I/O/PP	Data
13	DAT7	I/O/PP	Data	Not used			DAT7	I/O/PP	Data

Referring to [Table 1], the memory card 100 according to the present invention may include a ground pin VSS2 in addition to a command pin (hereinafter, referred to as a first command pin) defined in a conventional memory card specification. By defining it as a man pin, you can accept two commands from the host at the same time. The number of such channels and the definition of the input pins 120 are determined when the host initializes the memory card 100, and the ground pin VSS2 depends on whether the host uses a single channel or two channels.) Is determined to be dedicated to the second command pin.

For example, when the memory card 100 uses one data transmission / reception channel, the memory card 100 uses one bit of command line CMD and eight bits of data line DAT0-7 according to the existing memory card specification. Data transmission and reception of 1, 4, or 8 bits is performed. In addition, when the memory card 100 uses both data transmission / reception channels, a total of 2 bit command lines CMD0 and CMD1 and 8 bit data lines DAT0-3 and DAT4-7 may be used. Therefore, data transmission and reception of 1 or 4 bits are simultaneously performed using 1 bit command line and 4 bit data line in two channels. At this time, since data transmission and reception performed in each channel are all performed according to the communication method defined in the memory card specification, a single memory card 100 simultaneously executes a plurality of commands as if a plurality of memory cards are operating at the same time. You can do it.

Subsequently, a configuration of the memory controller 130 that performs data transmission and reception for each channel is as follows.

IPR2025-00645 Page 01756

The memory controller 130 may include an interface unit 140 for dividing a plurality of commands input from the input pins 120 for each channel, and multi-accessed to the host through a plurality of channels, thereby providing each command And first and second controllers 150 and 160 for writing / reading data in the memory core 180 according to the command. The interface unit 140 includes a one channel interface unit 142 and a two channel interface unit 144.

When the memory card 100 is used as a 1-channel memory card, the 1-channel interface unit 142 transfers commands and data input from the input pins 120 into a 1-bit command line CMD and an 8-bit data line. The command line CMD and the data line transmit a response signal and data generated from the first control unit 150 by the command to the first control unit 150 through DAT0-7. Performs a function of transmitting to the input pins 120 through (DAT0-7). The first controller 150 performs data transmission and reception of 1, 4, or 8 bits with the host through the one channel interface unit 142, and stores the data transmission and reception result in the memory core 180.

In addition, when the memory card 100 is used as a two-channel memory card, the two-channel interface unit 144 divides the command and data input from the input pins 120 for each channel and divides the divided command and data by 1 bit. The first command line CMD0 and CMD1 and the 4-bit data lines DAT0-3 and DAT4-7 are transmitted to the first controller 150 and the second controller 160, respectively. The first and second controllers 150 and 160 transmit a response signal and data to be transmitted to the host through the command lines CMD0 and CMD1 and the data lines DAT0-3 and DAT4-7. By transmitting to the channel interface unit 144, respectively, the two-channel interface unit 144 transmits response signals and data input from the first and second control units 150 and 160 to the host. At this time, the two command lines CMD0 and CMD1 share one clock line CLK to perform data transmission and reception of 1 or 4 bits, and the data transmission and reception results are stored in the memory core 180

Referring to FIG. 2, when the host performs an operation of reading data from the memory card 100 while writing data to the memory card 100, the write command and the read command may be connected to the first command line CMD0. The first control unit 150 and the second control unit 160 are respectively transmitted through the second command line CMD1. Each response signal generated from the first and second controllers 150 and 160 is transmitted to a host through the first command line CMD0 and the second command line CMD1, respectively. Data to be written to the memory card 100 and data read from the memory card 100 are transmitted and received through the 4-bit data lines DAT0-3 and DAT4-7, respectively. As a result, the first and second controllers 150 and 160 may be multi-accessed with the host through two channels to perform independent data transmission and reception for each channel, and one memory card 100 may include at least two The above functions can be performed simultaneously.

Here, the interface unit 140 may be configured as a channel multiplexer circuit that performs signal selection for each channel. The interface unit 140 may be separately configured according to the number of channels, such as the one-channel interface unit 142 and the two-channel interface unit 144, or may be configured as one circuit to interface to both one and two channels. You can also do In addition, software may perform an interface for data transmission and reception of one channel or two channels

3 is a block diagram of a three channel memory card 200 according to a preferred embodiment of the present invention. Referring to FIG. 3, the memory card 200 may also transmit and receive data through one channel according to a communication method defined in the conventional memory card specification, and may be two or more while being compatible with the existing memory card specification. Data transmission and reception through three channels may be performed simultaneously.

Compared to the memory card 100 illustrated in FIG. 2, the memory card 200 illustrated in FIG. 3 has a different configuration of the input pins 220 and the memory controller 230 for transmitting and receiving data for three channels. Other circuit configurations are the same as the memory card 100 of FIG. 2 except that the three-channel interface unit 246 and the third control unit 270 are further provided therein. Therefore, duplicate descriptions will be omitted for simplicity.

Pin #	MMC Mode(ver 4.0)			SPI Mode			3-Channel MMC Mode		
	Name	Type	Description	Name	Type	Description	Name	Type	Description
1	DAT3	I/O/PP	Data	CS	I	Chip select	DAT3	I/O/PP	Data
2	CMD	IO	Command/ Response	DI	I	Data In	CMD0	IO	Command0/ Response0
3	VSS1	S	Ground	VSS1	S	Ground	VSS	S	Ground
4	VDD	S	Power	VDD	S	Power	VDD	S	Power
5	CLK	I	Clock	CLK	I	Clock	CLK0	I	Clock
6	VSS2	S	Ground	VSS2	S	Ground	CMD1	IO	Command1/ Response1
7	DAT0	I/O/PP	Data	DO	O	Data Out	DAT0	I/O/PP	Data
8	DAT1	I/O/PP	Data	Not used			DAT1	I/O/PP	Data
9	DAT2	I/O/PP	Data	Not used			DAT2	I/O/PP	Data

10	DAT4	I/O/PP	Data	Not used	CLK1/DAT4	I/O/PP	Clock
11	DAT5	I/O/PP	Data	Not used	CMD2/DAT5	I/O/PP	Command2/ Response2
12	DAT6	I/O/PP	Data	Not used	DAT6	I/O/PP	Data
13	DAT7	I/O/PP	Data	Not used	DAT7	I/O/PP	Data

Referring to [Table 2], the memory card 200 according to the present invention includes a command pin (hereinafter, referred to as a first command pin) defined in an existing memory card specification (for example, MMC card specification). By defining the ground pin VSS2 as the second command pin, it is possible to simultaneously accept two commands from the host. In addition, the fifth data pin DAT4 210 is defined as the second clock input pin CLK1 among the eight data pins 201 and 207-213, and the sixth data pin DAT5 211 is a third command. Each pin (CMD2) is defined to allow three commands to be accepted simultaneously from the host. In addition to the existing first clock input pin CLK, an additional second clock input pin CLK1 is defined to provide an independent interface to the third command using the second clock.

The number of such channels and the definition of the input pins 220 are determined when the host initializes the memory card 200, and the ground pins depend on whether the host uses a single channel or two or three channels. It is determined whether or not VSS2 and the sixth and fifth data pins DAT5 and DAT4 are dedicated to the second and third command pins and the clock input pin, respectively.

For example, when the memory card 200 uses one data transmission / reception channel, a 1-bit command line (CMD) and an 8-bit data line (DAT0-7) are used according to a conventional memory card specification. 1, 4, or 8 bits of data transmission and reception. In addition, when the memory card 200 uses two data transmission /

reception channels, one of the two command lines CMD0 and CMD1 has a data line of up to 4 bits and performs one function while the other Another function can be performed simultaneously using the command line CMD2 and a data line of up to 2 bits, and each of the two command lines CMD0 and CMD1 has a data line of 4 bits and has two functions. You can also do this at the same time. When the memory card 200 uses all three data transmission / reception channels, a total of three bit command lines CMD0, CMD1, and CMD2 and six bit data lines DAT0-1, DAT2-3, Since DAT6-7) can be used, data transmission and reception of one or two bits are simultaneously performed using one command line and two bits of data lines in three channels, respectively. At this time, since the data transmission and reception performed in each channel are all performed according to the communication method defined in the existing memory card specification, even one memory card 200 can have the same effect as operating a plurality of memory cards at the same time. Can be.

4 is a timing diagram for explaining a three-channel multi-access operation of the memory card 200 shown in FIG.

Referring to FIG. 4, the host writes data to the memory card 200 through the first command line CMD0 and the second command line CMD1, respectively, and the memory through the third command line CMD2. When the three operations of reading data from the card 200 are performed at once, the write command is performed through the first command line CMD0 and the second command line CMD1, respectively. The command is transmitted to the controller 260, and the read command is transmitted to the third controller 270 through the third command line CMD2. Each response signal generated from the first and second controllers 250 and 260 is transmitted to a host through the first command line CMD0 and the second command line CMD1, respectively. The response signal generated from the third controller 270 is transmitted to the host through the third command line CMD2. Subsequently, data to be written to the memory card 200 is transferred to the first and second controllers 250 and 260 through two-bit data lines DAT0-1 and DAT2-3, respectively, and from the memory card 200. The read data is transferred to the host through a 2-bit data line (DAT6-7). As a result, the first to third controllers 250 to 270 are multi-accessed with the host through three channels, and thus can independently transmit and receive data for each channel

In the above, the configuration and operation of a memory card having two or three channels, for example, a memory card having a multi-channel, have been described. However, this is only an example. The present invention can also be applied to other memory cards using the memory.

5 is a flowchart illustrating a control method of a multi-channel memory card according to an exemplary embodiment of the present invention.

Referring to FIG. 5, the method for controlling a multi-channel memory card according to the present invention first determines whether the memory card is a first type memory card or a second type memory card (step 300). Here, the first or second type of memory card is a memory card with a flash memory, such as an MMC card and an SD card.

If it is determined in step 300 that the memory card is the first type of memory card (eg, MMC card), it is determined whether to use the multi-channel (step 310). If it is determined in step 310 that the multi-channel is not used, one-channel data transmission and reception specified in the specification of the first type of memory card is performed (step 320). For example, when the first type of memory card is an MMC card, data transmission and reception of 1, 4, or 8 bits supported by the specification of the MMC card is performed.

If it is determined in step 310 that the multi-channel is to be used, the number of channels is determined (step 330), and the command line and data line are set according to the number of channels determined in step 330 (step 340). Then, after determining the number of bits of data to be transmitted and received for each channel, data transmission and reception for each channel is performed (step 350). In this case, when performing data transmission and reception through two channels, each channel performs data transmission and reception of 1 or 4 bits, and when performing data transmission and reception through three channels, 1 in each channel. Alternatively, two bits of data transmission and reception are performed.

On the other hand, if it is determined in step 300 that the memory card is a second type of memory card (for example, an SD card), it is determined whether to use the multi-channel (step 360). If it is determined in step 360 that the multi-channel is not used, one-channel data transmission and reception specified in the specification of the second type of memory card is performed (step 370). For example, when the second type of memory card is an SD card, data transmission and reception of 1, 2, or 4 bits supported by the specification of the SD card is performed.

If it is determined in step 360 that the multi-channel is used, the number of channels is determined (step 380), and the command line and data line are set according to the number of channels determined in step 380 (step 390). Then, after determining the number of bits of data to be transmitted and received for each channel, data transmission and reception for each channel is performed (step 400). In this case, when data transmission and reception are performed through two channels, one or two bits of data transmission and reception are performed on each channel, respectively. When data transmission and reception are performed through three channels, one bit on each channel. It will perform data transmission and reception of each.

IPR2025-00645 Page 01758

As described above, the multi-channel memory card 100 or 200 according to the present invention executes a plurality of commands simultaneously by providing a command line corresponding to the number of channels. For example, if two command lines are provided (i.e., two channels are provided), each command line performs one function using a data line of up to 8 bits or a maximum of 4 bits. Two functions are performed simultaneously using the data line of.

In addition, when a command line of 3 bits is provided (that is, when 3 channels are provided), the 2 command lines each have a maximum of 4 bit data lines and perform one function while the other The command line and the data line of up to 2 bits may be used to simultaneously perform another function, or each of the two command lines may simultaneously perform two functions with the data line of up to 4 bits. In addition, the three command lines may each perform three functions simultaneously with data lines of up to two bits.

In addition, the memory card according to the present invention further defines at least one or more clock lines in addition to the clock lines defined in the memory card specification, so that data transmission / reception operations performed in each channel can be controlled independently (that is, the channel). Very independent interfaces). In addition, the definitions of the input pins of the first type of memory card (eg, MMC card) and the second type of memory card (eg, SD card) having multi-channels and the number of transmission bits for each channel have been described. , This is just an example, and the definition of the function of each input pin may be changed, or the input pin provided in the existing specification, or may be further provided with an additional pin.

As described above, the optimum embodiment has been disclosed in the drawings and the specification. Although specific terms have been used herein, they are used only for the purpose of describing the present invention and are not intended to limit the scope of the invention as defined in the claims or the claims. Therefore, those skilled in the art will understand that various modifications and equivalent other embodiments are possible from this. Therefore, the true technical protection scope of the present invention will be defined by the technical spirit of the appended claims.

According to the present invention as described above, the multi-channel memory card is activated one or more data transmission and reception channels in response to a command input from the host, and can perform data transmission and reception with the host through each data transmission and reception channel activated. Will be.

As a result, a plurality of instructions can be processed at one time using one memory card, thereby improving data processing efficiency.

Patent Citations (27)

Publication number	Priority date	Publication date	Assignee	Title
JPH08263353A *	1995-03-20	1996-10-11	Fujitsu Ltd	Card type storage medium
JPH11175692A	1997-12-10	1999-07-02	Fujitsu Ltd	Card type storage medium and access control method for the same and computer readable recording medium for recording access control program for card type storage medium
JP2001307038A	2000-04-14	2001-11-02	Ritsuwa Yo	Memory card with multi-interface and its conversion adaptor
JP2003005874A	2001-06-20	2003-01-08	Canon Inc	Card interface

Family To Family Citations

FR2680262B1	1991-08-08	1993-10-08	Gemplus Card International	INTEGRATED CIRCUITS FOR CHIP CARD AND MULTIPLE CHIP CARD USING THESE CIRCUITS.
US6349297B1 *	1997-01-10	2002-02-19	Venson M. Shaw	Information processing system for directing information request from a particular user/application, and searching/forwarding/retrieving information from unknown and large number of information resources
JP2502894B2	1992-08-13	1996-05-29	松下電器産業株式会社	IC card
DE4406704C1	1994-03-02	1995-07-20	Angewandte Digital Elektronik	Smart card
US5761732A *	1996-06-28	1998-06-02	Intel Corporation	Interleaving for memory cards
US6167466A *	1997-07-09	2000-12-26	Texas Instruments Incorporated	Multi-channel serial port with programmable features
US6018218B1 *	1998-01-05	2001-01-30	Intel Corporation	Method and apparatus for placing a memory in a read-while-write mode
JP2000046916A *	1998-07-30	2000-02-18	Ando Electric Co Ltd	Pattern data transferring circuit
US6279114B1	1998-11-04	2001-08-21	Sandisk Corporation	Voltage negotiation in a single host multiple cards system
JP4252139B2 *	1998-12-16	2009-04-08	株式会社日立製作所	Storage system
US6336983B1 *	1999-09-14	2002-04-02	Intel Corporation	Method and system for symmetric memory population
CN1218276C *	2000-04-28	2005-09-07	株式会社日立制作所	IC card
US6438638B1	2000-07-06	2002-08-20	Onspec Electronic, Inc.	Flashtoaster for reading several types of flash-memory cards with or without a PC
JP2002140234A *	2000-11-02	2002-05-17	Hitachi Ltd	Cache device
DE10056592A1	2000-11-15	2002-05-23	Philips Corp Intellectual Pty	Device with microprocessor, for smartcard controller has interfaces including USB interface for exchanging data signals with microprocessor
JPWO2002069127A1	2001-02-26	2004-07-02	東京エレクトロンデバイス株式会社	Storage medium control method, storage medium control device, and storage medium adapter
JP4188668B2	2001-07-09	2008-11-26	株式会社ルネサステクノロジ	Storage device
JP2003123032A	2001-10-12	2003-04-25	Hitachi Ltd	Ic card terminal and individual authentication method

IPR2025-00645 Page 01759

US7139893B2 *	2001-10-30	2006-11-21	Micron Technology, Inc.	Transparent SDRAM in an embedded environment
JP2003281485A	2002-03-26	2003-10-03	Toshiba Corp	Memory card and method for recording data of the memory card
KR100745514B1	2002-10-25	2007-08-02	가부시키가이샤 히타치세이사쿠쇼	Ic card
KR200316559Y1	2003-02-21	2003-06-18	퍼워 데이터 커뮤니케이션즈 캄퍼니 리미티드	Multiplex transmission interface memory card
US7062615B2 *	2003-08-29	2006-06-13	Emulex Design & Manufacturing Corporation	Multi-channel memory access arbitration method and system

* Cited by examiner, † Cited by third party

Cited By (15)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
DE102006021087A1 *	2006-05-05	2007-11-08	Giesecke & Devrient Gmbh	Simultaneous interface operation
KR100765786B1 *	2006-06-12	2007-10-12	삼성전자주식회사	Flash memory system, host system for programming and program method thereof
US7886212B2	2007-01-17	2011-01-04	Research In Motion Limited	Methods and apparatus for use in transferring user data between two different mobile communication devices using a removable memory card
US8160494B2	2007-01-17	2012-04-17	Research In Motion Limited	Methods and apparatus for use in switching user account data and operations between two different mobile communication devices
KR100875978B1	2007-02-06	2008-12-26	삼성전자주식회사	Memory card and memory system including it
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US8881305B2 *	2009-07-13	2014-11-04	Blackberry Limited	Methods and apparatus for maintaining secure connections in a wireless communication network
US10157678B2	2014-08-12	2018-12-18	Samsung Electronics Co., Ltd.	Memory card
KR20160019854A	2014-08-12	2016-02-22	삼성전자주식회사	Memory card
EP2996069A1	2014-09-09	2016-03-16	Kabushiki Kaisha Toshiba	Ic card, ic module, portable terminal, portable electronic apparatus, and terminal

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
KR101149887B1	2012-06-11	Multi-channel memory card and control method thereof
US20190129625A1	2019-05-02	Memory card and host device thereof
KR100843546B1	2008-07-04	Multi-chip packaged flash memory device and reading method of status data thereof
US8924627B2	2014-12-30	Flash memory device comprising host interface for processing a multi-command descriptor block in order to exploit concurrency
KR101626084B1	2016-06-01	Multi-chip memory system and data transfer method thereof

US9389804B2	2016-07-12	Host, system, and methods for transmitting commands to non-volatile memory card
US20110239009A1	2011-09-29	Storage device
US10725902B2	2020-07-28	Methods for scheduling read commands and apparatuses using the same
US20040030830A1	2004-02-12	Storage medium control method, storage medium control device, and storage medium adaptor
US10275013B2	2019-04-30	Apparatuses and methods of entering unselected memories into a different power mode during multi-memory operation
KR20130009536A	2013-01-23	Memory control device and method
KR20070066539A	2007-06-27	Method and apparatus for controlling flash memory
JP4794949B2	2011-10-19	MEMORY CONTROLLER, NONVOLATILE STORAGE DEVICE, AND NONVOLATILE STORAGE SYSTEM
KR20130084902A	2013-07-26	Storage device, storage system, and i/o control method for the same
KR100911944B1	2009-08-05	Flash memory control apparatus and method sharing control signal
US20200356407A1	2020-11-12	Controller and memory system having the same
KR1022A2957B1	2021-04-21	High speed NAND memory system and high speed NAND memory package device
US10394486B2	2019-08-27	Methods for garbage collection in a flash memory and apparatuses using the same
US20130019055A1	2013-01-17	Memory control device and method
KR100676223B1	2007-01-30	Apparatus for controling nand flash memory
KR20060047052A	2006-05-18	Multi-interfacing card and method of initializing the multi-interfacing card
KR20100070595A	2010-06-28	Access structure between processor and a plurality of nand flash memories

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
KR1020040022571A	2004-04-01	2004-04-01	Multi-channel memory card and control method thereof

Applications Claiming Priority (5)

Application	Filing date	Title
KR1020040022571A	2004-04-01	Multi-channel memory card and control method thereof
US11/073,543	2005-03-08	Multi-channel integrated circuit card and method of controlling the same
JP2005076031A	2005-03-16	Integrated circuit card system, memory card and control method thereof
DE102005015723A	2005-03-31	Memory card, IC card system and control method
US13/067,061	2011-05-02	Multi-channel integrated circuit card and method of controlling the same

Legal Events

Date	Code	Title	Description
2009-04-01	A201	Request for examination	
2010-09-30	E902	Notification of reason for refusal	
2011-06-27	E902	Notification of reason for refusal	
2012-02-20	E701	Decision to grant or registration of patent right	
2012-05-18	GRNT	Written decision to grant	
2015-04-29	FPAY	Annual fee payment	**Payment date:** 20150430 **Year of fee payment:** 4
2016-04-28	FPAY	Annual fee payment	**Payment date:** 20160429

IPR2025-00645 Page 01761

			Year of fee payment: 5
2017-04-26	FPAY	Annual fee payment	Payment date: 20170427 Year of fee payment: 6
2018-04-27	FPAY	Annual fee payment	Payment date: 20180430 Year of fee payment: 7
2019-05-19	LAPS	Lapse due to unpaid annual fee	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents IL119943

Contact/contactless data transaction card

Classifications

G06K19/07769 Constructional details, e.g. mounting of circuits in the carrier the record carrier being capable of non-contact communication, e.g. constructional details of the antenna of a non-contact smart card comprising at least a second communication arrangement in addition to a first non-contact communication arrangement the further communication means being a galvanic interface, e g. hybrid or mixed smart cards having a contact and a non-contact interface

View 2 more classifications

IL119943A

Issue

Find Prior Art Similar

Worldwide applications

1996 IL 1997 DE AT CA WO EP AU EE US 2000 HK

Application IL11994396A events

1996-12-31 Application filed by On Track Innovations LTd

1996-12-31 Priority to IL11994396A

1997-03-18 Publication of IL119943DD

2000-11-21 Publication of IL119943A

2012-03-26 First worldwide family litigation filed

Info: Patent citations (8), Cited by (198), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (8)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
DE3935364C1 *	1989-10-24	1990-08-23	Angewandte Digital Elektronik Gmbh, 2051 Brunstorf, De	
EP0447688B1 *	1990-02-06	1995-10-11	ALCATEL BELL Naamloze Vennootschap	Electronic fraud detector
US5241160A *	1990-12-28	1993-08-31	On Track Innovations Ltd.	System and method for the non-contact transmission of data
NL9101608A *	1991-09-24	1993-04-16	Nedap Nv	CHIP CARD WITH REMOTE IDENTIFICATION.
DE4310334A1 *	1993-03-31	1994-10-06	Walter Holzer	Chip (smart) card with which contact is made
DE4408793C1 *	1994-02-08	1995-07-20	Angewandte Digital Elektronik	Combined chip card
DE4406704C1 *	1994-03-02	1995-07-20	Angewandte Digital Elektronik	Smart card
WO1996038814A2 *	1995-06-02	1996-12-05	Philips Electronics N.V.	Chip-card

* Cited by examiner, † Cited by third party

Cited By (198)

Publication number	Priority date	Publication date	Assignee	Title
WO1999052061A1	1998-04-03	1999-10-14	On Track Innovations Ltd.	Data transaction system for process monitoring and event tracking
Family To Family Citations				
FR2761113B1 *	1997-02-24	1999-06-04	Gemplus Card Int	METHOD FOR MANUFACTURING A CONTACTLESS CARD WITH A COILED ANTENNA
JPH10320519A *	1997-05-19	1998-12-04	Rohm Co Ltd	Responder in ic card communication system
KR100540885B1 *	1997-10-22	2006-01-10	코닌클리케 필립스 일렉트	Dual-mode data carrier and circuit for such a carrier with simplified data transfer means

IPR2025-00645 Page 01763

			로닉스 엔.브이.	
GB2330957B *	1997-11-01	2002-06-05	Motorola Inc	Power supply clamp and method in a smartcard
IL122250A	1997-11-19	2003-07-31	On Track Innovations Ltd	Smart card amenable to assembly using two manufacturing stages and a method of manufacture thereof
DE19805282A1 *	1998-02-10	1999-08-19	Siemens Ag	Flat carrier with a display device
ES2157899T3 *	1998-02-17	2001-08-01	Infineon Technologies Ag	DATA SUPPORT FOR OPERATION BOTH WITHOUT CONTACT AND WITH CONTACT.
EP0993647A1 *	1998-05-07	2000-04-19	Orga Kartensysteme GmbH	Method for controlling communication between a microprocessor chip card and a contact terminal or a contactless terminal
EP0945828B1 *	1998-03-24	2006-11-15	Kabushiki Kaisha Toshiba	IC card with contacting and noncontacting interfaces
IL124424D0 *	1998-05-11	1998-12-06	On Track Innovations Ltd	Self-closing cap including an integral smart card
FR2783069B1 *	1998-09-04	2003-01-24	Inside Technologies	CHIP CARD READER
FR2783336B1 *	1998-09-11	2001-10-12	Schlumberger Ind Sa	DATA TRANSMISSION METHOD AND CARD FOR SUCH TRANSMISSION
EP1054616B1	1999-01-26	2003-07-30	Koninklijke Philips Electronics N.V.	Data carrier provided with at least two decoding stages
EP1026627A1 *	1999-01-29	2000-08-09	Siemens Aktiengesellschaft	Contactless data communication system and method
JP3833939B2 *	1999-06-29	2006-10-18	株式会社ルネサステクノロジ	Compound IC card
US6955308B1	1999-06-29	2005-10-18	Renesas Technology Corp	Dual interface IC card
DE19929766C1 *	1999-06-29	2001-03-22	Wacker Werke Kg	Nameplate with storage device
JP4022401B2 *	1999-06-29	2007-12-19	株式会社ルネサステクノロジ	IC chip and IC card
JP3349998B2 *	1999-09-07	2002-11-25	エヌイーシーマイクロシステム株式会社	Data processing device and operation control method thereof
JP4341127B2 *	1999-12-20	2009-10-07	ソニー株式会社	Information processing device, IC card and reader / writer
JP2001257672A *	2000-03-14	2001-09-21	Mitsubishi Electric Corp	Method, device and system for authentication and ic card
EP1279140B1 *	2000-05-03	2010-09-29	Gemalto SA	Integrated circuit card and case therefor
DE10107373A1	2001-02-16	2002-08-29	Infineon Technologies Ag	Security module with volatile memory for storing an algorithm code
FR2822272B1 *	2001-03-13	2003-06-27	St Microelectronics Sa	CONTACTLESS CHIP CARD WITH OPERATING SYSTEM USED IN CONTACT CARDS AND READER OF SUCH CONTACTLESS CARDS
FR2823339A1 *	2001-04-04	2002-10-11	St Microelectronics Sa	CONTACTLESS INTEGRATED CIRCUIT COMPRISING A CABLE LOGIC ANTI-COLLISION CIRCUIT
US6899277B2 *	2001-05-17	2005-05-31	Matsushita Electric Industrial Co., Ltd.	IC card and electronic devices
JP2003016398A *	2001-06-27	2003-01-17	Sony Corp	Portable terminal machine
US20030017848A1 *	2001-07-17	2003-01-23	Engstrom G. Eric	Personalizing electronic devices and smart covering
JP2003132313A *	2001-10-24	2003-05-09	Toshiba Corp	Lsi for combination card, combination card, and using method for combination card
JP3617491B2 *	2001-10-31	2005-02-02	ソニー株式会社	IC chip and information processing terminal
JP3617509B2 *	2001-10-31	2005-02-09	ソニー株式会社	IC card, information processing terminal, three-party data communication system and method
US20030085288A1 *	2001-11-06	2003-05-08	Luu Daniel V.H.	Contactless SIM card carrier with detachable antenna and carrier therefore
US20060163364A1 *	2002-06-10	2006-07-27	Ken Sakamura	Ic chip, card and mobile terminal connected to the same
US20030230631A1 *	2002-06-17	2003-12-18	Hitachi, Ltd.	IC card
US7792759B2 *	2002-07-29	2010-09-07	Emv Co. Llc	Methods for performing transactions in a wireless environment
JP2004218225A *	2002-12-17	2004-07-29	Sony Corp	Communication system, communication method, and data processing device

IPR2025-00645 Page 01764

JP4224809B2 *	2003-03-03	2009-02-18	旭精工株式会社	Communication board mounting device for IC card processing device
DE10311123A1 *	2003-03-12	2004-09-23	Giesecke & Devrient Gmbh	Method for handling portable data carrier usable as electronic entry card, involves first interface with first data protocol for public network and second interface with second data protocol for testing purposes
DE10311966A1 *	2003-03-18	2004-12-16	Infineon Technologies Ag	smart card
WO2005020135A1 *	2003-08-21	2005-03-03	Axalto Sa	Communication system and method
KR100560768B1 *	2003-09-05	2006-03-13	삼성전자주식회사	Dual interface integrated circuit card
FR2859560B1 *	2003-09-05	2007-08-17	Samsung Electronics Co Ltd	CHIP CARD AND METHOD OF PROCESSING DATA ON THE CARD
JP4412947B2 *	2003-09-08	2010-02-10	株式会社ルネサステクノロジ	Memory card
JP4617683B2	2004-02-24	2011-01-26	ソニー株式会社	Semiconductor integrated circuit, portable module, and message communication method.
KR100579953B1 *	2004-08-26	2006-05-12	삼성전자주식회사	Method of multi-interfacing between smart card and memory card and multi-interface card
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
JP5186359B2	2005-03-26	2013-04-17	プリバシーズ，インコーポレイテッド	Electronic financial transaction card and method
US8684267B2	2005-03-26	2014-04-01	Privasys	Method for broadcasting a magnetic stripe data packet from an electronic smart card
WO2006116772A2	2005-04-27	2006-11-02	Privasys, Inc.	Electronic cards and methods for making same
US7642781B2 *	2005-04-15	2010-01-05	Cornell Research Foundation, Inc.	High-pass two-dimensional ladder network resonator
US7793851B2 *	2005-05-09	2010-09-14	Dynamics Inc.	Dynamic credit card with magnetic stripe and embedded encoder and methods for using the same to provide a copy-proof credit card
US20080035738A1 *	2005-05-09	2008-02-14	Mullen Jeffrey D	Dynamic credit card with magnetic stripe and embedded encoder and methods for using the same to provide a copy-proof credit card
KR100728636B1 *	2005-08-09	2007-06-15	(주)한창시스템	Apparatus and Method for Performing Secure NFC with Secure Application Modules
KR100728637B1 *	2005-09-08	2007-06-15	(주)한창시스템	Apparatus and Method for Performing Secure NFC with Secure Application Modules in Plug-In Type
US20070087838A1 *	2005-09-12	2007-04-19	Jonathan Bradbury	Video game media
US20070087837A1 *	2005-09-12	2007-04-19	Jonathan Bradbury	Video game consoles
US7883420B2 *	2005-09-12	2011-02-08	Mattel, Inc.	Video game systems
US7261262B2 *	2005-09-15	2007-08-28	Dps, Llc	Bucket brace and method for use
DE102006021087A1 *	2006-05-05	2007-11-08	Giesecke & Devrient Gmbh	Simultaneous interface operation
CN100504921C *	2006-06-29	2009-06-24	北京握奇数据系统有限公司	Smart card operating system and method thereof
US8078226B2	2007-08-29	2011-12-13	Mxtran, Inc.	Multiple interface card in a mobile phone
US8070057B2	2007-09-12	2011-12-06	Devicefidelity, Inc.	Switching between internal and external antennas
US9311766B2 *	2007-09-12	2016-04-12	Devicefidelity, Inc.	Wireless communicating radio frequency signals
US20090070691A1 *	2007-09-12	2009-03-12	Devicefidelity, Inc.	Presenting web pages through mobile host devices
US9304555B2 *	2007-09-12	2016-04-05	Devicefidelity, Inc.	Magnetically coupling radio frequency antennas
US8915444B2	2007-09-12	2014-12-23	Devicefidelity, Inc.	Amplifying radio frequency signals
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090160617A1	2007-12-24	2009-06-25	Dynamics Inc.	Credit, security, debit cards and the like with buttons
US8199725B2 *	2008-03-28	2012-06-12	Research In Motion Limited	Rank indicator transmission during discontinuous reception
ITMI20080550A1 *	2008-03-31	2009-10-01	Incard Sa	INTEGRATED CIRCUIT BOARD WITH WIRELESS FUNCTIONS.

ITMI20080543A1 *	2008-03-31	2009-10-01	Incard Sa	INTEGRATED CIRCUIT CARD INCLUDING REFINED ELECTRICAL CONTACTS.
DE102008018896A1 *	2008-04-14	2009-10-15	T-Mobile International Ag	Chip card with transmitting and receiving device and antenna for radio transmissions
JP4640451B2 *	2008-06-06	2011-03-02	ソニー株式会社	Contact / non-contact composite IC card, communication method, program, and communication system
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2342681B1 *	2008-09-30	2013-03-27	Deutsche Telekom AG	Method and communication system for the authorization-dependent control of a contactless interface device
US8550361B2 *	2008-10-28	2013-10-08	First Data Corporation	Systems, methods, and apparatus to facilitate locating a user of a transaction device
US20100102131A1 *	2008-10-28	2010-04-29	First Data Corporation	Systems and Methods for Disabling a Contactless Transaction Device
US20100102123A1 *	2008-10-28	2010-04-29	First Data Corporation	Systems, Methods, and Apparatus for Facilitating Access to Medical Information
US10803351B2 *	2008-10-31	2020-10-13	First Data Corporation	Systems, methods, and apparatus for using a contactless transaction device reader with a computing system
WO2010066955A1	2008-12-11	2010-06-17	Yves Eray	Rfid antenna circuit
US8579203B1	2008-12-19	2013-11-12	Dynamics Inc.	Electronic magnetic recorded media emulators in magnetic card devices
US8931703B1	2009-03-16	2015-01-13	Dynamics Inc.	Payment cards and devices for displaying barcodes
US9329619B1	2009-04-06	2016-05-03	Dynamics Inc.	Cards with power management
US8172148B1	2009-04-06	2012-05-08	Dynamics Inc.	Cards and assemblies with user interfaces
US8622309B1	2009-04-06	2014-01-07	Dynamics Inc.	Payment cards and devices with budgets, parental controls, and virtual accounts
US8393545B1	2009-06-23	2013-03-12	Dynamics Inc.	Cards deployed with inactivated products for activation
JP5347813B2 *	2009-08-03	2013-11-20	ソニー株式会社	Communication apparatus and communication method
US8511574B1	2009-08-17	2013-08-20	Dynamics Inc.	Advanced loyalty applications for powered cards and devices
US9306666B1	2009-10-08	2016-04-05	Dynamics Inc.	Programming protocols for powered cards and devices
US8727219B1	2009-10-12	2014-05-20	Dynamics Inc.	Magnetic stripe track signal having multiple communications channels
US8523059B1	2009-10-20	2013-09-03	Dynamics Inc.	Advanced payment options for powered cards and devices
US8393546B1	2009-10-25	2013-03-12	Dynamics Inc.	Games, prizes, and entertainment for powered cards and devices
JP2011150561A *	2010-01-25	2011-08-04	Toshiba Corp	Portable electronic device and portable electronic device control method
JP5866302B2	2010-02-16	2016-02-17	ダイナミックス インコーポレイテッド	System and method for drive circuit of dynamic magnetic stripe communication device
US8348172B1	2010-03-02	2013-01-08	Dynamics Inc.	Systems and methods for detection mechanisms for magnetic cards and devices
US10693263B1	2010-03-16	2020-06-23	Dynamics Inc.	Systems and methods for audio connectors for powered cards and devices
JP2013533532A	2010-05-18	2013-08-22	ダイナミックス インコーポレイテッド	System and method for cards and devices communicating via light pulse and touch sensitive display
US8226001B1	2010-06-23	2012-07-24	Fiteq, Inc.	Method for broadcasting a magnetic stripe data packet from an electronic smart card
US8317103B1	2010-06-23	2012-11-27	FiTeq	Method for broadcasting a magnetic stripe data packet from an electronic smart card
USD687094S1	2010-07-02	2013-07-30	Dynamics Inc.	Multiple button interactive electronic card with light sources
USD652075S1	2010-07-02	2012-01-10	Dynamics Inc.	Multiple button interactive electronic card
USD652867S1	2010-07-02	2012-01-24	Dynamics Inc.	Multiple button interactive electronic card
USD674013S1	2010-07-02	2013-01-08	Dynamics Inc.	Multiple button interactive electronic card with light sources
USD652449S1	2010-07-02	2012-01-17	Dynamics Inc.	Multiple button interactive electronic card

IPR2025-00645 Page 01766

USD670759S1	2010-07-02	2012-11-13	Dynamics Inc.	Multiple button interactive electronic card with light sources
USD672389S1	2010-07-02	2012-12-11	Dynamics Inc.	Multiple button interactive electronic card with light sources
USD652448S1	2010-07-02	2012-01-17	Dynamics Inc.	Multiple button interactive electronic card
USD665022S1	2010-07-09	2012-08-07	Dynamics Inc.	Multiple button interactive electronic card with light source
USD792511S1	2010-07-09	2017-07-18	Dynamics Inc.	Display with font
USD666241S1	2010-07-09	2012-08-28	Dynamics Inc.	Multiple button interactive electronic card with light source
USD651237S1	2010-07-09	2011-12-27	Dynamics Inc.	Interactive electronic card with display
USD651238S1	2010-07-09	2011-12-27	Dynamics Inc.	Interactive electronic card with display
USD652076S1	2010-07-09	2012-01-10	Dynamics Inc.	Multiple button interactive electronic card with display
USD653288S1	2010-07-09	2012-01-31	Dynamics Inc.	Multiple button interactive electronic card
USD651644S1	2010-07-09	2012-01-03	Dynamics Inc.	Interactive electronic card with display
USD792512S1	2010-07-09	2017-07-18	Dynamics Inc.	Display with font
USD643063S1	2010-07-09	2011-08-09	Dynamics Inc.	Interactive electronic card with display
USD792513S1	2010-07-09	2017-07-18	Dynamics Inc.	Display with font
USD652450S1	2010-07-09	2012-01-17	Dynamics Inc.	Multiple button interactive electronic card
USD665447S1	2010-07-09	2012-08-14	Dynamics Inc.	Multiple button interactive electronic card with light source and display
US8322623B1	2010-07-26	2012-12-04	Dynamics Inc.	Systems and methods for advanced card printing
KR20120011974A *	2010-07-29	2012-02-09	삼성전자주식회사	Smart card supporting plurality of interfaces and interfacing method thereof
US10055614B1	2010-08-12	2018-08-21	Dynamics Inc.	Systems and methods for advanced detection mechanisms for magnetic cards and devices
US9053398B1	2010-08-12	2015-06-09	Dynamics Inc.	Passive detection mechanisms for magnetic cards and devices
US8485443B2	2010-08-31	2013-07-16	Dell Products L.P.	Apparatus and method for sensing an integrated circuit card
US10022884B1	2010-10-15	2018-07-17	Dynamics Inc.	Systems and methods for alignment techniques for magnetic cards and devices
US8561894B1	2010-10-20	2013-10-22	Dynamics Inc.	Powered cards and devices designed, programmed, and deployed from a kiosk
US9646240B1	2010-11-05	2017-05-09	Dynamics Inc.	Locking features for powered cards and devices
EP2469484A1 *	2010-12-22	2012-06-27	Gemalto SA	Smartcard receiving device for providing a remote communication with switching means
US8567679B1	2011-01-23	2013-10-29	Dynamics Inc.	Cards and devices with embedded holograms
US10095970B1	2011-01-31	2018-10-09	Dynamics Inc.	Cards including anti-skimming devices
US9818125B2	2011-02-16	2017-11-14	Dynamics Inc.	Systems and methods for information exchange mechanisms for powered cards and devices
US9836680B1	2011-03-03	2017-12-05	Dynamics Inc.	Systems and methods for advanced communication mechanisms for magnetic cards and devices
US8485446B1	2011-03-28	2013-07-16	Dynamics Inc.	Shielded magnetic stripe for magnetic cards and devices
CA2835508A1	2011-05-10	2012-11-15	Dynamics Inc.	Systems, devices, and methods for mobile payment acceptance, mobile authorizations, mobile wallets, and contactless communication mechanisms
USD670331S1	2011-05-12	2012-11-06	Dynamics Inc.	Interactive display card
USD670329S1	2011-05-12	2012-11-06	Dynamics Inc.	Interactive display card
USD670332S1	2011-05-12	2012-11-06	Dynamics Inc.	Interactive card
USD676904S1	2011-05-12	2013-02-26	Dynamics Inc.	Interactive display card
USD670330S1	2011-05-12	2012-11-06	Dynamics Inc.	Interactive card
US8628022B1	2011-05-23	2014-01-14	Dynamics Inc.	Systems and methods for sensor mechanisms for magnetic cards and devices
US8827153B1	2011-07-18	2014-09-09	Dynamics Inc.	Systems and methods for waveform generation for dynamic magnetic stripe communications devices

US20130181048A1 *	2011-07-19	2013-07-18	University Of Pittsburgh-Of The Commonwealth System Of Higher Education	Method and apparatus for storing and tracking information relating to a medical implant device
US8960545B1	2011-11-21	2015-02-24	Dynamics Inc.	Data modification for magnetic cards and devices
US9619741B1	2011-11-21	2017-04-11	Dynamics Inc.	Systems and methods for synchronization mechanisms for magnetic cards and devices
EP2600287A1 *	2011-12-01	2013-06-05	Gemalto SA	Electronic device including elements managed by various standardised protocols and method for managing communication between said elements
US9064194B1	2012-02-03	2015-06-23	Dynamics Inc.	Systems and methods for spike suppression for dynamic magnetic stripe communications devices
US9710745B1	2012-02-09	2017-07-18	Dynamics Inc.	Systems and methods for automated assembly of dynamic magnetic stripe communications devices
US8888009B1	2012-02-14	2014-11-18	Dynamics Inc.	Systems and methods for extended stripe mechanisms for magnetic cards and devices
US9916992B2	2012-02-20	2018-03-13	Dynamics Inc.	Systems and methods for flexible components for powered cards and devices
US9734669B1	2012-04-02	2017-08-15	Dynamics Inc.	Cards, devices, systems, and methods for advanced payment game of skill and game of chance functionality
US9033218B1	2012-05-15	2015-05-19	Dynamics Inc.	Cards, devices, systems, methods and dynamic security codes
US9064195B2	2012-06-29	2015-06-23	Dynamics Inc.	Multiple layer card circuit boards
USD673606S1	2012-08-27	2013-01-01	Dynamics Inc.	Interactive electronic card with display and buttons
US8828870S1	2012-08-27	2018-09-18	Dynamics Inc.	Display card
USD687487S1	2012-08-27	2013-08-06	Dynamics Inc.	Interactive electronic card with display and button
USD692053S1	2012-08-27	2013-10-22	Dynamics Inc.	Interactive electronic card with display and button
USD729871S1	2012-08-27	2015-05-19	Dynamics Inc.	Interactive electronic card with display and buttons
USD687488S1	2012-08-27	2013-08-06	Dynamics Inc.	Interactive electronic card with buttons
USD729869S1	2012-08-27	2015-05-19	Dynamics Inc.	Interactive electronic card with display and button
USD688744S1	2012-08-27	2013-08-27	Dynamics Inc.	Interactive electronic card with display and button
USD687095S1	2012-08-27	2013-07-30	Dynamics Inc.	Interactive electronic card with buttons
US0729870S1	2012-08-27	2015-05-19	Dynamics Inc.	Interactive electronic card with display and button
USD694322S1	2012-08-27	2013-11-26	Dynamics Inc.	Interactive electronic card with display buttons
USD687490S1	2012-08-27	2013-08-06	Dynamics Inc.	Interactive electronic card with display and button
USD676487S1	2012-08-27	2013-02-19	Dynamics Inc.	Interactive electronic card with display and buttons
USD687489S1	2012-08-27	2013-08-06	Dynamics Inc.	Interactive electronic card with buttons
USD687887S1	2012-08-27	2013-08-13	Dynamics Inc.	Interactive electronic card with buttons
USD730438S1	2012-08-27	2015-05-26	Dynamics Inc.	Interactive electronic card with display and button
USD695636S1	2012-08-27	2013-12-17	Dynamics Inc.	Interactive electronic card with display and buttons
US0730439S1	2012-08-27	2015-05-26	Dynamics Inc.	Interactive electronic card with buttons
USD675256S1	2012-08-27	2013-01-29	Dynamics Inc.	Interactive electronic card with display and button
US9514067B2	2012-08-31	2016-12-06	Nxp B.V.	Interface arbitration for a wired tag
US9053248B2	2012-08-31	2015-06-09	Nxp B.V.	SRAM handshake
US11126997B1	2012-10-02	2021-09-21	Dynamics Inc.	Cards, devices, systems, and methods for a fulfillment system
NO20121197A1 *	2012-10-16	2014-04-17	Sinvent As	Tracer particle for monitoring processes in at least one fluid phase, as well as methods and applications thereof
US9010647B2	2012-10-29	2015-04-21	Dynamics Inc.	Multiple sensor detector systems and detection methods of magnetic cards and devices
US9659246B1	2012-11-05	2017-05-23	Dynamics Inc.	Dynamic magnetic stripe communications device with beveled magnetic material for magnetic cards and devices

IPR2025-00645 Page 01768

US9010644B1	2012-11-30	2015-04-21	Dynamics Inc.	Dynamic magnetic stripe communications device with stepped magnetic material for magnetic cards and devices
US10949627B2	2012-12-20	2021-03-16	Dynamics Inc.	Systems and methods for non-time smearing detection mechanisms for magnetic cards and devices
USD765173S1	2013-03-04	2016-08-30	Dynamics Inc.	Interactive electronic card with display and button
USD765167S1	2013-03-04	2016-02-23	Dynamics Inc.	Interactive electronic card with buttons
USD765174S1	2013-03-04	2016-08-30	Dynamics Inc.	Interactive electronic card with button
USD751609S1	2013-03-04	2016-03-15	Dynamics Inc.	Interactive electronic card with display and button
USD777252S1	2013-03-04	2017-01-24	Dynamics Inc.	Interactive electronic card with buttons
USD751640S1	2013-03-04	2016-03-15	Dynamics Inc.	Interactive electronic card with display and button
USD750168S1	2013-03-04	2016-02-23	Dynamics Inc.	Interactive electronic card with display and button
USD764584S1	2013-03-04	2016-08-23	Dynamics Inc.	Interactive electronic card with buttons
USD750166S1	2013-03-04	2016-02-23	Dynamics Inc.	Interactive electronic card with display and buttons
WO2014145673A1 *	2013-03-15	2014-09-18	Mastercard International Incorporated	Methods and apparatus for providing and operating an enhanced payment display card with network support
USD767024S1	2013-09-10	2016-09-20	Dynamics Inc.	Interactive electronic card with contact connector
USD773737S1	2013-09-10	2016-08-25	Dynamics Inc.	Interactive electronic card with contact connector
KR101694520B1 *	2013-11-26	2017-01-10	한국전자통신연구원	Loop antenna and method for switching thereof
US10108891B1	2014-03-21	2018-10-23	Dynamics Inc.	Exchange coupled amorphous ribbons for electronic stripes
US10032049B2	2016-02-23	2018-07-24	Dynamics Inc.	Magnetic cards and devices for motorized readers
US11010652B2 *	2019-05-09	2021-05-18	Capital One Services, Llc	Orientationless chip layout for a transaction card

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
IL119943A	2000-11-21	Contact/contactless data transaction card
GB2307379B	1999-09-29	Non-contact type information card
AU6455999A	2000-05-15	Portable smart card reader and transaction system
GB2345370B	2000-08-23	Data reader
GB9722551D0	1997-12-24	Card reader
EP0878775A4	2001-07-04	Capacitive data card and reader thereof
GB9306805D0	1993-05-26	Smart card reader
AU4382997A	1998-04-02	Multiple tickets on smart cards
HK1022028A1	2000-07-21	Contactless chip card
GB2319375B	2000-09-06	Card reader
EP0724226A3	1997-08-06	IC card reader/writer
AU1345185	1998-07-31	Card reader
AU5520699A	2000-03-27	Smart card reader
HU9904025A3	2000-05-29	Transaction card
SG41952A1	1997-08-15	Smart card reader
AU5342798A	1998-08-07	Non-contact ic card
AU138868S	1999-11-22	Data card reader
GB9621438D0	1996-12-04	Improved card reader/writer

IPR2025-00645 Page 01769

ZA9764388	1998-02-19	Magnetic card reader.
TW520781U	2003-02-11	Information card
AU7303698A	1998-06-10	Smart card reader
GB2328787B	1997-12-16	Smart card
HRP980237A2	1997-02-28	Credit card reader
AU9081898A	1999-04-05	Smart card reader
AU1345615	1998-07-31	Card reader

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
IL11994396A	1996-12-31	1996-12-31	Contact/contactless data transaction card

Applications Claiming Priority (10)

Application	Filing date	Title
IL11994396A	1996-12-31	Contact/contactless data transaction card
ES97949085T	1997-12-29	DEVICE FOR DATA TRANSACTIONS THAT HAS OPERATING MODES WITH CONTACT AND WITHOUT CONTACT.
CA 2276132	1997-12-29	Data transaction device having contact and contactless modes of operation
EP19970949085	1997-12-29	Data transaction device having contact and contactless modes of operation
AT97949085T	1997-12-29	DATA EXCHANGE DEVICE WITH CONTACT AND CONTACTless MODE
DE1997621335	1997-12-29	DATA EXCHANGE DEVICE WITH CONTACT AND CONTACTless OPERATING MODE
AU78930/98A	1997-12-29	Data transaction device having contact and contactless modes of operation
PCT/IL1997/000436	1997-12-29	Data transaction device having contact and contactless modes of operation
US09/001,240	1997-12-30	Contact/contactless data transaction card
HK00108372A	2000-12-22	Data transaction device having contact and contactless modes of operation

Legal Events

Date	Code	Title	Description
2001-04-30	FF	Patent granted	
2001-07-24	KB	Patent renewed	
2003-04-10	KB	Patent renewed	
2007-02-12	KB	Patent renewed	
2010-12-30	KB	Patent renewed	
2014-11-30	KB	Patent renewed	
2017-07-31	EXP	Patent expired	

Data provided by IFI CLAIMS Patent Services

Patents WO1996026500

A magnetic stripe card simulation means, system and method

Abstract

A magnetic stripe card simulation means or 'test card' comprises a planar substrate component of a similar size to a magnetic stripe card and one or more small electrical coils carried by the test card such that the coil will be positioned adjacent the read head of a magnetic stripe card reader unit when the test card is inserted into the reader unit. The coils are energised to simulate the changing magnetic field at the read head created by movement of a magnetic stripe card past the read head. The system is useful by software developers in development of software for apparatus operated by magnetic stripe cards.

Classifications

» G06K19/06206 Record carriers for use with machines and with at least a part designed to carry digital markings characterised by the kind of the digital marking, e.g. shape, nature, code with magnetically detectable marking the magnetic marking being emulated

View 1 more classifications

WO1996026500A1
WIPO (PCT)

Download PDF Find Prior Art Similar

Other languages: French

Inventor: Garry Peek

Worldwide applications

1996 WO AU

Application PCT/NZ1996/000002 events

1995-02-21 Priority to NZ270883395

1995-02-21 Priority to NZ270883

1996-01-11 Application filed by Garry Peek

1996-08-29 Publication of WO1996026500A1

Info: Patent citations (5), Cited by (13), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, PatentScope, Discuss

Claims

Hide Dependent

1. A magnetic stripe card simulation means comprising a planar substrate component of a similar size to a magnetic stripe card, at least one electrical coil carried by the substrate component such that the coil will be positioned adjacent the read head of a magnetic stripe card reader unit when the substrate component is inserted into the reader

unit, and conductors from the substrate component enabling passing of a series of electrical pulses through the coil to simulate the changing magnetic field at the read head created by

movement of a magnetic stripe card past the read head.

2. A magnetic stripe card simulation means according to claim 1 , wherein the electrical coil(s) is/are sealed in a shallow recess or recesses in the substrate component.

3. A magnetic stripe card simulation means according to either one of claims 1 and 2 comprising two or more coils and wherein each coil is wound such that the magnetic field produced when an electrical pulse is passed through the coil is substantially cancelled on

either side of the coil in the plane of the substrate component to minimise adjacent channel crosstalk.

4. A magnetic stripe card simulation means according to any one of claims 1 to 3, wherein the or each coil(s) is/are wound around a U-shaped core oriented so that the two arms of the core lie above and below each other perpendicular to the plane of the substrate

component.

5. A magnetic stripe card simulation system, comprising:

at least one electrical coil positionable adjacent a read head, and

programmable test means connectable to said electrical coil and programmable to pass a series of electrical pulses through the coil to simulate the changing magnetic field

at the read head created by movement of a magnetic stripe card past the read head.

6. A magnetic stripe card simulation system according to claim 5, wherein the electrical coil(s) is are carried by a substrate component of a similar size to a magnetic

stripe card such that the coil(s) will be positioned adjacent the read head of a magnetic stripe card reader unit when the substrate component is inserted into the reader unit.

7. A magnetic stripe card simulation system according to claim 6, wherein the coil(s) is/are sealed in a shallow recess or recesses in the substrate component.

8. A magnetic stripe card simulation system according to either one of claims 6 and 7 comprising two or more coils and wherein each coil is wound such that the magnetic field produced when an electrical pulse is passed through the coil is substantially cancelled on either side of the coil in the plane of the substrate component to minimise adjacent channel

crosstalk.

IPR2025-00645 Page 01771

9. A magnetic stripe card simulation system according to any one of claims 5 to 8, wherein the or each coil(s) is/are wound around a U-shaped core oriented so that the two arms of the core lie above and below each other perpendicular to the plane of the substrate component.

10. A magnetic stripe card simulation system according to any one of claims 5 to 9, wherein said programmable test means is programmed to energise the coil(s) in a test regime comprising any one or more of:

a) causing the electrical pulses to simulate stored card data representative of data of actual magnetic stripe cards,

b) faster and slower series of electrical pulses representing stored card data to simulate faster and slower card movement past the read head,

c) introduction of sub-integral and/or adjacent bit-to-bit jitter into the electrical pulses representing stored card data for test purposes,

d) variations in the number of leading and trailing clock pulses in the electrical pulses simulating stored card data, and

e) variations of the amplitude of the electrical pulses to vary the magnetic field strength produced by the coil(s), for test purposes.

11. A magnetic stripe card simulation system according to any one of claims 5 to 10, wherein the programmable test means is a personal computer.

12. A method of simulation of movement of a magnetic stripe card past a read head, comprising providing at least one electrical coil positioned adjacent the read head, and passing a series of electrical pulses through the coil to simulate the changing magnetic field created by movement of a magnetic stripe card past the read head.

13. A method according to claim 12, wherein said read head is the read head of a magnetic stripe card reader unit and the electrical coil(s) is/are carried by a substrate component of a similar size to a magnetic stripe card such that the coil(s) will be positioned adjacent the read head when the substrate component is inserted into the reader unit.

14. A method according to either one of claims 12 and 13 including energising said coil in a test regime comprising any one or more of:

a) causing the electrical pulses to simulate stored card data representative of a real magnetic stripe card,

b) faster and slower series of electrical pulses representing stored card data to simulate faster and slower card movement past the read head,

c) introduction of sub-integral and adjacent bit-to-bit jitter into the electrical

pulses representing stored card data for test purposes,

d) variations in the number of leading and trailing clock pulses in the electrical pulses simulating stored card data, and e) variations of the amplitude of the electrical pulses to vary the magnetic field strength produced by the coil(s), for test purposes.

15. A magnetic stripe card simulation means substantially as described herein with reference to Figs 3 and 4 of the accompanying drawings.

16. A magnetic stripe card simulation system substantially as described herein.

17. A method of simulating movement of a magnetic stripe card past a read head substantially as described herein.

Description

A MAGNETIC STRIPE CARD SIMULATION MEANS, SYSTEM & METHOD

FIELD OF INVENTION

The invention comprises a magnetic stripe card simulation means, system and method useful by software developers in development of software for apparatus operated by magnetic stripe cards and incorporating a magnetic stripe card reader unit, such as retail point of sale units, apparatus used in security applications, automatic teller machines or ATMs and other applications in banking and finance or similar, and useful in testing the performance or developing of such magnetic card reader units.

BACKGROUND

Magnetic stripe cards are now in everyday use. Retailers including oil companies issue cards to their customers as credit cards or preferred customer cards or similar. Banks and financial institutions issue such cards to their customers as credit cards, debit cards and cards enabling use of ATMs. Magstripe cards are also commonly used as security cards issued to persons to allow access to buildings and similar. Inevitably the use of magstripe cards in various applications will increase.

A magstripe card is typically a planar plastic card comprising a strip of magnetic media which acts as a store for data. International standards define the physical size of the card and the size and characteristics of the magnetic stripe. These standards allow for up to

three tracks to be defined along the length of the magnetic stripe, each for storing data which may be programmed onto the card on issue of the card to the user by the card issuing authority. Typically track 1 is a read only track used to carry the customers name and account information in banking or retail applications for example. Typically track 2 is a read only track carrying data which identifies the card type, the customers account number, any personal identification number or PIN and other issuer specific data. Typically

track 3 is designated a read/write track and can carry rewritable data such as customer account balances. The physical position of each track on the card is closely defined by international standards.

Magnetic card reader units generally comprise 1, 2 or 3 adjacent pick-up coils mounted in a read head assembly. The read head is mounted in the reader unit such that the coils are centered where the encoded tracks 1 , 2 and 3 of a magnetic stripe card inserted into the reader will be positioned. The magnetically encoded card is passed over the read head either by a motorised transport mechanism of the reader unit or by a manual card swipe. Card guides ensure correct location of the magnetic media over the read head. As the encoded card moves past the read head, the magnetic lines of force emanating from the magnetic media of the card induce a current in the pick-up coils. This current is amplified and processed by decoding circuits to recover stored data. Tracks 1 , 2 and 3 can be read simultaneously if all are used.

IPR2025-00645 Page 01772

Each application which uses magnetic stripe card technology requires software to be produced for that application. For example, each time a retailer converts to use of magcard technology, software must be developed for use in the associated point of sale terminals of the retailer. The same is true for other magcard users such as individual banks and financial institutions, and in security card applications where magcards are used as access cards. Various aspects of the software development require simulation of the end use of the cards. For example, in testing new software it may be necessary to trial various card

encodings, to test the system response to expired cards, to trial a range of account codes, PINs, purchase restrictions and similar. At present this is commonly carried out by encoding a number of cards with each parameter to be tested and manually swiping a card through a reader unit during the software development.

SUMMARY OF INVENTION

The present invention provides a magnetic stripe card simulation means, system and method suitable for use by developers of software for magcard applications such as those referred to above, for testing the performance of and in the development of magcard reader units, and in other related applications.

In broad terms in one aspect the invention comprises a magnetic stripe card simulation means or "test card", comprising a planar substrate component of a similar size to a magnetic stripe card, at least one electrical coil carried by the substrate component such that the coil will be positioned adjacent the read head of a magnetic stripe card reader unit when the substrate component is inserted into the reader unit, and conductors from the substrate component enabling passing of a series of electrical pulses through the coil to simulate the changing magnetic field at the read head created by movement of a magnetic stripe card past the read head.

In broad terms in another aspect the invention comprises a magnetic stripe card simulation

system, comprising: at least one electrical coil positionable adjacent a read head, and

programmable test means connectable to said electrical coil and programmable to pass a series of electrical pulses through the coil to simulate the changing magnetic field at the read head created by movement of a magnetic stripe card past the read head.

Preferably the electrical coil(s) is/are carried by a substrate component of a similar size to a magnetic stripe card such that the coil(s) will be positioned adjacent the read head of a

magnetic stripe card reader unit when the substrate component is inserted into the reader unit.

In broad terms in a further aspect the invention comprises a method of simulation of movement of a magnetic stripe card past a read head, comprising providing at least one electrical coil positioned adjacent the read head, and passing a series of electrical pulses through the coil to simulate the changing magnetic field at the read head created by movement of a magnetic stripe card past the read head.

DESCRIPTION OF DRAWINGS

The invention will be further described with reference to the accompanying drawings, by way of example and without intending to be limiting, wherein:

Figure 1 schematically illustrates use of a magnetic card simulation system in software

development using a personal computer, Figure 2 shows a typical magnetic stripe card from one side showing the approximate position of the three data tracks,

Figure 3 shows a preferred form magnetic stripe card simulation means or test card of the

invention,

Figure 4 shows one preferred coil design,

Figure 5 shows positioning of a test card adjacent the read head of a magstripe card reader unit when the test card is inserted into the reader unit, and

Figure 6 schematically shows the interaction between the coil(s) of a test card of the invention and the pickup coil of a magcard read head.

DETAILED DESCRIPTION OF PREFERRED FORMS

Typically, but not exclusively, the test card and simulation system of the invention will be used with a personal computer used by a software developer or similar. Figure 1 schematically shows a personal computer 1 and a magstripe card reader unit 2. The test card 3 is inserted into the reader unit as shown, and a small cable 4 connects

the test card to a port of the computer via a standard plug 5, so that test software in the personal computer may energise the test card to simulate swiping of a standard magstripe card

through the reader unit. Figure 2 shows a standard magnetic stripe card. The card typically comprises a substrate 6 of standard dimensions and thickness, carrying a stripe 7 of magnetic media again in a standard position on the card. The magnetic media 7 provides three tracks in accordance with international standards, for storing data on the card. Tracks 1 , 2 and 3 are indicated at T1, T2 and T3 in Figure 2.

As stated previously, track 1 is typically used as a read only track to carry a customers name and account information. Track 2 is typically used as a read only track most often used by the banking and oil industries. On track 2 the first six digits after the start sentinel are termed the card prefix and identify the card type e.g. Visa, Mastercard, Fuelcard, Debitcard, etc. The next digits give the customers account number. Together the prefix and account number make up the Primary Account Number or PAN. A separator designates the end of the PAN which may vary between 13 and 19 digits in length. The PAN separator is usually followed by the card expiry date, a PIN offset plus other issuer specific data. Track 3 is designated a read/write track and can carry rewritable data such as customer account balances (but is generally not used).

Various applications use different tracks. For example, a security access system may use only track 1 for encoding access privileges, a banking application such as EFTPOS may use only track 2 for customer account identification, and an oil industry application may use both tracks 1 and 2 using track 1 for account information and track 2 for product purchase restrictions. While three tracks are provided for by international standards at present, it is possible in the future that a larger number of tracks may be provided on a magnetic stripe card such as 4 or 5 tracks, and it is also possible that the data tracks may be located at other positions on the card than shown in Figure 2.

Figure 3 shows a preferred form magnetic stripe card simulation means or "test card". The test card comprises a substrate component 10 which is typically a piece of plastic or other suitable material of the same or similar dimensions to those of a standard magnetic stripe card. Where the magnetic stripe cards of a particular system do not comply with the international standards because the cards are for use with an in-house system of the card issuer who desires that the cards are of a non-standard size or that the data track(s) are in

a non-standard location, the test card will also be of a non-standard size for use with the particular reader units used. Instead of a magnetic stripe, three small electrical

IPR2025-00645 Page 01773

coils 1 1 are carried by the substrate component 10. The coils 11 are positioned on the substrate component 10 such that they will in turn be positioned adjacent the read head of a standard magcard reader unit when the test card is inserted into the unit, as shown in Figure 1.

Figure 5 shows how the small coils 11 are positioned on the substrate component 10 such that when the test card is inserted into the reader unit the coils 11 will be positioned

immediately adjacent the read head 12.

In the preferred form test card shown each coil 11 is mounted in a shallow recess 13 formed in the thickness of the substrate component 10 forming the test card. For example the recesses 13 may be formed using a router. A shallow channel 14 is provided from the recesses 13 to an edge of the test card and wires pass from the coils 1 1 along the channel 14 to connect to a cable 15 the other end of which carries a plug for connecting the test card to the port of a personal computer for example. The coils 11 may be secured in position in the recesses 13 as well as protected, by a resin or filler compound which also covers the wires in the channel 14. Optionally the whole surface of the card may then be covered with an adhesive film or similar. One, two or three coils may be provided depending upon the application and the number of tracks used, and it is also possible that four or more adjacent coils 1 1 or similar could be carried by the test card for some particular non-standard application.

The coils 11 may be small coils of any suitable configuration but in the preferred form each coil is wound such that the magnetic field generated when an electrical pulse is passed through the coil is substantially cancelled on either side of the coil in the plane of the test card to avoid detection of the magnetic field created by the coil by another read head pick up coil i.e. to avoid adjacent channel crosstalk. In the preferred form this is achieved as shown in Figure 4, by winding each coil 1 1 in two parts around the legs of a U-shaped core 17, the ends of which are subsequently crimped together, so that when the coil is energised a magnetic flux will radiate predominantly in directions perpendicular to the plane of the card as indicated by arrows F in Figure 4. Figure 4 shows the coil before crimping of the ends of the legs of the core together. The core 17 may be formed from permalloy sheet or other suitable coil material or alternatively the coils may be air cored. Use of a magnetic coil material increases the field strength generated Various other coil constructions are possible however

As stated, when the test card is inserted into a reader unit, the coils 11 are positioned

adjacent the read head as shown in Figure 5. A series of electrical pulses may then be sent through each coil 1 1 to be picked up by the read head to create a changing magnetic field at the read head which simulates movement of a magnetic stripe card past the read head. Energising the coil or coils 1 1 with a series of pulses will simulate movement of a magstripe card comprising a number of stored data digits past the read head. Figure 6 shows the interaction of a test card coil 1 1 with a pickup coil 19 of the read head.

The driving current to the coils may be supplied directly from a parallel or serial port of the PC. Current limiting resistors may be provided, in the port adaptors for example, to restrict the current flow through the coils. Variable resistors may be inserted into the current path to allow adjustment of the magnetic field strength of each of the coils. Other electronic circuits may be included to limit or boost the driving current, modify its wave

shape or buffer the signal. A microprocessor may be included to remove some of the processing load and time dependency from the PC.

More than one test card may be operated from the designated system port. Additional cards may be connected to the same port using appropriate adaptors and each card may be individually driven by the PC. Additional cards may be wired together in series or in parallel to operate simultaneously.

Associated software generates the pulse stream which energises the coils of the test card to simulate swiping or motorised movement of a magnetic stripe card. In the design and development of magnetic card readers and decoders the software may be arranged to energise the test card to simulate faster and slower or maximum and minimum swipe speeds, in both directions, to introduce and vary sub-integral and/or adjacent bit to bit jitter in the test signal, to vary the number of leading and trailing clock pulses, and to vary the magnetic field strength for example. In the development of software applications based around magnetically encoded cards various card encodings can be quickly and easily simulated to check the response of the application software during development, such as purchase limitations, expiry dates, security access levels, invalid check characters, and similar. Test cards can be stored in a card data base for easy access. In production and test centre testing of card based systems test scrips using a data base of cards can be repeatedly played. A single PC can connect to many cards simulating multiple simultaneous swipes or to test maximum system load. The swipes can be triggered from an external event to synchronise the next swipe to the availability of the card reader. The ability to simulate a card avoids having to encode real magnetic cards for each and every combination of card type.

While in the preferred form test card the coils 11 or similar are carried by a substrate component of a size the same as or similar to a standard mag stripe card, it is possible in other forms that the coils may be carried by other means enabling the coils to be placed adjacent the read head of a card reader, such as a smaller substrate strip which may be inserted into a card reader or other means insertable into a card reader to position the coils adjacent the read head.

The foregoing describes the invention including a preferred form thereof. Alterations and modifications as will be obvious to those skilled in the art are intended to be incorporated within the scope hereof, as defined in the accompanying claims.

Patent Citations (5)

Publication number	Priority date	Publication date	Assignee	Title
US4701601A *	1985-04-26	1987-10-20	Visa International Service Association	Transaction card with magnetic stripe emulator
US4786791A *	1987-02-10	1988-11-22	Gateway Technology	Data processing apparatus with portable card having magnetic strip simulator
US4791283A *	1986-06-03	1988-12-13	Intellicard International, Inc.	Transaction card magnetic stripe emulator
US4818853A *	1986-05-26	1989-04-04	Kabushiki Kaisha Toshiba	Data card with inductive signal transfer device
EP0554830A1 *	1992-02-03	1993-08-11	Angewandte Digital Elektronik GmbH	Plastic card with electronic simulation of a magnetic strip

Family To Family Citations

* Cited by examiner, † Cited by third party

Cited By (13)

Publication number	Priority date	Publication date	Assignee	Title
WO2006091709A2 *	2005-02-22	2006-08-31	Tyfone, Inc.	Electronic transaction card
WO2007011937A2 *	2005-07-18	2007-01-25	Tyfone, Inc.	Electronic stripe cards
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US8231061B2	2009-02-24	2012-07-31	Tyfone, Inc	Contactless device with miniaturized antenna
US8814055B2	2008-08-08	2014-08-26	Tyfone, Inc.	Mobile payment device with small inductive device powered by a host device
US8866614B2	2008-08-08	2014-10-21	Tyfone, Inc.	Active circuit for RFID
CN104240724A *	2014-09-24	2014-12-24	福建联迪商用设备有限公司	Method and device for magnetic head testing
WO2016041055A1 *	2014-09-17	2016-03-24	Dashpass Inc.	An enabling card and method and system using the enabling card in a pos
US9619796B2	2014-09-17	2017-04-11	Dashpass Inc.	Enabling card and method and system using the enabling card in a P.O.S
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US10074888B2	2015-04-03	2018-09-11	NXT-ID, Inc	Accordion antenna structure
US10970709B2	2009-02-10	2021-04-06	4361423 Canada Inc.	Apparatus and method for commercial transactions using a communication device
US11144900B2	2014-09-17	2021-10-12	Dashpass Inc.	Enabling card and method and system using the enabling card in a POS

Family To Family Citations

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US5359183A	1994-10-25	Payment card with display
WO1996026500A1	1996-08-29	A magnetic stripe card simulation means, system and method
US5336871A	1994-08-09	Holographic enhancement of card security
US7938318B2	2011-05-10	System and method for controlling secured transaction using directionally coded account identifiers
EP0428233B1	1993-09-22	Method and apparatus for producing admission tickets
US4791283A	1988-12-13	Transaction card magnetic stripe emulator
US6402029B1	2002-06-11	Method and apparatus for combining data for multiple magnetic stripe cards or other sources
US20050279825A1	2005-12-22	Transaction card packaging
US4228348A	1980-10-14	Security document and system
KR19990036269A	1999-05-25	Security credit card
EP0579206A2	1994-01-19	Checking objects to be checked for authenticity and a method and an apparatus for checking the authenticity of the objects
JPH0780384B2	1995-08-30	Prepaid cards and methods of preventing their unauthorized use
US4639584A	1987-01-27	Non-alterable magnetic coding
JPH08202842A	1996-08-09	Magnetic card or the like
US4101905A	1978-07-18	Method for writing and viewing magnetic human readable characters and viewing means therefor
GB2027965A	1980-02-27	Improvements in or relating to metering devices
JPH08194786A	1996-07-30	Prepaid card unauthorized use preventing system in pinball saloon
US20080135631A1	2008-06-12	Multiple card product with multiple data strips
JP2553770B2	1996-11-13	Card and card processing device
JP3322729B2	2002-09-09	Method and apparatus for determining authenticity of an object to be detected

JP2550313B2	1996-11-06	Information processing method for purchasing prizes exchanged for pachinko balls
JP2550174B2	1996-11-06	Magnetic card
JP2695482B2	1997-12-24	Card processing equipment
JPH0832781B2	1996-03-21	Similar product discriminating device for cash prize
JP3566542B2	2004-09-15	Magnetic card

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
NZ270533		1995-02-21	
NZ270533		1995-02-21	

Applications Claiming Priority (1)

Application	Filing date	Title
AU44982/96A	1996-01-11	A magnetic stripe card simulation means, system and method

Legal Events

Date	Code	Title	Description
1996-08-29	AK	Designated states	**Kind code of ref document:** A1 **Designated state(s):** AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN AZ BY KZ RU TJ TM
1996-08-29	AL	Designated countries for regional patents	**Kind code of ref document:** A1 **Designated state(s):** KE LS MW SD SZ UG AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN
1996-10-24	DFPE	Request for preliminary examination filed prior to expiration of 19th month from priority date (pct application filed before 20040101)	
1996-11-27	121	Ep: the epo has been informed by wipo that ep was designated in this application	
1998-01-02	REG	Reference to national code	**Ref country code:** DE **Ref legal event code:** 8642
1998-06-17	122	Ep: pct application non-entry in european phase	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents MX2007000546

Contactless payment card reader with a frusto-conical operating volume.

Abstract

A contactless payment card reader has a frusto-conical operating volume. Thefrusto-conical shaped operating volume has defined magnetic field strengthsfor powering and communicating with proximity payment cards. The reader canserve as a reference reader, which is representative of product readers deployedin contactless payment card systems, to test product contactless payment cardsunder conditions that simulate field use of the cards.

Classifications

» G06K5/00 Methods or arrangements for verifying the correctness of markings on a record carrier; Column detection devices

View 16 more classifications

MX2007000546A

Mexico

Find Prior Art Similar

Other languages: Spanish

Inventor: Patrik Smets, Eddy Lodewijk Hortensia Velde, Duncan Garrett

Worldwide applications

2005 MX KR JP US CN AU BR CR KR WO CN WO EP KR US CN AU CA AU CA JP KR EP CA US AU CA WO JP EP EP BR MX JP MX MX CA WO MX KR CN US AU US WO BR JP EP BR CN 2007 IL IL IL IL IL ZA ZA ZA ZA 2008 US

Application MX2007000546A events

2004-07-15 Priority to US58827004P

2005-07-15 Application filed by Mastercard International Inc

2005-07-15 Priority to PCT/US2005/025110

2007-03-30 Publication of MX2007000546A

Info: Patent citations (58), Cited by (158), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (13)

Hide Dependent

1. CLAIMS 1. A reader arrangement for reading contactless payment cards, the reader consists of: an RF antenna circuit; and a landing plane positioned at a fixed distance from the RF antenna, where the RF antenna circuit is configured to generate a magnetic field Hov in a frustoconically operating volume, where the landing plane forms the base of smaller diameter of the operating volume in a frusto-conical manner, and in which the magnetic field Hov in the operating volume in a frusto-conical manner is specified to feed and communicate with the contactless payment cards placed in the operating volume in a frusto-conical manner. 2. The reader array of claim 1, characterized in that the frusto-conically operating volume consists of: a truncated cone having an axial length Si, a smaller base diameter DI and a diameter of the large base D2; and a cylindrical section having a diameter D2 and an axial length S23. The reader array of claim 2, characterized in that the RF antenna has a diameter of about 7 cm, wherein the landing plane is positioned at a fixed distance of about 15 cm from the RF antenna, and where the parameters Si, S2, DI and D2 have nominal values of approximately 1, 3, 3 and 5 cm, respectively. 4. The reader array of claim 1, characterized in that the magnetic field H0 corresponds to a power transfer voltage Vov measured at a point on the circuit of the RF antenna, and wherein the Vov measured in the antenna circuit of RF has a nominal value of approximately 3-az volts in an RF antenna circuit, where z is the distance of a payment card from the landing plane in cm, and where a is equal to approximately 0.35. 5. A reference reader for testing a contactless payment card that can be used with any of the different card readers deployed in an electronic payment system, the reference reader comprises: an RF antenna circuit whose external behavior is representative of the behavior of the different readers deployed in the electronic payment system, where the circuit of the RF antenna is configured to present the representative external behavior for the non-contact payment card under test and to generate a magnetic field Hov in a volume operationally frustoconical, where the magnetic field Ho in the operating volume in a frustoconical manner is specified to feed and communicate with the contactless payment card placed in the operating volume in a frustoconical manner. 6. The reference card of claim 5, characterized in that the different readers are contactless payment card readers and wherein the circuit of the RF antenna comprises an antenna having a resonant frequency of about 13.56 MHz. 7. The reference reader of claim 6, characterized in that the RF antenna is a circular antenna fabricated on a circuit board, and wherein the reference reader further comprises a landing plate on which the cards are placed for testing and which they are placed at a fixed distance of approximately 15 cm away from the printed circuit board. 8. The reference reader of claim 7, characterized in that the antenna is a circular antenna having a diameter of approximately 7 cm representing an average of the antenna sizes of the different readers deployed in the field and generating a magnetic field that is representative of the readers deployed in the field. 9. The reference reader of claim 8, characterized in that the frustoconical operating volume consists of: a truncated cone having an axial length Si, a diameter of the small base DI and a diameter of the large base D2; a cylindrical section having a diameter D2 and a length S2. 10. The reference reader of claim 9, characterized in that the landing plane is placed at a fixed distance of approximately 15 cm from the RF antenna, and wherein the parameters Si, S2, Di, and D2 have nominal values of approximately 1, 3, 3 and 5 cm, respectively. 11. The reference reader of claim 10, characterized in that the magnetic field Hov corresponds to an equivalent energy transfer voltage Vov measured at a point on the circuit of the RF antenna, and where the Vov measured in the antenna circuit RF has a nominal value of approximately (3-az) volts, where z is the distance of the payment card from the landing plane in cm, and where a equals 0.35. 12. A method for testing the behavior of a contactless payment card that can be used with any of the different card readers deployed in an electronic payment system, the method comprises the steps of: having a reference reader having an operational volume frustoconically, the reference reader contains an RF antenna circuit whose external behavior is representative of the behavior of the different readers deployed in the electronic payment system, where the circuit of the RF antenna is configured to present the representative external behavior for the payment card to be tested and to generate a Hov magnetic field in the operating volume in a frusto-conical manner, and in which the magnetic field Hov in the operating volume in a frusto-

IPR2025-00645 Page 01778

conical manner is specified to feed and communicate with the contactless payment card when it is placed in the operating volume in a frustoconical way; place the contactless payment card in a first position in the operating volume in a frustoconical way; and measure the reception of the data and the sensitivity of the energy of the contactless card placed in the operating volume. 13. The method of claim 12 further comprises: placing the contactless payment card in a series of positions in the operating volume in a frusto-conical manner; and measuring the reception of the data and the energy sensitivity of the product card in each of the series of positions in the operating volume in a frustoconical manner.

Description

NON-CONTACT PAYMENT CARD READER WITH FRUSTOCONIC OPERATING VOLUME SPECIFICATION CROSS REFERENCE TO RELATED APPLICATIONS This application claims the benefit of United States Provisional Patent Application 60 / 588,279, filed July 15, 2004. This application also relates to United States patent applications S / N, and S / N, S / N, and S / N, filed on the same date, all of which claim the benefit before the aforementioned Patent Application NO. 60 / 588,270. All of the aforementioned patent applications are hereby incorporated by reference in their entirety.

BACKGROUND OF THE INVENTION Radio Frequency Identification Labels (RFID) are small integrated circuits (IC) connected to an antenna, which can respond to a signal from Questionable RF with simple identification information, or with more complex signals, depending on the size of the IC, RFID technology does not require contact or visual line for communication. Radio Frequency Identification (RFID) technology is now economically viable and is deployed in more and more commercial and industrial applications. For example, RFID technology is now widely used for identification tags on items in warehouses, stores, ID or access cards, among others. In addition, RFID technology has been introduced in the payment card industry (such as Master Card, American Express and Visa) in the form of "contactless" credit or payment cards embedded with RFID tags. These contactless payment cards can be used to make electronic payment transactions through radio communication with an RFID-enabled payment terminal. Contactless payment cards can provide consumers with simple, fast and convenient ways to pay for products and services, for example in retail establishments, warehouses or super markets.

Some RFID technologies are available for use in contactless payment cards and card readers / terminals. The main components of a non-contact system are the contactless reader (or Coupler Device operating in Proximity).

(PCD)) and a transponder. The contactless reader is an antenna that is connected to an electronic circuit. A transponder consists of an inductive antenna and an integrated circuit connected to the ends of this antenna. The reader-transponder combination behaves like a transformer. An alternating current passes through a primary coil (the reader antenna) that creates an electromagnetic field, which induces a current in the secondary coil (the transponder antenna). The transponder converts the electromagnetic field (or RF field) transmitted by the non-contact reader (PCD) to a DC voltage by means of a diode rectifier. This DC voltage feeds the transponder's internal circuits. The configuration and tuning of both antennas determines the coupling efficiency of one device to the other. The transponders can be contactless payment cards.

For contactless payment card systems to be economically viable and to obtain commercial acceptance, contactless payment cards must be interoperable on all or most payment terminals enabled with RFID, even when the cards and terminals have features technology that are owned by suppliers / issuers, vendors or manufacturers of specific card terminals. Interoperability is convenient throughout the industry. To this end, organizations and standards groups for the industry (for example the International Organization for Standardization (ISO) and the International Electrotechnical Committee (IEC) have formulated voluntary standards for the industry to implement contactless payment technologies. Three of these exemplary standards that have been defined by the ISO / IEC are the I? O / IEC 10536, ISO / IEC 14443 and ISO / IEC 15693, standards applicable to close coupling cards, operating in proximity and neighborhood, respectively.

The standards of the cards that operate in the vicinity of ISO / IEC 14443 (ISO 14113) have been used for various contactless card deployments throughout the world. The range of operations chosen for cards operating in proximity to ISO 14443 is up to 10 cm, although this range varies depending on the energy requirements, memory size, CPU and coprocessor.

The document of ISO 14443 standards has four different parts.

• Part 1: Physical Characteristics, defines the physical dimensions for an Integrated Circuit Card that operates in proximity (PICC). The card is ID-1 size (85.6 mm x 54.0 mm x 0.76 mm). This is the same size as a bank credit card.

• Part 2: Radio Frequency Energy and Signal Interface, defines the important technical characteristics of the non-contact IC chips, including aspects such as frequency, data rate, modulation and Bits coding procedures. In part 2, two variations are detailed, the type A interface and the type B interface. Both operate on the same frequency and use the same data rate, but differ in the areas of modulation and bit coding.

• Part 3: initialization and anti-collision, the initialization describes the requirements for the coupler device operating in proximity (PCD) (ie the reader) and the card to establish communication when the card is taken to the radio frequency (RF) field of the reader. Anti-collision defines what happens when multiple cards enter the magnetic field at the same time, identifying how the system determines which card to use in the transaction and ensuring that all cards presented are inventoried and processed.

• Part 4: transmission protocols, defines the form of data and data elements that enable communication during a transaction.

For a payment card system and contactless card readers to comply with ISO 14443, they must meet the requirements of at least some of the parts of the voluntary standard. In addition to contactless technologies that are standardized in accordance with ISO 14443, various patented non-contact interfaces are also used in the industry (eg Cubil's GO-Card and Sony's FeliCa card). With deployments of existing card technology, interoperability can be a problem. Card readers deployed by vendors in the market should preferably house several different types of cards. For example, a desirable card reader would support type A and type B cards of ISO 14443, ISO 15693 cards and some type of additional patented card.

interoperability problems can arise even with deployments of cards that are supposed to comply with a single ISO standard (for example ISO 14443). In ISO 14443, all requirements or specifications related to RF energy and signal interfaces in the contactless card and reader system (ie, the physical layer in an Open System Interconnection (OSI) model view) of a system) are defined using independent standardized tests for the cards and for the readers. Part 6 (ISO 10373-6) of the ISO / IEC 10373 standard dealing with analytical methods, which are specific to non-contact integrated circuit card technology (cards that operate in proximity). The compliance of cards and readers without contact with ISO 14443 is verified using the reference devices. In accordance with ISO 10373-6, a series of "reference" cards (ie, reference PICC), which represents the characteristics of the cards in contact, is used to measure compliance with the specification of a non-contact reader . (See for example Figure Ia). For example, the reference PICC is used to test the magnetic field produced or transmitted by a PCD, and to test the ability of the PCD to feed a PICC. Similarly, a "reference" reader (ie, a test or reference PCD), which can represent the characteristics of a typical contactless reader, is used to measure compliance with the specification of contactless cards. For example, the reference PCD in conjunction with a pair of external sensing coils is used to test the modulation of the charge generated by the cards during testing.

IPR2025-00645 Page 01779

While the independent procedures of card and reader compliance testing in accordance with ISO 10373-6 can guarantee that the deployed product devices each have features that fall within the specifications ranges designed for cards and readers, the procedures do not guarantee interoperability in the field. The cards and / or readers verified as compliant can only be arginally so (for example by having a characteristic value at the end or the limit of a designated range of specifications). This form of compliance with standards can lead to operational failures in the field. For example, a card that meets marginally may be non-readable or difficult to read using a card reader that only marginally meets as well.

In addition, with respect to the verification of the transmission and reception of important data from non-contact device functions, ISO 10373-6 makes provision for only indirect measurements of the data signals with modulated load generated by the cards. A PCD test assembly prescribed by ISO 10373-6 to test product cards has a pair of sensing coils that are external to the reference PCD reader. These external sensing coils are used to measure the data signal with modulated load generated and transmitted by the card under test. However, there is no direct or obvious relationship between the modulated charge signal measured by the sensing coils and the signal that is physically received by the reference PCD antenna. Therefore, testing the data transmission functions of a product card using the external sensing coils provides direct assurance that a product card modulation that is putatively compliant with the ISO of the data signals is sufficient or compatible with the ability of a product reader to receive or process appropriately modulated data signals.

Patent applications US N / S, N / S, and N / S, describe solutions to improve the interoperability of devices based on improvements in the definitions of the specifications, the reference equipment and the compliance tests related to the RF energy and the signal interface between the card interacting devices and reader.

Other ways to improve the interoperability of electronic payment devices are now being taken into account and also to make the operation of robust and fail-safe electronic contactless payment systems. Attention is now being directed to aspects of electronic payment systems related to the physical characteristics and dimensions of contactless payment devices.

COMPENDIUM OF THE INVENTION A contactless card reader has a "frusto-conical" operative volume that is configured as a cylinder that reduces its section to a truncated cone. An RF antenna circuit generates electromagnetic RF operation fields for power and communication with the payment cards placed in the frustoconical operating volume. The RF antenna, which is adjusted to approximately mi3.56 MHz, is placed about 15 cm below a covered plate, which serves as a landing plane for the reader. The smaller diameter base of the frustoconical operating volume rests on the landing plane. The operational RF fields (ie, the near-field magnetic fields Hov generated by the RF antenna in the operating volume in a frusto-conical manner are specified to feed and communicate with non-contact payment cards of different origin that can be placed in the operating volume in a frustoconical way.

In one version of the reader, the RF antenna has a diameter of approximately 7 cm and is placed at a fixed distance of approximately 15 cm below the landing plane. The frustoconical portion of the frustoconical operating volume has an axial length of about 1 cm, a small base diameter of about 1 cm and a large base diameter of about 3 c. The cylindrical portion of the frustoconical operating volume cylinder portion has a diameter of approximately 3 cm and an axial length of approximately 5 cm, respectively.

The reader with the frustoconical operating volume can be configured with a reference reader whose external behavior is representative of the behavior of the different readers deployed in an electronic payment system. The circuit of the RF antenna is configured to generate a magnetic field Hov in a frustoconical operating volume that is representative of the magnetic fields of operating volume of the different readers deployed in the electronic payment system. The reference reader can be used in an analysis procedure to characterize the functional or operational behavior of the payment cards. During a test procedure, the reception of the data and the sensitivity of the energy of the payment card placed in the frustoconical operating volume are measured. The payment card under test is placed in different orientations and in a different position in the frustoconical operating volume to simulate the use of the card field.

Other characteristics of the invention, its nature and the different advantages will be more evident from the accompanying drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS Figure 1 is a demonstration of a frustoconical or truncated cone geometry of the minimum operational volume of an exemplary reader designed in accordance with the principles of the present invention.

Figure 2 is an image of an exemplary Pa Pass reference reader designed in accordance with the principles of the present invention.

Figure 3 is an image of an exemplary PayPass reference card designed in accordance with the principles of the present invention.

Figure 4 is a demonstration of a cover plate serving as a landing plane for the PayPass reference reader of Figure 2.

Figure 5 is a demonstration of a series of geometry positions in which a particular payment card is placed in the frusconic operating volume of the PayPass reference reader to simulate the use of the payment card field in a card-testing procedure in accordance with the principles of the present invention.

DETAILED DESCRIPTION OF THE INVENTION The present invention provides an arrangement of the card reader that has a frusto-conical operating volume. The operating volume in a frusto-conical manner has defined intensities of the magnetic field that are appropriate for robust and consistent interactions with the payment cards operating by proximity presented or placed in the operating volume. Figure 1 shows an example of a frustoconical operating volume definition for a reader.

The reader array can be used as a reference device to test compliance with the specifications of the product payment cards. As an example, the PayPass reference reader (Figure 2), which is described in the United States patent application N / S, can be designed to have an operational volume in a frustoconical to evaluate or observe the behaviors and efficiency of the payment cards.

The arrangement of the inventive reader is described herein in the context of implementations of electronic payment systems in which the specifications of the contactless payment device are intended to conform to a common industry standard, such as ISO 11443. , which also specifies standardized test methods (ie, ISO 103373-6 test methods, cards that operate in proximity) for the verification of the specification of individual non-contact payment devices. In recent times, the international Master Card transferee ("Master Card") has developed the patented specifications Master Card Pay-Pass ™ ISO / IEC 14443 implementation specification ("PayPass") for the implementation of payment card technologies that they operate in proximity (for example by issuers, vendors or manufacturers of cards or card readers). The PayPass implementation is in accordance with ISO 14443 and provides a convenient example that shows the principles of the present invention. It will be understood that the selection of the PayPass implementation for purposes of illustration herein is but one example, and that the principles of the present invention may be applied more generally to electronic payment devices and systems operating under other industry standards, common or property.

With reference to Figure 2, the PayPass reference reader includes an RF antenna 200 which is designed to resonate at 13.56 MHz. The antenna of the reader 200 is printed on a circuit board 210 which is placed at a certain distance from below. a covered plate 400 (Figure 4). The cover plate 400 can serve as a landing plane, that is, a reader surface, in which a cardholder can place his payment card for processing. In field use, the cover plate 400 may have appropriate guide marks or logos that can visually direct a holder to the positions chosen for the placement of his payment card for the processing of the transactions.

A landing plane defines the base of the inverted frustoconical operating volume with the axis of the frustoconical operating volume being generally normal to the surface of the landing plane. The antenna of the reader has a circular shape, and generates magnetic fields that are usually cylindrically symmetrical around the normal plane of

IPR2025-00645 Page 01780

landing. The size and windings of the reader antenna can be properly designed using the known design principles of RF antennas to generate operational magnetic fields (Hov) at 13.56 MHz for activation with payment card devices operating in the vicinity. The intensities of the Hov are in a specific range at least within the inverted frustroconical operating volume. The specified range is selected taking into account that the payment cards displayed in the field, which can be manufactured by different issuers or sellers of cards for different specifications, can show a range of behaviors. For example, inductive coupling antennas or RFID tags on cards that operate in the vicinity issued by different vendors may have different sizes and shapes. The specified range of the magnetic field strengths in the frustoconical operating volume is selected to obtain adequate energy to activate and communicate with a range of interacting payment cards of different origin and behaviors.

The frustoconical operating volume is defined by the geometric parameters (for example, the diameters of the base DI and D2, and the axial length of the SI cone and the axial cylindrical length S2) shown in Figure 1). Table I lists the nominal values of these selected parameters for an exemplary definition of the frustoconical operating volume for the PayPass reference reader of Figure 2.

TABLE 1 Volume DI 3 cms operative D2 5 cms dimensions SI 1 cm S2 3 cms In the exemplary PayPass reference reader, the reader antenna has a diameter of approximately 7 cm and is placed approximately 15 cm below the landing plane. The antenna has dual activity and dummy or simulated windings that when they are food with electric currents, provide at least a minimum field strength Hmin needed to feed and communicate with a payment card that is placed within the specified frustroconomic operating volume. At the same time, the operational magnetic fields (Hov) generated by the antenna are restricted to remain below a certain maximum intensity Hmax. The value of Hmax is appropriately selected to limit energy dissipation in payment cards to thresholds below those commonly accepted to avoid damage to the device. Likewise, the magnetic field strengths inside and outside the operating volume are limited to comply with all international and national regulations and laws related to safe use and exposure limits for such radiations.

The operating volume of the exemplary PayPass reference reader can be characterized or calibrated using an appropriate reference card, for example, a PayPass reference card (Figure 3), which is also described in the co-pending US patent application No. Operating magnetic fields (Hov) in the frustoconical operating volume can be specified or measured in equivalent terms of the required energy transfer (Vov voltage) from the reader to a payment card.

Table II shows a specification of the minimum and maximum values for the Vov energy transfer voltages in the frusconical operating volume of the PayPass reference reader. Electromagnetic coupling (ie, mutual inductance) between the card and the reader's antennas disturbs the operational magnetic fields when a card is brought to the operating volume. In particular, the magnetic field strength within the operating volume decreases due to the additional load caused by the card. The Vov values for the reader and 1 card can be measured at appropriate definition points in the reference reader and antenna circuits of the reference card, respectively. The charge of a card can be measured by observing a circuit voltage drop? Vov (Vov, air-free) at an appropriate point in the antenna circuit of the PayPass reference reader. Table II also shows a maximum acceptable value of? Vov corresponding to a nominal charge of the card.

TABLE II Topic Parameter PCD Nom. Max. PICC Non. Max. Units min min. Transfer VOT 3-az 8.5 2.8-az 8.7 V power PCD? PICC _a 0.35 0.35 V / cm? Vo ^ pat C 8 V The arrangement of the inventive reader (eg, the PayPass reference reader) having a defined frustoconical operating volume can be used in conjunction with the systems and methods described in the co-pending US patent application N / S for testing the product payment cards, for example, to verify compliance with specifications. An exemplary procedure to verify compliance with the specifications of a product card may include the following steps: (a) measure the transmission of the data by the product card in the reference reader PayPass, with the reader sending "average" value instructions to the product card and with the PayPass reference reader providing an "average" energy level. The energy level and characteristics of the instructions produced by the PayPass reference reader are calibrated with respect to a reference card, and (b) measuring the data reception and energy sensitivity of the product card under test using the PayPass reference reader.

During operation a signal of ± 600 mW can be fed to the input impedance of 50 O of the reader input to generate a magnetic field, which is representative of most PayPass readers deployed in the field. The product cards can be characterized under conditions that simulate the conditions of use of the card in the field. For example, the behavior of a product card can be characterized or measured at different distances from and in different orientations in relation to the reader antenna. In an exemplary test routine, the reader is held in a stationary position and the target product card moves slowly through the operating volume from one test position to the next for the measurements. Figure 5 shows a series of these test positions that are used in the exemplary test routine. The series of test positions is distributed along a three-dimensional space of the frustoconical operating volume. The test positions are shown as quadruplet coordinates (r, f, z,?) In Figure 5, where the polar coordinates r, f and z represent the center of the product card under test. With reference to Figure 1, (r, f, z) = (0,0,0) represents the center of the landing plane. In the exemplary testing routine, all measurements on the object product card are made with the card held perpendicular to the z-axis. the z coordinate represents the height of the payment card from the landing plane. The coordinate? represents the orientation of the card in relation to the axis f = 0. While the present invention has been described particularly with reference to the exemplary embodiments thereof, those skilled in the art will understand that various modifications and alterations can be made without departing from the spirit. and scope of the invention. Accordingly, the described embodiments of the invention are considered only demonstrative, and the invention is limited in scope only as specified in the appended claims.

Patent Citations (58)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US4066873A	1976-01-26	1978-01-03	The First National Bank Of Chicago	Identification and access card with associated optical decoding means
JPS61201390A	1985-03-04	1986-09-06	Casio Comput Co Ltd	Ic card
FR2586428B1 *	1985-08-26	1988-11-25	Pasteur Institut	POLYPEPTIDES AND ANTIBODIES, CHARACTERISTICS OF PAPILLOMAVIRUS AND THEIR APPLICATIONS TO IN VITRO DIAGNOSIS, PREVENTION AND / OR CONTROL OF PAPILLOMAVIRUS INFECTIONS
US5880452A *	1990-11-15	1999-03-09	Geo Labs, Inc.	Laser based PCMCIA data collection system with automatic triggering for portable applications and method of use
US5225977A *	1991-03-18	1993-07-06	Hooper John B	Card payment system for service dispensing devices
GB9105851D0	1991-03-20	1991-05-08	Security Systems Consortium Th	Securing financial transactions
US5466919A *	1993-04-02	1995-11-14	Hovakimian; Henry	Credit/charge card system enabling purchasers to contribute to selected charities

US5511111A *	1993-11-01	1996-04-23	Engineering And Business Systems, Inc.	Caller name and identification communication system with caller screening option
US5623552A	1994-01-21	1997-04-22	Cardguard International, Inc.	Self-authenticating identification card with fingerprint identification
US5511114A *	1994-06-06	1996-04-23	Call Processing, Inc.	Telephone pre-paid calling card system and method
US5602744A *	1994-09-29	1997-02-11	Meek, Jean L.	Universal send/receive utility usage data gathering system
JPH08123919A *	1994-10-28	1996-05-17	Mitsubishi Electric Corp	Noncontact ic card system and communication method thereof
US5748737A *	1994-11-14	1998-05-05	Daggar; Robert N.	Multimedia electronic wallet with generic card
US5625628A *	1995-03-15	1997-04-29	Hughes Electronics	Aloha optimization
US6010074A *	1996-04-01	2000-01-04	Cubic Corporation	Contactless proximity automated data collection system and method with collision resolution
US6486813B1 *	1996-07-30	2002-10-15	Micron Technology, Inc.	Radio frequency data communications device with adjustable receiver sensitivity and method
DE19635311A1 *	1996-09-02	1998-03-12	Angewandte Digital Elektronik	Adaptive identification of contactless chip cards
US6150955A *	1996-10-28	2000-11-21	Tracy Corporation Ii	Apparatus and method for transmitting data via a digital control channel of a digital wireless network
GB2319698B *	1996-11-21	2001-08-08	Motorola Inc	Method for communicating with a plurality of contactless data carriers and contactless data carrier for use therein
US6119940A *	1997-02-18	2000-09-19	Unisys Corporation	Identification methods
US6112981A	1997-02-25	2000-09-05	Dresser Industries, Inc.	Bar code reader for a fuel dispenser
GB9719583D0	1997-09-16	1997-11-19	Ncr Int Inc	A method of authenticating a magnetic card
US6810304B1	1997-09-26	2004-10-26	Gilbarco Inc.	Multistage ordering system for a fueling and retail environment
US6134309A *	1997-09-30	2000-10-17	Creative Games International, Inc.	Pre-paid phone card system with promotional link
US6061344A *	1998-02-19	2000-05-09	Micron Technology, Inc.	Method of addressing messages and communications system
US6072801A *	1998-02-19	2000-06-06	Micron Technology, Inc.	Method of addressing messages, method of establishing wireless communications, and communications system
US6315195B1 *	1998-04-17	2001-11-13	Diebold, Incorporated	Transaction apparatus and method
US6710701B2	1998-04-22	2004-03-23	Gilbarco Inc.	Rfid tag location using tag or host interaction record
DE19830526A1 *	1998-07-08	2000-01-13	Orga Kartensysteme Gmbh	Method and device for controlling communication between a terminal and a number of chip cards
US6297789B2 *	1998-07-09	2001-10-02	Tyco Electronics Corporation	Integrated circuit card with liquid crystal display for viewing at least a portion of the information stored in the card
US6640643B1 *	1998-10-15	2002-06-11	Amerasia International Technology, Inc.	Article having an embedded electronic device, and method of making same
US6557729B1 *	1999-06-10	2003-06-10	Cubic Corporation	Multiple protocol smart card communication device
JP3824451B2 *	1999-07-29	2006-09-20	富士通株式会社	Non-contact IC card presence / absence detection circuit
AU6674000A *	1999-08-11	2001-03-13	Mark Iv Industries Limited	Method and means for rf toll collection
JP2001076117A	1999-08-31	2001-03-23	Toppan Forms Co Ltd	Advantageous card
US6145742A *	1999-09-03	2000-11-14	Drexler Technology Corporation	Method and system for laser writing microscopic data spots on cards and labels readable with a CCD array
US6394346B1 *	1999-10-07	2002-05-28	Cubic Corporation	Contactless smart card high production encoding machine
WO2001031555A1 *	1999-10-28	2001-05-03	Gould David B	Prepaid cash equivalent card and system
DE10055602A1	1999-12-30	2001-07-12	Ibm	Exit control system for supermarket or department store, produces receipt based on contactlessly received information and updates payment status
FR2809251B1 *	2000-05-17	2003-08-15	St Microelectronics Sa	DEVICE FOR PRODUCING AN ELECTROMAGNETIC FIELD FOR A TRANSPONDER
KR100486758B1 *	2000-08-31	2005-05-03	매그나칩 반도체 유한회사	Radio Frequency Identification Tag System for preventing collision and collision preventing method thereof

AU9260001A	2000-09-08	2002-03-22	American Express Travel Relate	A system and method for loyalty program distribution and settlement
FR2815490B1 *	2000-10-16	2006-07-07	Inside Technologies	CONTACTLESS INTEGRATED CIRCUIT READER
US7253717B2 *	2000-11-29	2007-08-07	Mobile Technics Llc	Method and system for communicating with and tracking RFID transponders
JP2002351685A *	2001-05-22	2002-12-06	Sankyo Seiki Mfg Co Ltd	Data updating method and controller for nonvolatile memory
US7889052B2	2001-07-10	2011-02-15	Xatra Fund Mx, Llc	Authorizing payment subsequent to RF transactions
US6666982B2	2001-10-22	2003-12-23	Tokyo Electron Limited	Protection of dielectric window in inductively coupled plasma generation
JP2003162755A	2001-11-27	2003-06-06	Great Information Kk	Prepaid card information issuing system, call tariff settling system, and value settling system
US7011250B2 *	2001-12-20	2006-03-14	Matsushita Electric Industrial Co., Ltd.	IC card reader/writer, identification method and program
US7792759B2 *	2002-07-29	2010-09-07	Emv Co. Llc	Methods for performing transactions in a wireless environment
KR100560770B1 *	2003-09-15	2006-03-13	삼성전자주식회사	Contactless integrated circuit card with real-time protocol switching function and card system including the same
US20050222961A1 *	2004-04-05	2005-10-06	Philippe Staib	System and method of facilitating contactless payment transactions across different payment systems using a common mobile device acting as a stored value device
MX2007000546A *	2004-07-15	2007-03-30	Mastercard International Inc	Contactless payment card reader with a frusto-conical operating volume.
US7692532B2 *	2004-07-30	2010-04-06	Reva Systems Corporation	Interference monitoring in an RFID system
KR101059872B1 *	2005-01-03	2011-08-29	삼성전자주식회사	Communication collision prevention protocol using unique identifier
US7274284B2 *	2005-02-04	2007-09-25	Atmel Corporation	Method for RF card detection in a contactless system
US20060273176A1 *	2005-06-03	2006-12-07	Actividentity, Inc.	Blocking contactless personal security device
JP4584082B2 *	2005-09-05	2010-11-17	ソニー・エリクソン・モバイルコミュニケーションズ株式会社	Reader / writer and communication method

* Cited by examiner, † Cited by third party

Cited By (158)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
MX2007000546A *	2004-07-15	2007-03-30	Mastercard International Inc	Contactless payment card reader with a frusto-conical operating volume
WO2006069330A2	2004-12-20	2006-06-29	Proxense, Llc	Biometric personal data key (pdk) authentication
KR101059872B1 *	2005-01-03	2011-08-29	삼성전자주식회사	Communication collision prevention protocol using unique identifier
US7506813B2 *	2005-01-06	2009-03-24	Quad/Graphics, Inc.	Resonator use in the print field
FR2881007B1 *	2005-01-19	2007-02-23	Gemplus Sa	ESTABLISHING COMMUNICATION BETWEEN NON-CONTACT DEVICES
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
CN102968604B *	2005-09-28	2016-06-15	维萨国际服务协会	Reduce the equipment of the interaction time of contactless transaction, system and method
US8988436B2 *	2006-01-18	2015-03-24	Symbol Technologies, Inc.	Peer-to-peer radio frequency communications for management of RFID readers
US8412949B2	2006-05-05	2013-04-02	Proxense, Llc	Personal digital key initialization and registration for secure transactions
US9401063B2 *	2006-06-08	2016-07-26	Mastercard International Incorporated	All-in-one proximity payment device with local authentication
US7958291B2 *	2006-10-10	2011-06-07	Atmel Rousset S.A.S.	Supplemental communication interface

EP2156367B1 *	2006-10-12	2011-11-23	Nxp B.V.	Device, system and method for compensating signal delays in an rfid communication system
US9269221B2	2006-11-13	2016-02-23	John J. Gobbi	Configuration of interfaces for a location detection system and application
US8281998B2	2006-12-07	2012-10-09	Smart Systems Innovations, Llc	Public transit system fare processor for transfers
US8763900B2	2006-12-07	2014-07-01	Smart Systems Innovations, Llc	Mass transit fare processing system
US7991156B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
CN101617330A *	2006-12-19	2009-12-30	迅城有限公司	The transaction system of in authorising cashless transactions, using
US8052055B2 *	2007-01-31	2011-11-08	Hewlett-Packard Development Company, L.P.	Method and system for perturbing multi-radio-frequency-identification-tag-reader networks to increase interrogation efficiency
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US7844568B2 *	2007-05-09	2010-12-07	Atmel Rousset S.A.S.	Managing power and timing in a smart card device
WO2009006635A1 *	2007-07-05	2009-01-08	Mastercard International Incorporated	Method and system for detecting a signal generated by a proximity-based transaction device
US9038914B2 *	2007-07-05	2015-05-26	Mastercard International Corporation	Method and system for simulating a proximity-based transaction device
JP4977543B2	2007-07-20	2012-07-18	日本電気通信システム株式会社	Control device, control system, control method, and control program
JP5260908B2	2007-07-20	2013-08-14	日本電気通信システム株式会社	Control device, communication device, control system, control method, and control program
US20090070691A1 *	2007-09-12	2009-03-12	Devicefidelity, Inc.	Presenting web pages through mobile host devices
US8659427B2	2007-11-09	2014-02-25	Proxense, Llc	Proximity-sensor supporting multiple application services
JP4420296B2 *	2007-11-19	2010-02-24	フェリカネットワークス株式会社	Information processing apparatus, information processing method, and program
US8171528B1	2007-12-06	2012-05-01	Proxense, Llc	Hybrid device having a personal digital key and receiver-decoder circuit and methods of use
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US9251332B2 *	2007-12-19	2016-02-02	Proxense, Llc	Security system and method for controlling access to computing resources
US8838198B2 *	2008-01-09	2013-02-26	Nxp B.V	Evaluating an electromagnetic field strength of an electromagnetic gate apparatus
WO2009102979A2	2008-02-14	2009-08-20	Proxense, Llc	Proximity-based healthcare management system with automatic access to private information
KR101527368B1 *	2008-03-12	2015-06-09	한국전자통신연구원	RFID reader device for situational command retransmission and control method therefor
KR20090097784A *	2008-03-12	2009-09-16	한국전자통신연구원	Rfid interrogator with a collision diagnostics function and method for controlling of the same
US11120449B2	2008-04-08	2021-09-14	Proxense, Llc	Automated service-based order processing
EP2131313A1	2008-06-02	2009-12-09	Gemplus	Method for selecting an application in a mobile wireless communication device in an NFC system and corresponding mobile wireless communication device
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
KR101039449B1 *	2008-11-25	2011-06-07	엘지엔시스(주)	Method for testing PBPR using a damaged type of financial contract information
CN101739583B *	2008-11-26	2013-04-10	國民技术股份有限公司	Radio frequency SIM card, radio frequency card reader and magnetic induction control method for radio frequency communication
US8630584B2	2008-11-26	2014-01-14	Nationz Technologies Inc.	RF SIM card, card reader, and communication method
DE102009009846A1 *	2009-02-20	2010-09-02	Bundesdruckerei Gmbh	Improved card reader for contactless readable cards and method of operating such a card reader

EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
CN101833378 *	2009-03-11	2014-08-13	中兴通讯股份有限公司	Method and terminal for realizing application selection in non-contact electronic payment
JP5169937B2 *	2009-03-25	2013-03-27	株式会社デンソー	Portable machine
US8485436B2 *	2009-04-06	2013-07-16	Mastercard International Incorporated	Simulated contactless identification card reader
US8135354B2 *	2009-06-02	2012-03-13	Symbol Technologies, Inc	Method and system for chopped antenna impedance measurements with an RFID radio
US20110007843A1 *	2009-07-07	2011-01-13	Broadcom Corporation	Low power fm transmitter
CN102048928 *	2009-08-31	2014-03-26	鸿富锦精密工业（深圳）有限公司	Multi-function card reader testing device and method
SK288555B6 *	2009-11-14	2018-05-02	Smk Corporation	Method and system of data transmission from the transponder to the reader, especially in payment solutions with a mobile communication device
CN101742469B *	2009-11-24	2012-05-30	候万春	System and method for controlling mobile phone RFID non-contact transaction attribution
JP5304615B2 *	2009-11-26	2013-10-02	株式会社デンソーウェーブ	Non-contact communication device
US9418205B2	2010-03-15	2016-08-16	Proxense, Llc	Proximity-based system for automatic application or data access and item tracking
CN102215050B *	2010-04-02	2014-03-19	国民技术股份有限公司	Detection method for radio-frequency SIM (Subscriber Identity Module) card collision with low-frequency magnetic communication
CN102468988A *	2010-11-11	2012-05-23	上海华虹集成电路有限责任公司	Device for automatically detecting signal protocol type in international standardization organization/international electrotechnical commission (ISO/IEC) 14443 protocol
CN102479308B *	2010-11-23	2014-10-08	上海华虹宏力半导体制造有限公司	Radio frequency identification anti-collision circuit and realizing method thereof
FR2968804B1	2010-12-13	2013-01-04	St Microelectronics Rousset	METHOD FOR MANAGING THE DIALOGUE BETWEEN EQUIPMENT AND AT LEAST ONE MULTI-APPLICATION OBJECT SUCH AS A CONTACTLESS CHIP CARD AND CORRESPONDING OBJECT
US9265450B1	2011-02-21	2016-02-23	Proxense, Llc	Proximity-based system for object tracking and automatic application initialization
DE102011103740A1 *	2011-05-31	2012-12-06	Smartrac Ip B.V.	A method and arrangement for providing and managing information associated with RFID media in a network
CN102982294B *	2011-09-05	2015-12-02	国民技术股份有限公司	A kind of collision detection method utilizing magnetic two-way communication
US9022427B2	2012-02-29	2015-04-28	Verifone, Inc.	Point of sale device and method for operating same
CN102622565A *	2012-03-06	2012-08-01	无锡儒安科技有限公司	Processing method and device for detecting and preventing electronic tag collision
US8690412B2 *	2012-03-15	2014-04-08	Apple Inc.	Backlight structures and backlight assemblies for electronic device displays
KR101383566B1 *	2012-09-14	2014-02-17	주식회사 티제텍스	Apparatus and method for generating unique identity of radio frequency
US9852419B2 *	2012-09-17	2017-12-26	Capital One Financial Corporation	Systems and methods for providing near field communications
US9406898B2	2013-05-10	2016-08-02	Proxense, Llc	Secure element as a digital pocket
US9323964B2 *	2013-08-20	2016-04-26	Cubic Corporation	Card detection and selection
US9014323B2 *	2013-08-30	2015-04-21	Nxp B.V.	Clock synchronizer for aligning remote devices
CN104636771A *	2013-11-12	2015-05-20	上海华虹集成电路有限责任公司	Non-contact module testing circuit and method
CA2924701A1 *	2013-11-21	2015-05-28	Jet Medical, Inc.	System for facilitating intranasal guidance
CN103761492A *	2013-12-10	2014-04-30	上海动联信息技术股份有限公司	Method of non-contact device for carrying out operation on multiple cards on the basis of 13.56 MHz working frequency
US10509939B2 *	2014-12-24	2019-12-10	Intel Corporation	Method and apparatus for energy harvest from a proximity coupling device

CN104484636A *	2014-12-31	2015-04-01	深圳市科漫达智能管理科技有限公司	Data reading method and device
EP3082061A1	2015-04-13	2016-10-19	Phitek Systems Limited	Communications system for aircraft
CN105668480B *	2015-08-04	2019-05-07	电子科技大学	Ultrahigh frequency RFID signal scanner
US20170200148A1 *	2016-01-07	2017-07-13	Vantiv, Llc	Point of interaction device emulation for payment transaction simulation
US11188893B2 *	2016-01-15	2021-11-30	Mastercard International Incorporated	Access control bypass on mobile for mass transit
CN106934431B *	2017-02-24	2019-09-13	飞天诚信科技股份有限公司	A kind of method and card reader of testing smart card
CN107403118A *	2017-07-06	2017-11-28	上海动联信息技术股份有限公司	The test suite and method of a kind of card reader
EP3493097B1 *	2017-11-29	2021-03-24	ams AG	Method for supplying energy wirelessly by means of radio frequency identification, rfid, and rfid system
CN108021957B *	2017-12-05	2021-07-23	深圳市艾特智能科技有限公司	Anti-collision method and system, readable storage medium and card reading device
CN108038397B *	2017-12-15	2021-01-01	神思电子技术股份有限公司	Test device and method for read-write timing of RFID reader-writer
CN108288008A *	2018-02-08	2018-07-17	飞天诚信科技股份有限公司	A kind of method and device of card activation
US10546644B2	2018-06-21	2020-01-28	Capital One Services, Llc	Systems and methods for secure read-only authentication
CN109033906A *	2018-07-27	2018-12-18	天津科畅慧通信息技术有限公司	A kind of device and method for testing RFID sensitivity
CA3115142A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10630653B1	2018-10-02	2020-04-21	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10992477B2	2018-10-02	2021-04-27	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
WO2020072550A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10489781B1	2018-10-02	2019-11-26	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
CA3108917A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10733564B2	2018-10-02	2020-08-04	Capital One Services, Llc	Systems and methods for establishing identity for order pick up
US10511443B1	2018-10-02	2019-12-17	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10783519B2	2018-10-02	2020-09-22	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
AU2019355110A1	2018-10-02	2021-04-08	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
AU2019355878A1	2018-10-02	2021-02-25	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
KR20210065961A	2018-10-02	2021-06-04	캐피탈 원 서비시즈, 엘엘씨	System and method for cryptographic authentication of contactless card
WO2020072687A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10771253B2	2018-10-02	2020-09-08	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10607214B1	2018-10-02	2020-03-31	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10505738B1	2018-10-02	2019-12-10	Capital One	Systems and methods for cryptographic authentication of contactless cards

IPR2025-00645 Page 01786

			Services, Llc	
US10582386B1	2018-10-02	2020-03-03	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10565587B1	2018-10-02	2020-02-18	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10579998B1	2018-10-02	2020-03-03	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
KR20210068028A	2018-10-02	2021-06-08	캐피탈 원 서비시즈, 엘엘씨	System and method for cryptographic authentication of contactless card
US10558411B1	2018-10-02	2020-02-04	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
CA3115064A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10592710B1	2018-10-02	2020-03-17	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10581611B1	2018-10-02	2020-03-03	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10841091B2	2018-10-02	2020-11-17	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10949520B2	2018-10-02	2021-03-16	Capital One Services, Llc	Systems and methods for cross coupling risk analytics and one-time-passcodes
US10909527B2	2018-10-02	2021-02-02	Capital One Services, Llc	Systems and methods for performing a reissue of a contactless card
US10542036B1	2018-10-02	2020-01-21	Capital One Services, Llc	Systems and methods for signaling an attack on contactless cards
US10771254B2	2018-10-02	2020-09-08	Capital One Services, Llc	Systems and methods for email-based card activation
KR20200060623A	2018-11-22	2020-06-01	삼성전자주식회사	Operating method of electronic device performing near field communication functions
US11037136B2	2019-01-24	2021-06-15	Capital One Services, Llc	Tap to autofill card data
US10510074B1	2019-02-01	2019-12-17	Capital One Services, Llc	One-tap payment using a contactless card
US10467622B1	2019-02-01	2019-11-05	Capital One Services, Llc	Using on-demand applications to generate virtual numbers for a contactless card to securely autofill forms
US11120453B2	2019-02-01	2021-09-14	Capital One Services, Llc	Tap card to securely generate card data to copy to clipboard
US10425129B1	2019-02-27	2019-09-24	Capital One Services, Llc	Techniques to reduce power consumption in near field communication systems
US10523708B1	2019-03-18	2019-12-31	Capital One Services, Llc	System and method for second factor authentication of customer support calls
US10438437B1	2019-03-20	2019-10-08	Capital One Services, Llc	Tap to copy data to clipboard via NFC
US10535062B1	2019-03-20	2020-01-14	Capital One Services, Llc	Using a contactless card to securely share personal data stored in a blockchain
US10643420B1	2019-03-20	2020-05-05	Capital One Services, Llc	Contextual tapping engine
US10984416B2	2019-03-20	2021-04-20	Capital One Services, Llc	NFC mobile currency transfer
US10970712B2	2019-03-21	2021-04-06	Capital One Services, Llc	Delegated administration of permissions using a contactless card
US10467445B1	2019-03-28	2019-11-05	Capital One Services, Llc	Devices and methods for contactless card alignment with a foldable mobile device
US10515447B1	2019-06-17	2019-12-24	Capital One Services, Llc	Dynamic power levels in NFC card communications
US10871958B1	2019-07-03	2020-12-22	Capital One Services, Llc	Techniques to perform applet programming

US10713649B1	2019-07-09	2020-07-14	Capital One Services, Llc	System and method enabling mobile near-field communication to update display on a payment card
US10498401B1	2019-07-15	2019-12-03	Capital One Services, Llc	System and method for guiding card positioning using phone sensors
US10885514B1	2019-07-15	2021-01-05	Capital One Services, Llc	System and method for using image data to trigger contactless card transactions
US10733601B1	2019-07-17	2020-08-04	Capital One Services, Llc	Body area network facilitated authentication or payment authorization
US11182771B2	2019-07-17	2021-11-23	Capital One Services, Llc	System for value loading onto in-vehicle device
US10832271B1	2019-07-17	2020-11-10	Capital One Services, Llc	Verified reviews using a contactless card
US10506426B1	2019-07-19	2019-12-10	Capital One Services, Llc	Techniques for call authentication
US10541995B1	2019-07-23	2020-01-21	Capital One Services, Llc	First factor contactless card authentication system and method
US10701560B1	2019-10-02	2020-06-30	Capital One Services, Llc	Client device authentication using contactless legacy magnetic stripe data
US10825408B1	2019-12-23	2020-12-08	Capital One Services, Llc	Method for mapping NFC field strength and location on mobile devices
US11113685B2	2019-12-23	2021-09-07	Capital One Services, Llc	Card issuing with restricted virtual numbers
US10733283B1	2019-12-23	2020-08-04	Capital One Services, Llc	Secure password generation and management using NFC and contactless smart cards
FR3105662B1 *	2019-12-23	2021-11-26	St Microelectronics Rousset	Setting up a transaction in an electronic contactless device
US10885410B1	2019-12-23	2021-01-05	Capital One Services, Llc	Generating barcodes utilizing cryptographic techniques
US10657754B1	2019-12-23	2020-05-19	Capital One Services, Llc	Contactless card and personal identification system
US10664941B1	2019-12-24	2020-05-26	Capital One Services, Llc	Steganographic image encoding of biometric template information on a card
US10853795B1	2019-12-24	2020-12-01	Capital One Services, Llc	Secure authentication based on identity data stored in a contactless card
US10757574B1	2019-12-26	2020-08-25	Capital One Services, Llc	Multi-factor authentication providing a credential via a contactless card for secure messaging
US10909544B1	2019-12-26	2021-02-02	Capital One Services, Llc	Accessing and utilizing multiple loyalty point accounts
US11038688B1	2019-12-30	2021-06-15	Capital One Services, Llc	Techniques to control applets for contactless cards
US10860914B1	2019-12-31	2020-12-08	Capital One Services, Llc	Contactless card and method of assembly
US10886006B1	2020-04-30	2020-12-08	Capital One Services, Llc	Systems and methods for data access control using a short-range transceiver
US11030339B1	2020-04-30	2021-06-08	Capital One Services, Llc	Systems and methods for data access control of personal user data using a short-range transceiver
US10915888B1	2020-04-30	2021-02-09	Capital One Services, Llc	Contactless card with multiple rotating security keys
US10963865B1	2020-05-12	2021-03-30	Capital One Services, Llc	Augmented reality card activation experience
US11063979B1	2020-05-18	2021-07-13	Capital One Services, Llc	Enabling communications between applications in a mobile operating system
US11100511B1	2020-05-18	2021-08-24	Capital One Services, Llc	Application-based point of sale system in mobile operating systems
US11062098B1	2020-08-11	2021-07-13	Capital One Services, Llc	Augmented reality information display and interaction via NFC based authentication
US11165586B1	2020-10-30	2021-11-02	Capital One Services, Llc	Call center web-based authentication using a contactless card

IPR2025-00645 Page 01788

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
MX2007000546A	2007-03-30	Contactless payment card reader with a frusto-conical operating volume.
EP1896983B1	2010-07-07	Rfid communication systems and methods
US9038914B2	2015-05-26	Method and system for simulating a proximity-based transaction device
US8442796B2	2013-05-14	Method and system for simulating a proximity-based transaction device
Murfett	2004	The challenge of testing RFID integrated circuits
US20190266457A1	2019-08-29	Rfid screw specifically for use on eyeglass frames
Proffitt II	2013	Experimental investigation to inform optimal configurations for dynamic near-field passive uhf rfid systems

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
US58827004P	2004-07-15	2004-07-15	*US Provisional Application*
PCT/US2005/025110	2004-07-15	2005-07-15	Contactless payment card reader with a frusto-conical operating volume

Legal Events

Date	Code	Title	Description
2013-09-30	FA	Abandonment or withdrawal	

Data provided by IFI CLAIMS Patent Services

Patents ITMI981564

NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY

Classifications

G11C7/00 Arrangements for writing information into, or reading information out from, a digital store

View 2 more classifications

ITMI981564A1
Italy

Find Prior Art Similar

Other languages: Italian

Inventor: Giovanni Campardo

Worldwide applications

1998 IT 1999 EP US

Application IT98MI001564A events

1998-07-09 Application filed by St Microelectronics Srl

1998-07-09 Priority to IT98MI001564A

2000-01-09 Publication of ITMI981564A1

Info: Patent citations (16), Cited by (15), Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (16)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
JPH0738818782 *	1984-03-23	1995-04-26	株式会社日立製作所	Microcomputer configured in LSI
US5444665A *	1985-06-17	1995-08-22	Hitachi, Ltd.	Semiconductor memory device
US5165023A *	1986-12-17	1992-11-17	Massachusetts Institute Of Technology	Parallel processing system with processor array and network communications system for transmitting messages of variable length
US5546343A *	1990-10-18	1996-08-13	Elliott; Duncan G.	Method and apparatus for a single instruction operating multiple processors on a memory chip
US5325500A *	1990-12-14	1994-06-28	Xerox Corporation	Parallel processing units on a substrate, each including a column of memory
JPH04248642A *	1991-01-18	1992-09-04	Kenneth W Iobst	Pim chip for memory integrated circuit and its controlling method
US5687345A *	1992-03-17	1997-11-11	Hitachi, Ltd.	Microcomputer having CPU and built-in flash memory that is rewritable under control of the CPU analyzing a command supplied from an external device
TW231343B *	1992-03-17	1994-10-01	Hitachi Seisakusyo Kk	
JPH06215160A *	1992-08-25	1994-08-05	Texas Instr Inc <Ti>	Method and apparatus for data processing
TW260788B *	1993-09-01	1995-10-21	Philips Electronics Nv	
JPH0845269A *	1994-07-27	1996-02-16	Hitachi Ltd	Semiconductor memory
EP0757356B1 *	1995-07-31	2001-06-06	STMicroelectronics S.r.l.	Flash EEPROM with controlled discharge time of the word lines and source potentials after erase
US6185704B1 *	1997-04-11	2001-02-06	Texas Instruments Incorporated	System signaling schemes for processor and memory module
US6026478A *	1997-08-01	2000-02-15	Micron Technology, Inc.	Split embedded DRAM processor

US6023761A *	1997-08-13	2000-02-08	Visi Technology, Inc.	Method and system for using decompression on compressed software stored in non-volatile memory of an embedded computer system to yield decompressed software including initialized variables for a runtime environment
US6141705A *	1998-06-12	2000-10-31	Microsoft Corporation	System for querying a peripheral device to determine its processing capabilities and then offloading specific processing tasks from a host to the peripheral device when needed

* Cited by examiner, † Cited by third party

Cited By (15)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7350056B2 *	2005-09-27	2008-03-25	International Business Machines Corporation	Method and apparatus for issuing instructions from an issue queue in an information handling system
US20070198812A1 *	2005-09-27	2007-08-23	Ibm Corporation	Method and apparatus for issuing instructions from an issue queue including a main issue queue array and an auxiliary issue queue array in an information handling system
JP4984666B2 *	2006-06-12	2012-07-25	ソニー株式会社	Non-volatile memory
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8543112282	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9177646B2	2013-05-06	2015-11-03	International Business Machines Corporation	Implementing computational memory from content-addressable memory
US9785545B2 *	2013-07-15	2017-10-10	Cnex Labs, Inc.	Method and apparatus for providing dual memory access to non-volatile memory
CN107548492B *	2015-04-30	2021-10-01	密克罗奇普技术公司	Central processing unit with enhanced instruction set
EP3115109A1 *	2015-07-06	2017-01-11	Base4 Innovation Limited	Droplet sequencing device

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
ITMI981564A1	2000-01-09	NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY
DE69810096D1	2003-01-23	Non-volatile memory
DE19880311T1	1999-05-12	Non-volatile memory structure
DE60129025D1	2007-08-02	MEMORY AREA ASSIGNMENT IN A FILE SYSTEM FOR DESCRIPTING ANY AREAS
DE69936028D1	2007-06-21	Non-volatile semiconductor memory
DE69822412T2	2002-05-29	Non-volatile semiconductor memory
FR2770328B1	2001-11-23	REMANENT MEMORY POINT
NO20032188L	2003-07-17	A self-adjusting non-volatile memory cell
DE69814450D1	2003-06-17	Check non-volatile memory
NO20002265L	2000-05-15	Programmable access protection in a temporary memory device
DE10085013T1	2002-10-31	Arranging information stored in non-volatile reprogrammable semiconductor memories

IPR2025-00645 Page 01791

DE19882486T1	2000-06-15	Synchronous, non-volatile page mode memory
AT328375T	2006-06-15	IN A SHAPED CROSS DIPOLANTENNE
DE69431735D1	2002-12-19	Non-volatile memory
AU5314101A	2001-10-15	Page mode erase in a flash memory array
DK101250ZT3	2002-04-15	Grating construction in a fluid bed boiler
DE69700328T2	1999-11-04	Compensate for latency in a memory
FR2771839B1	2000-01-28	PROGRAMMABLE AND ELECTRICALLY ERASABLE NON-VOLATILE MEMORY
DE60043453D1	2010-01-14	DUNG IN A SODAKESSEL
DE60038133D1	2008-04-03	Non-volatile memory
DE59913627D1	2006-08-10	Integrated memory
DE69812038D1	2003-04-17	Non-volatile MOS memory
DE59712601D1	2006-05-11	NON-VOLATILE MEMORY CELL
AT517990T	2011-08-15	EFFECTIVE NUCLEAR PROGRAMMING IN MAMMALS
FR2812753B1	2003-01-03	NON-VOLATILE MEMORY POINT

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
IT98MI001564A	1998-07-09	1998-07-09	NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY

Applications Claiming Priority (3)

Application	Filing date	Title
IT98MI001564A	1998-07-09	NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY
EP19990202169	1999-07-02	Non-volatile memory capable of autonomously executing a program
US09/349,702	1999-07-08	Non-volatile memory capable of autonomously executing a program

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

IPR2025-00645 Page 01792

Patents JP2001167187

Subscription contract mediation method and mobile communication network

Abstract

PROBLEM TO BE SOLVED: To mediate more quickly the subscription contacts of various types of electronic commerce services without forcing the great burden on users. SOLUTION: A credit system comprises a mobile station 100, a mobile telephone network 20, a mobile packet communication network 30, the CAT terminals 40a, 40b..., a CAFIS network 50, the credit servers 60A, 60B..., the Internet 70, etc. A credit contact request given from the station 100 is transmitted to one of credit servers via a gateway server 32. When the credit contact is permitted, the credit contract information is transmitted from one of credit servers to the station 100 via the server 32 and stored in the station 100.

Classifications

- H04W88/02 Terminal devices

View 31 more classifications

JP2001167187A

Japan

Find Prior Art Similar

Other languages: Japanese

Inventor: Takeshi Natsuno, [redacted]

Worldwide applications

1999 JP 2000 IL CA BR AU SN WO KR CN PL US HU EP BR TW 2001 IL NO 2002 HK

Application JP35226599A events

1999-12-10	Application filed by NTT Docomo Inc, [redacted]
1999-12-10	Priority to JP35226599A
2000-12-07	Priority claimed from PCT/JP2000/008858A
2000-12-07	Priority claimed from US09/890,830
2000-12-07	Priority claimed from CA2549387A
2001-06-22	Publication of JP2001167187A
Status	Pending

Info: Patent citations (12), Cited by (23), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (16)

Hide Dependent

[Claims]

1. 1. A mobile communication terminal connected to a network of a contract institution server connected to a network of a user of a mobile communication terminal accommodated in the mobile communication network to mediate a subscription contract for electronic commerce. Receiving a request for the subscription from the user at the mobile communication terminal, and inputting information required for the subscription in response to the request for the subscription at the mobile communication terminal. Prompting the user, and transmitting information required for the subscription entered from the user to the mobile communication terminal to a server of the contracting institution via the mobile communication network. Subscription agreement mediation method.

    2. 2. The method according to claim 1, further comprising the step of transmitting information on whether or not to subscribe to the request for the subscription to the mobile communication terminal via the mobile communication network. In this case, the information necessary for e-commerce after the subscription transmitted from the server of the contract organization,
    A subscription contract comprising: transmitting to the mobile communication terminal via the mobile communication network; and receiving and storing information required for the electronic commerce after the subscription at the mobile communication terminal. Mediation method.

    3. 3. The subscription mediation method according to claim 1, wherein the step of prompting the user at the mobile communication terminal to input information required for the subscription is performed by the user so that the user inputs the required information. Transmitting input screen information to the mobile communication terminal via the mobile communication network; receiving the input screen information at the mobile communication terminal; and displaying the input screen indicated by the received input screen information. Displaying a subscription contract mediation method.

    4. 4. The subscription contract mediation method according to claim 3, wherein the input screen information is stored in a server of the contract organization.

    5. 5. The subscription mediation method according to claim 3, wherein the input screen information is stored in a relay device that relays data exchange between the mobile communication terminal and a server of the contract organization. Subscription agreement mediation method characterized by the above-mentioned.

    6. 6. The subscription mediation method according to claim 1, further comprising the step of performing user authentication of the user.

    7. 7. The method of claim 2, wherein the step of transmitting information necessary for the electronic commerce to the mobile communication terminal via the mobile communication network is transmitted from a server of the contract organization. Storing the information necessary for the electronic commerce; requesting the mobile communication terminal to acquire the information necessary for the electronic commerce in accordance with the information on whether the subscription is possible; Transmitting necessary information for the electronic commerce to the mobile communication terminal via the mobile communication network when there is a request for acquisition of important information. Method.

IPR2025-00645 Page 01793

8. 8. The subscription agreement intermediation method according to claim 2, further comprising the step of judging whether the subscription agreement is valid or not based on information necessary for the subscription agreement input by the user. Subscription mediation method.

9. 9. The subscription mediation method according to claim 8, wherein the server of the contract institution determines whether the subscription is acceptable.

10. 10. The subscription contract intermediation method according to claim 8, wherein a relay device that relays data transfer between the mobile communication terminal and a server between the contract machines determines whether the subscription contract is acceptable or not. Characteristic subscription mediation method.

11. 11. The subscription mediation method according to claim 2, wherein all the steps are executed by one communication

12. 12. The subscription contract intermediation method according to claim 2, wherein: a step of receiving the request for the subscription contract from the user; and a step of prompting the user to input information necessary for the subscription contract at the mobile communication terminal. Transmitting the information necessary for the subscription to the server of the contracting organization via the mobile communication network; and transmitting the information on whether or not the subscription is possible via the mobile communication network to the mobile communication terminal. Transmitting the information necessary for the electronic commerce after the subscription to the mobile communication terminal via the mobile communication network; receiving the information necessary for the electronic commerce after the subscription, and storing the information. And a communication performing the steps of performing the above steps is separated from each other.

13. 13. The subscription mediation method according to claim 1, wherein said subscription is a credit contract.

14. 14. The subscription mediation method according to claim 1, wherein said mobile communication terminal is a mobile phone.

15. 15. A mobile communication network for relaying data exchange between a mobile communication terminal and a server of a contract organization that concludes a subscription contract for e-commerce with a user of the mobile communication terminal, According to the request of the subscription from the mobile communication terminal,
Means for transmitting to the mobile communication terminal input screen information for prompting input of information necessary for the subscription contract, and information necessary for the subscription contract input to the mobile communication terminal by the user from the mobile communication terminal. Means for receiving and transmitting to a server of the contracting institution.

16. 16. The mobile communication network according to claim 15, further comprising: means for receiving, from a server of the contract organization, information on whether or not the request for the subscription can be accepted, and transmitting the information to the mobile communication terminal; Means for receiving information required for electronic commerce after the subscription from the server of the contract organization and transmitting the information to the mobile communication terminal.

Description

DETAILED DESCRIPTION OF THE INVENTION

[0001]

BACKGROUND OF THE INVENTION 1. Field of the Invention The present invention relates to a subscription contract mediation method for mediating a contract when subscribing to an electronic commerce service concluded between a user and a contract institution, and to execute the method. It relates to a mobile communication network.

[0002]

2. Description of the Related Art When a credit contract is concluded with a credit company or a deposit account is opened at a financial institution, a user usually first goes to a store of a contract institution such as a credit company (or by mail) to make a necessary payment. Submit the application form with the required items. After receiving the application for the contract, the contracting organization performs a predetermined examination and concludes the contract, creates a credit card or the like for the user to use the e-commerce service, and mails it to the user.

[0003]

As described above, a user who wants to apply for a subscription to various electronic commerce services must go to the store of the contract organization (or mail the application form to the contract organization). Must be done). In addition, a process of creating these cards (for example, a process of imprinting a name or a card number on a credit card and storing predetermined magnetic information in a magnetic stripe on the card) requires a certain time. In addition, these cards are generally delivered to the user by registered mail, which, in addition to a certain number of days for mailing, takes extra time if the user is not home at the time of mail arrival. Therefore, it takes a certain number of days from when the user completes the application for the subscription contract to when he or she obtains a credit card or the like, and it has been difficult to meet the user's need to obtain the card immediately. The present invention has been made in view of the circumstances described above, and has as its object to mediate the subscription contract more quickly without imposing a large burden on the user in various electronic commerce service subscription contracts. .

[0004]

According to an aspect of the present invention, there is provided a mobile communication system in which a contract institution server is accommodated in a mobile communication network via a mobile communication network connected to the network. A method for mediating a subscription contract for electronic commerce between a user of a communication terminal and the contract organization, the method comprising: receiving a request for the subscription contract from the user at the mobile communication terminal; Prompting the user at the mobile communication terminal to input information necessary for the subscription in response to a request for a contract, and transmitting the information required for the subscription entered by the user to the mobile communication terminal, Transmitting to a server of the contract organization via a communication network.

According to a second aspect of the present invention, in the subscription mediation method according to the first aspect, a step of transmitting to the mobile communication terminal via the mobile communication network information on whether or not the subscription to the subscription request has been made, Transmitting, when the subscription contract is approved, information necessary for electronic commerce after subscription transmitted from a server of the contract organization to the mobile communication terminal via the mobile communication network, Receiving and storing information necessary for the electronic commerce after the subscribing at the terminal.

According to a third aspect of the present invention, in the subscription agreement mediation method of the first aspect, the step of prompting the user to input information required for the subscription at the mobile communication terminal includes the step of: Transmitting input screen information for inputting information to the mobile communication terminal via the mobile communication network; and receiving the input screen information at the mobile communication terminal; and receiving the input screen information. And a step of displaying an input screen indicated by the following.

According to a fourth aspect of the present invention, there is provided the subscription mediation method according to the third aspect, wherein the input screen information is stored in a server of the contract organization. Is what you do.

According to a fifth aspect of the present invention, in the method of the third aspect, the input screen information relays data exchange between the mobile communication terminal and a server of the contract organization. Is provided.

According to a sixth aspect of the present invention, there is provided the subscription mediation method according to the first aspect, further comprising a step of performing user authentication of the user.

[0010] According to a seventh aspect of the present invention, in the subscription contract intermediation method according to the second aspect, the step of transmitting information necessary for the electronic commerce to the mobile communication terminal via the mobile communication network includes the contracting institution. Storing information necessary for the electronic commerce transmitted from the server of the mobile communication terminal; requesting the mobile communication terminal to acquire information necessary for the electronic commerce in accordance with the information on whether the subscription is possible; And transmitting a stored information necessary for the electronic commerce to the mobile communication terminal via the mobile communication network when there is a request for obtaining information necessary for the electronic commerce. A feature of the present invention is to provide a subscription mediation method.

[0011] The invention according to claim 8 is the subscription contract mediation method according to claim 2, further comprising a step of judging whether the subscription contract is valid or not based on information necessary for the subscription contract input by the user. The present invention provides a subscription mediation method characterized by performing the following.

[0012] According to a ninth aspect of the present invention, there is provided the subscription mediation method according to the eighth aspect, wherein the server of the contract institution determines whether or not the subscription is permitted. It is.

According to a tenth aspect of the present invention, in the subscription contract intermediation method according to the eighth aspect, a relay device for relaying data exchange between the mobile communication terminal and a server between the contract machines is provided. It is an object of the present invention to provide a subscription mediation method characterized by judging whether or not it is possible.

According to an eleventh aspect of the present invention, there is provided the subscription mediation method according to the second aspect, wherein all the steps are executed by one communication.

According to a twelfth aspect of the present invention, in the subscription contract intermediation method of the second aspect, a step of receiving the request for the subscription from the user, and inputting information required for the subscription in the mobile communication terminal. The step of prompting the user, the step of transmitting the information required for the subscription to the server of the contracting organization via the mobile communication network, and the step of transmitting Transmitting the information necessary for the electronic commerce after the subscription to the mobile communication terminal via the mobile communication network; and transmitting the information necessary for the electronic commerce after the subscription. The method of receiving and storing information is separated from the communication that performs the steps of subscribing.

The invention according to claim 13 is the invention according to claims 1 to 12
The method of claim 1, wherein the subscription is a credit contract.

The invention according to claim 14 is the invention according to claims 1 to 12
The method of claim 1 wherein the mobile communication terminal is a mobile phone.

According to a fifteenth aspect of the present invention, there is provided a mobile communication system for relaying data transfer between a mobile communication terminal and a server of a contract organization which concludes a subscription contract for electronic commerce with a user of the mobile communication terminal. A means for transmitting, to the mobile communication terminal, input screen information for prompting input of information necessary for the subscription contract, in response to a request for the subscription contract from the mobile communication terminal; Means for receiving, from the mobile communication terminal, information required for the subscription contract input to the mobile communication terminal, and transmitting the information to a server of the contract organization. .

According to a sixteenth aspect of the present invention, in the mobile communication network according to the fifteenth aspect, means for receiving, from a server of the contract organization, information on whether or not the subscription to the subscription request is possible, and transmitting the information to the mobile communication terminal Means for receiving information necessary for the electronic commerce after the subscription from the server of the contract organization and transmitting the information to the mobile communication terminal when the subscription contract is approved. It provides a net.

[0020]

DETAILED DESCRIPTION OF THE INVENTION [1. Configuration] [1-1. Configuration of Mobile Station] FIG. 1 is a block diagram showing a configuration of a mobile station 100 used in one embodiment of the present invention. The mobile station 100 includes a transmitting / receiving unit 110, a control unit 12
0, user interface 130, data input / output terminal 1
40, a magnetic writer 150, a magnetic stripe 160, and the like.

The transmitting / receiving unit 110 performs wireless communication with a base station of a mobile communication network that provides mobile telephone communication and mobile packet communication.

The control unit 120 controls each unit of the mobile station 100, and includes a CPU 121, a program R
OM122, ROM123 for credit, RAM124
And so on. Here, the mobile station 100 has a "call mode" for making a call using a mobile communication network,
At least two types of modes can be set, including a "packet communication mode" for performing packet communication using a mobile packet communication network.
The control unit 120 controls each unit of the mobile station 100 according to the setting status of each of these modes.

The RAM 124 is used as a work area for the CPU 121 and a user data area for telephone directory data and the like.

The credit ROM 123 stores information on attributes of a credit contract concluded between the user and the credit company (hereinafter referred to as credit contract information). This credit contract information is given from the credit company to the user, and includes, for example, the name of the credit company with which the user has made a credit contract, the URL of the server of the credit company (described later), the credit number (given for each credit contract). Identification number, usually
16

Digits), credit contract expiration date, user name, and the like. When the user has a plurality of credit contracts with a plurality of credit companies, credit contract information relating to the plurality of contracts is stored in the ROM 123 for credit.

The credit ROM 123 can be accessed only from a dedicated ROM reader / writer or a dedicated server of a credit company. RO for credit from dedicated ROM reader / writer
When accessing M123, the data input / output terminal 14
9, the write information to the credit ROM 123 is sent from the ROM reader / writer connected to the control unit 120 to the control unit 120. The control unit 120 checks the validity of the ROM reader / writer that has accessed the RO
The contents are written to M123. When accessing the credit ROM 123 from a dedicated server, the server writes information to the credit ROM 123 to the control unit 120 via a network such as a mobile packet communication network. Then, after confirming the validity of the accessed server, the control unit 120 writes the contents into the credit ROM 123. In addition,
When the control unit 120 detects a means other than the above that attempts to access the credit ROM 123, the control unit 120 performs processing for disabling the mobile station 100 itself.

A control program is stored in the program ROM 122, and the CPU 121 reads out the control program and executes various control processes. The control programs include various programs described below, in addition to programs related to the call function that the mobile station 100 normally has. This control program includes document data browsing software (so-called browser). CP
U121 loads the browser into the program ROM 122.
By reading and executing the data, it is possible to obtain HTML-format data from various information providing servers connected to the Internet via a gateway server (described later). The mobile station 100 acquires HTML data by transmitting an acquisition request designating a URL of a resource to the information providing server via the gateway server, and correspondingly transmitting the HTML data transmitted from the information providing server. The processing is completed by storing the data in the RAM 124.

In this control program, credit contract information is stored in the ROM 123 for credit,
Alternatively, a program for reading, changing, or deleting credit contract information stored in the credit ROM 123 is included.
The control program further includes a credit ROM by controlling the magnetic writer 150.
A program for writing and erasing the credit contract information read out from the magnetic stripe 160 to the magnetic stripe 160 and a program for giving the credit contract information read out from the credit ROM 123 to the mobile communication network are included.

The control program includes the mobile station 1
When the power of 00 is turned on, a program for transmitting the power on, the identification number of the mobile station 100 (hereinafter referred to as transmission information) using a specific channel is included.

Further, as described above, this control program contains the credit ROM 123 by unauthorized means.
A program for making the mobile station 100 itself unusable when an act of trying to access is detected.

The magnetic writer 150 transmits the credit contract information provided from the control unit 120 to the magnetic stripe 160.
Or the credit contract information on the magnetic stripe 160 is erased.

The magnetic stripe 160 is similar to a magnetic stripe widely used in current credit cards. Therefore, the credit contract information written on the magnetic stripe 160 is a magnetic stripe reading terminal (so-called CAT terminal) which is currently widely used.
Can be read. This magnetic stripe 160
is provided on a plastic card (hereinafter referred to as a magnetic card 161) housed in the mobile station 100. The magnetic card 161 is driven in accordance with a predetermined key operation on a keypad, which will be described later, and is normally stored in the mobile station 100. However, during credit shopping, the magnetic stripe 160 is used. The part is exposed from the mobile station 100 to the outside.

The user interface 130 includes a liquid crystal display 132 for displaying characters and the like, a keypad for the user to perform various input operations, a microphone and a speaker for the user to talk. The keypad may be provided with a "card storage / exposure key" for operating storage / exposure of the magnetic stripe 160,
Alternatively, the magnetic stripe 160 may be stored and exposed by a predetermined key operation using an existing numeric keypad.

FIG. 2 is a perspective view showing the appearance of the mobile station 100 provided with the card storage / exposure key 131. FIG. 4A shows the mobile station 1 in which the magnetic card 161 is stored.
The mobile station 100 is provided with a throttle 101 for storing and exposing the magnetic card 161. FIG. 2B shows the mobile station in a state where the magnetic stripe 160 of the magnetic card 161 is exposed to the outside. By the above-mentioned predetermined operation of the user,
The state shown in FIG. 7A and the state shown in FIG. Note that a signature field for the user is provided on the back surface of the magnetic card 161 in the same manner as a conventional credit card.

[1-2. Configuration of Credit System] FIG.
1 is a block diagram showing a configuration of a credit system using a mobile station 100. This credit system includes a mobile station 100, a mobile telephone network 20, a mobile packet communication network 3
0, CAT terminals 40a, 40b..., CAFIS (Cr
edit and FinanceInformation System) network 50, credit servers 60A, 60B ..., Internet 7
0, user store servers 80C, 80D, etc.

A user who has signed a credit contract
The mobile station 100 is owned. The mobile station 100 is connectable to a mobile telephone network 20 and a mobile packet communication network 30.

The mobile telephone network 20 is a network for providing a general call service using a mobile station.
0 can receive the service through the mobile telephone network 20. The mobile telephone network 20 includes a number of base stations 31 installed at predetermined intervals in a communication area, an exchange (not shown) for performing a circuit switching service, a control station 33 for controlling the network, and a communication line (see FIG. (Not shown). The control station 33 is provided with a subscriber database 331 for storing various information on subscribers who use communication services. The base station 31, the exchange, the control station 33, the communication line and the like are shared with the mobile packet communication network 30.

Here, the subscriber database 331 will be described. FIG. 4A shows the subscriber database 331.
FIG. As shown in the figure, the subscriber database 331 stores, for each "subscriber" of the mobile telephone network 20 (that is, the user of the mobile station 100), the mobile station 10.

5 "phone number", "name", "sex", "date of birth"
In addition, various data such as mobile station 100 and use prohibition information indicating prohibition of credit use are stored. In addition,
A use prohibition flag is registered in the use prohibition information column of the mobile station 100 and a user whose credit use is prohibited.

Referring back to FIG. 3, the configuration of the credit system will be described. In the figure, the mobile packet communication network 30
includes a gateway server 32 in addition to the above-described base station 31, switching center, control station 33, communication line, and the like. The gateway server 32 is a computer system provided in a mobile packet gateway relay exchange for interconnecting the mobile packet communication network 30 with another network such as the Internet 70, and converts different communication protocols among a plurality of networks. I do. In the present embodiment, a mutual conversion between a transmission protocol for the mobile packet communication network 30 and TCP / IP which is a standard communication protocol of the Internet 70 is performed. Also, this gateway server 32
is the mobile station 100, the credit servers 60A, 60B
Controls various data distribution processes performed between the store servers 80C, 80D, and so on.

Here, the gateway server 32 will be described. FIG. 5 is a block diagram showing the configuration of the gateway server 32. This gateway server 32
It comprises a control unit 301, a subscriber information management unit 302, a data distribution management unit 303, and the like. The control unit 301
It controls each unit of the gateway server 32 and functions as an interface between networks, such as performing protocol conversion between the mobile packet communication network 30 and another network such as the Internet 70. Further, the control unit 301 is, for example, an SSL (Secure Sockets L.
ayer), thereby protecting the contents of communication with the credit servers 60A, 60B,... and the user store servers 80C, 80D,. Further, when the user uses a predetermined service of mobile packet communication, the control unit 301 performs user authentication of a user who uses the mobile station 100 that has accessed the gateway server 32. This user authentication is performed by password collation described later.

The subscriber information management unit 302 stores and manages a subscriber registration information file 304 obtained by referring to the subscriber database 331 of the control station 33. The configuration of the subscriber registration information file 304 will be described later.

The data distribution management unit 303 is provided between the users of the plurality of mobile stations 100, between the user of the mobile station 100 and a user of another network such as the Internet 70, or between the user of the mobile station 100 and the credit server 60A. ,
.. And the store servers 80C, 80D,...
For example, the data distribution management unit 303 receives a communication request from the mobile station 100, the credit servers 60A, 60B, and the like, and transmits the communication contents to the destination of the communication request.
Alternatively, the data distribution management unit 303 temporarily stores the received communication content and notifies the terminal of the destination of the communication request (for example, the mobile station 100) that the communication content is stored. When receiving a communication content acquisition request from the terminal, the data distribution management unit 303 transmits the stored communication content to the terminal. For this purpose, the data distribution management unit 303 has a memory (not shown) for temporarily storing communication contents therein. The memory also stores service menu screen information transmitted to the mobile station 100 and used to display a menu of various service items on the liquid crystal display 132 of the mobile station 100. The service menu screen information is HTML format data, and the data of each service item includes the URLs of various servers that execute the respective services. Further, in this memory, store information where credit shopping is possible via the mobile packet communication network 30 is stored. The store information is also HTML format data, and the data of each store includes the URL of the server of each store. The user store information is transmitted to the mobile station 100 and displayed on the liquid crystal display 132 of the mobile station 100. When a user requests a specific service using the mobile station 100, the mobile station 100 transmits a URL included in the data of the service item to the gateway server 32, and the gateway server 32 performs the service based on the received URL. To the server that runs. Further, when the user is in the mobile packet communication network 3
Also, when performing a credit shopping at a certain store via the Internet, the URL of the HTML format data is similarly used.

Here, the subscriber registration information file 304 will be described. FIG. 4B is a diagram showing a data format of the subscriber registration information file 304. As shown in FIG. 2B, the subscriber registration information file 304 contains the "telephone number" of the mobile station 100 for each "subscriber" of the mobile packet communication network 30 (that is, the user of the mobile station 100). "Name", "Gender", "Date of birth", data and e-mail delivered to the user are stored in the data distribution management unit 30.
3 stores various data such as a "storage location" indicating where the information is stored, and a "password" previously registered by the user for application. Control unit 3 of gateway server 32
in step 31, user authentication is performed by comparing a password entered by the user into the mobile station 100 with a password stored in the subscriber registration information file 304.

Referring back to FIG. 3, the configuration of the credit system will be described. In FIG. 3, a number of CAT terminals 40
are installed in a store, a cash dispenser (CD), or the like. The CAT terminals 40a, 40
are provided with a magnetic reader (not shown),
It is possible to read the credit contract information recorded on the magnetic stripe 160 of 00. The CAT terminals 40a, 40b,... Are provided with an input interface (not shown), and a store clerk or the like can input predetermined information (for example, a purchase amount) from the input interface. The CAT terminals 40a, 40b ...
is connected to a dedicated network called the CAFIS network 50 and provides the CAFIS network 50 with the credit contract information read from the magnetic stripe 160 and the information such as the amount of money used, the date of use, and the shop used for credit shopping (Hereinafter, the CAT terminals 40a, 40b,.
The information given to the AFIS network 50 is called credit information).

The CAFIS network 50 has a large number of CAT terminals 4.
0a, 40b ... and credit servers 60A, 60B
.. Are connected. The CAFIS network 50 is a network connecting credit companies, distribution companies, and financial institutions at a nationwide level, and a CAFIS control center (not shown) controls the inside of the network. This CAFI
The S network 50 transfers various credit information generated by the user's credit shopping, cashing, etc. to the credit server 6 which is the credit contractor.
0A, 60B,... Or credit shopping availability information from any of the credit servers 60A, 60B,.
b.

The credit servers 60A, 60B... Are installed in each credit company, and the CAFIS network 50
And the Internet 70. The credit servers 60A, 60B,... Store user attribute information, credit contract information, and the like, and the credit database 62A, which stores contract user credit use history and fund settlement information. 62B ...

Here, the user databases 61A, 61
B and the credit databases 62A, 62B
・ ・ Is explained. 6A is a data format diagram of the user databases 61A, 61B,..., And FIG.
It is a data format figure of 2B ... Figure (A)
The user databases 61A, 61B

, The user database 61A, 61B,

・ The "Name", "Age", "Address",

User attribute information such as "phone number", "workplace", "annual income", "credit number" related to each credit contract,

Credit contract information such as "expiration date" and "use limit" is stored. This user attribute information is given by an application from the user at the time of the credit contract,

it is changed at any time by a change application from the user. The credit contract information is information that the credit company grants for each contract at the same time as when the credit contract is concluded, and part of the information is updated each time the expiration date elapses. Also,

As shown in FIG.

A, 628 . Include credit usage history of each user such as "usage date", "usage store", and "usage amount" of credit shopping and cashing, and "settlement amount" for each "settlement month". Is stored. The credit use history ("use date", "use shop" and "usage amount") is obtained from the CAT terminals 40a, 40b... And the use shop servers 80C, 80D.

A, 60B... The credit servers 60A, 60B,... Calculate the "payment amount" for each "payment month" based on the given "use date" and "use amount" information, and store them as fund settlement information. .

The credit servers 60A, 60B,.

・ The main functions of the credit contract (contract conclusion, renewal,

Change, cancellation, etc.), credit use determination, accumulation of various information related to credit contracts and credit use, fund settlement related to credit use, provision of various information to users, etc. Each function will be described in detail.

The credit servers 60A, 60B,...

Has previously stored an input screen given to the mobile station 100 for a credit contract, a change screen given to the mobile station 100 for a contract change, and upon receiving a credit contract request or the like from the mobile station 100, An input screen or the like corresponding to the request is displayed on the Internet 70 and the gateway server 3.

2 and the like to the mobile station 100.

The credit servers 60A, 60B

Create and store contract update candidate user files 601A, 601B,... For contract update processing.

The contract update candidate files 601A, 601B,...

Stores information about a user whose contract is about to be renewed.

Here, the contract update candidate user file 60

1A, 601B,... Will be described. FIG. 6 (C)

The contract update candidate user files 601A, 601B

・ ・ The data format diagram is shown. As shown in FIG. 7C, contract update candidate user files 601A and 601

B... Store data such as "name", "credit number", "telephone number", and "expiration date" of each user. The credit servers 60A, 60B ...

The "expiration date" of the credit contract stored for each user in the user database 61A is set to a fixed period (for example, 2

.. Every four hours) to extract users whose expiration date of the credit contract is approaching (for example, within one week until the expiration date) and to extract information on the extracted users from the user databases 61A, 61B, and so on. Obtain the contract update candidate user files 601A, 601B

・ ・ It is stored in

Again, the credit servers 60A, 60B

・ ・ Return to explanation. Credit server 60A, 60B

.., Have previously stored examination conditions for determining whether or not to accept a credit contract, receive contents input by the user from the mobile station 100 according to the input screen from the mobile station 100, and perform credit based on the input contents and the examination conditions. An examination is conducted to determine whether the contract is valid. And the credit server 60A, 60B

.., If the result of the examination indicates that a credit contract is permitted, generate credit contract information to be stored in the magnetic stripe 160 of the mobile station 100 and give it to the mobile station 100;

Also, user attribute information and credit contract information relating to the contract are stored in the user databases 61A, 61B,.

When the user performs credit shopping or the like, the credit servers 60A and 60B

Are credit information provided from the CAT terminals 40a, 40b (or the user store servers 80C, 80D,...) And the user databases 61A, 61B..

It is determined whether or not the generated credit shopping is valid using various information stored in the CAT terminals 40a, 40b,... (Or as a credit availability information). User store server 80C,

80D ...). And the credit server 6

0A, 60B,... Store the data of the generated credit shopping or the like in the credit databases 62A, 62B.

... is stored.

The credit servers 60A, 60B

. notifies the financial institution with the credit debit account of the fund settlement information via the CAFIS network 50,

Perform credit debit processing.

Further, the credit servers 60A, 60B

. Obtains desired information of the user from information stored in the user databases 61A, 61B... And the credit databases 62A, 62B.

It is provided to the mobile station 100 via the Internet 70 and the mobile packet communication network 30.

The credit servers 60A, 60A

8 ... have an encryption communication algorithm such as SSL (Secure Sockets Layer), so that the gateway server 32 and the store server 80C, 8

0D etc. are protected.

Are servers that provide a so-called virtual shop where the user can perform online shopping. .. Store the shopping screen information displayed on the mobile station 100 as HTML format data. The shopping screen information includes information on a product to be sold to the user (for example, a product name, a product description, a sales price, and the like).

.. Receive the credit shopping request from the user's mobile station 100,

... The mobile station 100 is provided with shopping screen information, and performs processing related to the credit shopping in cooperation with one of the credit servers 60A, 60B,. In addition, the user store servers 80C, 80D,...

For example, it has an encryption communication algorithm such as SSL (Secure Sockets Layer), so that the gateway server 32 and the credit servers 60A, 60B,.

IPR2025-00645 Page 01798

・ The contents of communications with other parties are protected. [2. Operation] Next, the operation of the present embodiment will be described by dividing it into the following operation modes 1. At the time of credit contract 2-. At the time of credit shopping at stores 2- 2. At the time of credit shopping via the mobile packet communication network 30 3. When renewing credit contract When changing the credit contract 5. When canceling credit contract 6. When use of mobile station 100 and credit is prohibited. When referencing credit usage history, etc.

[2-1. Operation at the Time of Credit Contract] FIGS. 7 and 8 are flowcharts showing the operation when a user makes a credit contract using the mobile station 100. FIG. (A) to (J) are diagrams of screens displayed on the liquid crystal display 132 of the mobile station 100 at the time of a credit contract,
FIGS. 7A to 7J are arranged in chronological order corresponding to the operations at the time of the credit contract shown in FIGS. Hereinafter, the operation at the time of a credit contract will be described with reference to FIGS. 7, 8, and 9.

First, in step SP101, the user makes a call to the gateway server 32 with a predetermined telephone number and requests the start of the packet communication mode.

In step SP102, the gateway server 32 starts the packet communication mode for the user by receiving the packet communication mode start request, and displays the service menu screen information stored therein to the mobile station 100. Send.

At step SP103, the mobile station 100
Receives the service menu screen information and displays the service menu screen on the liquid crystal display 132. FIG.
(A) is a diagram of a screen displayed on the mobile station 100 at this time.

In step SP104, the user selects a desired service from the displayed service menu screen by key operation. Here, on the screen shown in FIG. 9A, the user moves the cursor over "credit" and selects it. Then, the mobile station 100 transmits the selected service request (here, "credit") to the gateway server 32.

In step SP105, the gateway server 32 transmits service menu screen information indicating more detailed service contents to the mobile station 100 in response to the received service request.

In step SP106, the mobile station 100
Receives the detailed service menu screen information and displays the service menu screen on the liquid crystal display 132. FIG. 9B is a diagram of a screen displayed on mobile station 100 at this time.

At step SP107, the user selects a desired service from the displayed detailed service menu screen by key operation. Here, FIG. 9 (B)
On the screen shown in FIG. 7, the user moves the cursor on "credit contract" and selects it. Then, the mobile station 100 transmits the selected detailed service request (here,
"Credit contract") to the gateway server 32. The above-described service menu screen is transmitted to the mobile station 100 a plurality of times until the user finally specifies a desired service.

At step SP108, the gateway server 32 receives the detailed service request, and transmits to the mobile station 100 password input screen information for the user to input a password.

In step SP109, the mobile station 100
Receives the password input screen information, and the liquid crystal display 132 displays the password input screen. The user
The password registered in advance in the gateway server 32 is entered in the password entry field 135 on the password entry screen. FIG. 9C is a diagram of a password input screen displayed on mobile station 100 at this time. The user
Enter the password in the password entry field, move the cursor and select "Execute".

At step SP111, the mobile station 100
Transmits the password information input by the user to the gateway server 32.

At step SP113, the gateway server 32 receives the password information.

At step SP115, the gateway server 32 determines whether the password received from the mobile station 100 is
The mobile station 10 stored in the subscriber information management unit 302
User authentication is performed by checking the password of the user 0.

In step SP117, it is determined whether or not the user is authenticated as a result of the user authentication.

If it is determined in step SP117 that the user is a valid user, the process proceeds to step SP119, where the gateway server 32 sends a request to the mobile station 100 in response to a final service request (credit contract request) from the user. The displayed next screen information is transmitted to the mobile station 100.

On the other hand, if it is determined in step SP117 that the user is not a valid user, the process proceeds to step S117.
Proceeding to P121, the gateway server 32 transmits to the mobile station 100 a service refusal notice indicating that a service request (credit contract request) from the user is not accepted.

Then, in step SP123, the mobile station 100 receives the information transmitted from the gateway server 32.

Next, in FIG. 8, step SP125
Then, the next screen received by the mobile station 100 is displayed on the liquid crystal display 132. In this case, the credit company name to which the user can make a contract is displayed on the liquid crystal display 132. FIG. 9D is a diagram of a screen displayed on mobile station 100 at this time. Note that, when the mobile station 100 receives the service unavailable notification, the mobile station 100 displays the notification on the liquid crystal display 132 (not shown), and the process ends.

At step SP126, the user selects a desired credit company from the displayed credit companies by key operation. In other words, the user can see FIG.
A cursor is moved to a desired credit company on the screen shown in (D), and the credit company is selected by a predetermined key operation. Here, for example, it is assumed that the credit company A is selected.

At step SP127, the mobile station 100
Sends the selected credit company name (Company A) and the URL of the credit server 60A of Company A to the gateway server 3
Send to 2.

At step SP129, the gateway server 32 receives the credit company name (company A) and the URL, and transmits a credit contract request to the credit server 60A based on the received URL. At this time, the gateway server 32 protects the content transmitted to the credit server 60A with SSL. In the following description of various operations, the gateway server 3

2. When communication is performed between each of the credit servers 60A, 608,... And the user store servers 80C, 80D,.

At step SP131, the credit server 60A receives a credit contract request from the gateway server 32.

At step SP133, the credit server 60A transmits the information (eg, name, age, date of birth, address, telephone number, work location,
Screen information for input for the user to input annual income, password, etc.) is transmitted to the Internet 70 to the mobile station 100 as a destination.

At step SP135, the gateway server 32 receives the input screen information from the credit server 60A and transmits it to the mobile station 100.

At step SP137, the mobile station 100
Receives the input screen information from the gateway server 32 and displays the input screen on the liquid crystal display 132.
FIG. 9E is a diagram of a screen displayed on mobile station 100 at this time.

At step SP139, the user inputs necessary information while referring to the input screen displayed on the liquid crystal display 132. That is, the user can use FIG.
On the screen shown in (E), necessary information is entered in each input field. Items to be input by the user include various items such as "telephone number" and "workplace" in addition to "name", "date of birth" and "address" shown in FIG. The other items are sequentially displayed on the liquid crystal display 132 when the user scrolls down the screen.

In step SP141, the mobile station 100
Transmits the input content (hereinafter, referred to as input information) to the gateway server 32.

At step SP143, the gateway server 32 receives the input information, and
Send to A.

At the same time, in step SP145, the gateway server 32 sends a transmission completion notification indicating that the input information has been transmitted to the credit server 60A.
Send to 00.

In step SP 147, the mobile station 100 receives the transmission completion notification from the gateway server 32 and displays it on the liquid crystal display 132 to notify the user. FIG. 9F is a diagram of a transmission completion notification screen displayed on the mobile station 100 at this time.

On the other hand, in step SP149, credit server 60A receives input information from gateway server 32.

At step SP151, the credit server 60A examines whether or not a credit contract is possible based on the received input information while referring to the examination conditions stored by itself.

In step SP153, the result of the examination by the credit server 60A is determined. If the result of the determination is that the contract is not possible, the process proceeds to step SP155, where the credit server 60A sends a contract refusal notice to the mobile station 100 as an address to the Internet. 70.

As a result of the determination in step SP153,
If the contract is permitted, the process proceeds to step SP157, in which the credit server 60A generates new credit contract information, and sends the contract permission notification and the generated credit contract information to the Internet 70 to the mobile station 100 as a destination.

Then, in step SP159, the credit server 60A stores the user attribute information and the credit contract information of this contract in the user database 61A.

In step SP161, the gateway server 32 receives the contract refusal notice or the contract permit notification and the credit contract information from the credit server 60A, and temporarily stores the information therein.

At step SP163, gateway server 32 calls mobile station 100 and transmits an information reception notification indicating that information addressed to mobile station 100 has been received from credit server 60A.

At step SP165, the mobile station 100
Receives the information reception notification from the gateway server 32 and displays it on the liquid crystal display 132 to notify the user. FIG. 11G shows the mobile station 1 at this time.
It is a figure of the screen displayed on 00.

Then, in step SP167, the mobile station 100 is operated by a predetermined key operation of the user who saw the display.
Transmits to the gateway server 32 an information acquisition request that requests acquisition of information stored in the gateway server 32. That is, when the user selects "reference" on the screen shown in FIG. 9G, an information acquisition request is transmitted from the mobile station 100 to the gateway server 32.

At step SP169, the gateway server 32 receives the information acquisition request from the mobile station 100,
In response, he / she remembers the contract refusal notice,
Alternatively, the contract acceptability notice and the credit contract information are transmitted to the mobile station 10.
Send to 0.

At step SP171, the mobile station 100
Receives a contract refusal notice or a contract permit notice and credit contract information from the gateway server 32.

At step SP173, the mobile station 100
Displays the received content on the liquid crystal display 132. When the mobile station 100 receives the credit contract availability notification and the credit contract information, the mobile station 100
The received credit contract information is stored in the OM 123.
FIG. 9 (G) is a diagram of a screen showing a notification that a credit contract cannot be made. FIG. 9H is a screen showing a notification that a credit contract is available. When the user selects "next" on this screen, the screen moves to the next screen (FIG. 1I). FIG. 9 (I) is a screen for the user to confirm the contents of the credit contract. As shown in FIG. 1I, a "credit number", an "expiration date", and the like relating to the credit contract are displayed on this screen. Note that the screen information shown in FIG. 1I is stored in the credit ROM 123, and the liquid crystal display 132
And the user can check the credit contract information at any time.

As described above, the mobile station 10 owned by the user
9 and the credit server 60 of the credit company
A, 608,... Perform a process related to a credit contract by an electric communication means, and therefore perform the process (particularly, application of a credit

contract from a user to a credit company, notification of credit availability from a credit company to a user, and credit (Assignment of contract information) can be executed quickly.

Note that the above described step SP in FIG.
The operations shown in 101 to step SP123 are mainly operations from packet communication request to user authentication. In addition to the above-described credit contract, when using a credit using a mobile packet communication network, when changing a credit contract. This is an operation commonly performed at the stage prior to each operation at the time of cancellation or inquiry of credit use history or the like.

[2-2. Operation at Credit Shopping] Next, an operation at the time of credit shopping using the mobile station 100 will be described. There are two forms of credit shopping using the mobile station 100. That is, the credit contract information on the magnetic stripe 160 is provided to the credit server 80 via the CAT terminal 40 at the store, and the credit contract information stored in the ROM 123 for credit is transferred to the credit server 80 via the mobile packet communication network 30. There is a form to give to
Hereinafter, these will be described separately. [2-2. Operation during Credit Shopping at Store] FIG. 10 is a flowchart showing the operation of the mobile station 100 and the credit system in a mode in which the magnetic stripe 160 is used at the store.

First, in accordance with a predetermined operation of the user, in-store credit shopping processing is started in mobile station 100.

At step SP201, the control unit 120 of the mobile station 100 reads out all credit contract information stored in the credit ROM 123 and displays the credit company names on the liquid crystal display 132.

in step SP203, the user selects a desired credit company from the displayed credit companies by key operation. Here, for example, it is assumed that the credit contract of the credit company A is selected. If the number of contracted credit companies is singular, "OK" may be input to the displayed credit company.

At step SP205, the control unit 120 of the mobile station 100 gives the credit contract information of the selected company A to the magnetic writer 150, and the magnetic writer 150 writes the given credit contract information on the magnetic stripe 160.

When the credit contract information is the magnetic stripe 16
When the value is written to 0, the magnetic card 11 is set in an exposing state, and the control unit 120 displays on the liquid crystal display 132 that the exposing is possible. And step SP
in 207, when the user visually confirms that the exposure is possible, the user presses the card storage / exposure key of the mobile station 100, and the magnetic stripe 160 portion of the magnetic card 161 is moved to the mobile station 100.
Exposed from

in step SP209, the magnetic stripe 160 is slid to the magnetic reader of the CAT terminal (here, the CAT terminal 40b), and
0 is read into the CAT terminal 40b.

At step SP211, the clerk or the like
A usage amount or the like related to credit shopping is input to an input interface (not shown) of the CAT terminal 40b.

in step SP213, the CAT terminal 40
b transmits the credit contract information and the CAT terminal 40 to the credit server 60A of the company A via the CAFIS network 50.
b (these information is hereinafter referred to as credit information).

At step SP215, the credit server 60A receives the credit information from the CAT terminal 40b.

In step SP217, the credit server 60A searches the user database 61A based on the received credit information, and determines whether the requested credit shopping is legitimate. This determination may be, for example, whether the credit contract has expired, whether the credit limit has been exceeded, whether the magnetic card has been disabled, or the credit contract itself has become invalid. This is to check whether or not they are not.

If the result of the determination in step SP217 is that the credit is not valid, the process proceeds to step SP219, and the credit server 60A issues a credit rejection notification indicating that the requested credit use is not possible (and if necessary, The reason why credit cannot be used)
0 to the CAT terminal 40b.

On the other hand, as a result of the determination in step SP217,
When it is determined that the credit is valid, the process proceeds to step SP221, and the credit server 60A sends a credit permission notification indicating that the requested credit is available to the CAT terminal 40.
b, and in step SP223, the credit use history and fund settlement information for this credit shopping are stored in the credit database 62A.

In step SP225, the CAT terminal 40
b receives the notification and the like from the credit server 60A.

Then, in step SP227, the CAT
The terminal 40b outputs the received notification or the like to a credit slip or a display device (not shown) of the CAT terminal. The clerk performs a predetermined procedure according to the displayed contents. Thereafter, when the user writes the same signature as the signature on the back of the magnetic card 161 in the signature field of the credit slip displaying the usage amount and the like, the credit shopping is completed.

On the other hand, when the reading of the credit contract information on the magnetic stripe 160 is completed, the user presses the card storage / exposure key of the mobile station 100, and in step SP229, the magnetic card 161 is moved to the throttle 101 of the mobile station 100. Is stored inside.

When the magnetic card is stored, step SP
In 231, the control unit 120 of the mobile station 100 gives a message to the magnetic writer 150 that the credit contract information of the company A stored in the magnetic stripe 160 is erased, and the magnetic writer 150 executes it.

[2-2. Operation during Credit Shopping Using Mobile Packet Communication Network] Next, operation during credit shopping using the mobile packet communication network 30 will be described. FIG. 7 and FIG. 11 are flowcharts showing operations when the user performs credit shopping using the mobile station 100. The operation shown in FIG. 7 is substantially the same as the operation at the time of the credit contract, but in step SP107 in the figure, the user selects "credit shopping" as the desired service. Description of the other operations in FIG. 7 is omitted.

In step SP301 of FIG. 8, the names of all shops where the user can perform credit shopping are displayed on the liquid crystal display 132.

At step SP303, the user selects a desired user shop from the displayed user shops by key operation. Here, it is assumed that, for example, the store C is selected.

At step SP305, the mobile station 100
is the selected store name (store C) and the store server 80
The URL of C is transmitted to the gateway server 32.

In step SP307, the gateway server 32 receives the store name (store C) and the URL, and transmits a credit shopping request to the store server 80C based on the received URL.

In step SP309, the user store server 8
0C receives the credit shopping request from gateway server 32.

At step SP311, the user store server 8
In response to the received credit shopping request, 0C sends the shopping screen information stored by itself to the Internet 70 with the mobile station 100 as the destination.

In step SP313, the gateway server 32 receives the shopping screen information from the credit server 60A and transmits it to the mobile station 100.

In step SP315, the mobile station 100
Receives the shopping screen information from the gateway server 32 and displays the shopping screen on the liquid crystal display 132.

In step SP 317, the user selects a product to purchase while referring to the shopping screen displayed on the liquid crystal display 132.

When the product selection is completed, the mobile station 100
All the credit contract information stored in the credit ROM 123 is read, and the credit company names are displayed on the liquid crystal display 132. Then, in step SP319, the user selects a credit company desired to use in the credit shopping from the displayed credit companies. Here, it is assumed that the credit company B has been selected.

At step SP321, the mobile station 100
Transmits to the gateway server 32, as input information, information on the selected product and the amount of use, credit contract information of the selected company B, the URL of the store server 80C, the URL of the credit server 60B, and the like.

In step SP323, the gateway server 32 receives the input information from the mobile station 100, refers to the contents of the input information, and uses the input information to store the information in the user store server 8.
Send to 0C.

In step SP325, the store server 8
0C receives the input information from the gateway server 32. Then, the store server 80C transmits the credit contract information and the usage amount information among the received input information to the credit server 60B as credit information.

In step SP327, the credit server 60B receives the credit information from the store server 80C.

In step SP329, the credit server 60B searches the user database 61B based on the received credit information, and determines whether or not the requested credit shopping is legitimate. This determination may be, for example, whether the credit contract has expired, whether the credit limit has been exceeded, whether the magnetic card has been disabled, or the credit contract itself has become invalid. This is to check whether or not they are not.

If the result of the determination in step SP329 is that the credit server 60B determines that the credit shopping is not valid, the process proceeds to step SP331, and the credit server 60B sends a credit unavailable notification indicating that the requested credit shopping is unavailable. Send it to server 80C.

On the other hand, as a result of the determination in step SP329,
If it is determined to be valid, the process proceeds to step SP333, in which the credit server 60B transmits a credit available notification indicating that the requested credit shopping is available to the user store server 80C, and further proceeds to step SP335. Store the credit use history and the fund settlement information in the credit database 62B.

In step SP337, the user store server 8
0C receives the notification from credit server 60B.

Then, in step SP339, the store server 80C transmits the received notification to the gateway server 32 with the mobile station 100 as the destination. If the notification is a credit availability notification, the user store server 80C stores the product or the like selected by the user as credit shopping information, and sends the product to the user.
Perform predetermined processing.

[0139] At step SP341, the gateway server 32 receives the notification from the store server 80C and transmits it to the mobile station 100.

In step SP343, the mobile station 100
Receives the notification from the gateway server 32 and displays the received content on the liquid crystal display 132 to notify the user.

[2-3. Behavior when renewing credit contract]
Next, an operation at the time of updating a credit contract will be described. FIG. 12 is a flowchart showing a flow of operation at the time of updating a credit contract.

In step SP401, the credit server (here, credit server 60A) creates a contract update candidate user file 601 with reference to the user database 60A.

In step SP403, the credit server 60A refers to the contract update candidate user file 601, and sends a contract update advance notification for notifying the update of the credit contract in advance to the mobile station of the contract update candidate user (here, the mobile station 100). To the Internet 70 as a destination.

In step SP405, when the gateway server 32 receives the contract update advance notification, the mobile station 1
Call 00 to transfer the above notification.

In step SP407, the mobile station 100
Receives the contract update advance notice from the gateway server 32 and displays the received contract update advance notice on the liquid crystal display 132.

IPR2025-00645 Page 01802

In step SP409, the mobile station 100
Transmits response information to the displayed contract update advance notice by a key operation of the user. This response information indicates that the contract is renewed, or that the contract is not renewed.

At step SP411, the gateway server 32 receives the response information from the mobile station 100 and transmits it to the credit server 60A.

At step SP413, the credit server 60A receives the response information from the gateway server 32.

[0149] In step SP415, the credit server 60A determines the mobile station 1 based on the received response information.
It is determined whether the credit contract of the user 00 is renewable.

If the result of determination in step SP415 is that updating is possible, the flow proceeds to step SP417, where the credit server 60A generates updated new credit contract information, and stores the generated credit contract information in the user database 60A. At the same time, and sends it to the Internet 70 with the mobile station 100 as a destination.

If the result of determination in step SP415 is that renewal is not possible, the process proceeds to step SP421, where the credit server 60A deletes information about users whose contract renewal is not possible, stored in the user database 61A. Then, in step SP423, the credit server 60A sends a contract non-renewal notice indicating the contract non-renewal to the Internet 70 to the mobile station 100 as a destination.

Then, at step SP425, the gateway server 32 receives the updated credit contract information or the contract non-update notice from the credit server 60A, and temporarily stores the information.

In step SP427, gateway server 32 calls mobile station 100 and transmits an information reception notification indicating that information addressed to mobile station 100 has been received from credit server 60A.

In step SP429, the mobile station 100
Receives the information reception notification from the gateway server 32 and displays it on the liquid crystal display 132 to notify the user.

In step SP431, the mobile station 100 transmits to the gateway server 32 an information acquisition request for acquiring information stored in the gateway server 32 by a predetermined key operation of the user who has viewed the display.

In step SP433, the gateway server 32 receives the information acquisition request from the mobile station 100,
In response, the mobile station 100 transmits the updated credit contract information or the contract non-renewal notification stored therein.
Send to

At step SP435, the mobile station 100
Receives updated credit contract information or a contract non-renewal notice from the gateway server 32.

In step SP437, the mobile station 100
Displays the received content on the liquid crystal display 132. Then, when receiving the updated credit contract information, the mobile station 100 updates information such as the expiration date. In addition, when the mobile station 100 receives the notification that the contract has not been renewed, the mobile station 100 sets the credit ROM 123 when the expiration date has passed.
Deletes the credit contract information stored in.

It is also conceivable that the user does not respond to the credit contract advance notification given to mobile station 100 even if the expiration date has expired. In such a case, the credit server 60A transfers the updated credit contract information after the expiration date via the gateway server, assuming that the user has responded to the contract renewal with a "yes" response. This is transmitted to the station 100, and the mobile station 100 updates information such as an expiration date.

[2-4. Operation when Credit Contract is Changed] Even when the user changes the name or address, the mobile station 100
It is possible to carry out such a change procedure using. Hereinafter, the operation when the credit contract is changed will be described.
FIG. 7 and FIG. 13 are flowcharts showing the operation when the user makes a credit contract using the mobile station 100. The operation shown in FIG. 7 is almost the same as the operation at the time of the credit contract, but in step SP107 in the figure, the user selects "change credit contract" as the desired service. Description of other operations is omitted.

At step SP501 in FIG. 13, all credit companies with which the user has contracted are displayed on the liquid crystal display 132.

At step SP503, the user selects a desired credit company from the displayed credit companies by key operation. Note that it is also possible to select all credit companies. Here, it is assumed that the credit company A is selected.

In step SP505, the mobile station 100 stores the name of the selected credit company in the gateway server 32.
Send to

At step SP509, the gateway server 32 receives the credit company name from the mobile station 100 and transmits a credit contract change request to the credit server 60A.

In step SP511, the credit server 60A receives the credit contract change request

At step SP513, the credit server 60A sends screen information for changing the credit contract of the company A to the Internet 70 with the mobile station 100 as a destination.

In step SP515, the gateway server 32 receives the screen information for change from the credit server 60A and transmits the screen information to the mobile station 100 as a destination.

In step SP517, the mobile station 100
Receives the change screen information from the gateway server 32 and displays the change screen on the liquid crystal display 132.

At step SP519, the user inputs the contents to be changed while referring to the change screen displayed on the liquid crystal display 132.

In step SP521, the mobile station 100
Transmits the input contents (hereinafter, referred to as changed contents) to the gateway server 32.

At step SP523, the gateway server 32 receives the content of the change, and

IPR2025-00645 Page 01803

Send the change to A.

At step SP525, credit server 60A receives the content of the change.

In step SP527, the credit server 60A changes the contents of the user attribute information and the credit contract attribute information stored therein based on the received change content.

When the change processing is completed, step SP52
Proceeding to 9, the credit server 60A sends a completion notification indicating that the contract change processing has been completed to the Internet 70 to the mobile station 100 as a destination.

At step SP531, the gateway server 32 receives the completion notification via the Internet 70 and transmits it to the mobile station 100.

In step SP533, the mobile station 100
Receives the completion notification from the gateway server 32.

In step SP535, the mobile station 100
Displays the received completion notification on the liquid crystal display 132. [2-5. Operation when Canceling a Credit Contract] In addition, cancellation processing of a credit contract can be performed using this system. Hereinafter, an operation when a user makes a credit contract using the mobile station 100 will be described. FIG. 7 and FIG. 14 are flowcharts showing the operation when the user makes a credit contract using the mobile station 100. FIG.
is substantially the same as the operation at the time of the credit contract, but at step SP107 in the figure, the user selects "Credit Cancellation" as the desired service. Description of other operations is omitted.

At step SP601 in FIG. 14, all credit companies with which the user has contracted are displayed on the liquid crystal display 132.

In step SP603, the user selects a desired credit company from the displayed credit companies by key operation. Here, it is assumed that the credit company A is selected.

In step SP605, the mobile station 100 stores the name of the selected credit company in the gateway server 32.
Send to

At step SP607, the gateway server 32 receives the credit company name from the mobile station 100 and transmits a credit contract cancellation request to the credit server 60A.

At step SP609, the credit server 60A receives the credit contract cancellation request from the gateway server 32.

In step SP611, the credit server 60A deletes the credit contract, for example, deletes the user attribute information and the credit contract attribute information stored in the user database 61A based on the received credit contract cancellation request.

In step SP613, the credit server 60A sends a completion notification indicating that the contract cancellation processing has been completed to the Internet 70 with the mobile station 100 as a destination.

[0185] In step SP615, the gateway server 32 receives the completion notification via the Internet 70 and transmits it to the mobile station 100.

In step SP617, the mobile station 100
Receives the completion notification from the gateway server 32.

In step SP619, the mobile station 100
Displays the received completion notification on the liquid crystal display 132.

[2-6. Operation When Prohibition of Use of Mobile Station 100 and Credit] A case in which a user loses or stolen the mobile station 100 is considered.
in such a case, if the use of the credit is not prohibited, there is a possibility of unauthorized use by a third party. Hereinafter, the operation when the mobile device 100 and the use of the credit are prohibited will be described. FIG. 15 is a flowchart illustrating a flow of processing for prohibiting use of the mobile device 100 and credit.

When the user loses the mobile station 100, the user contacts the communication company that manages the mobile telephone network 20 and the mobile packet communication network 30 by a predetermined method to use the communication of the mobile station 100 and use the credit. Communicate the prohibition. In step SP701, the communication company that has received the above notification from the user accesses the subscriber database 331 of the control station 33 using a predetermined management terminal, and prohibits the use of communication services and credits for the user. Is registered. Thereafter, the mobile station 10 of the user Use of communication services and credits by 9 is prohibited. Specifically, the operation is as follows.

First, in step SP703, the mobile station 10
The third party illegally acquiring 9 turns on the power of the mobile station 100.

In step SP705, the mobile station 100
indicates that the power is turned on and the mobile station 1 uses a specific channel.
It transmits an identification number 00 (hereinafter referred to as transmission information). The base station including the location of the mobile station 100 in the jurisdiction area (here, the base station 32) receives the transmission information from the mobile station 100 and sends it to the control station 33.

In step SP707, the control station 33
The transmission information is received from the base station 32.

Then, in step SP709, the control station 33 determines the subscriber database 3 based on the received transmission information.
Access is made to the mobile station 100 to check for communication and credit use prohibition information.

In step SP711, the control station 33, which has determined that there is use prohibition information, informs the mobile station 1 via the base station 32 of the prohibition of communication of the mobile station 100 and use of credit.
Send to 00.

In step SP713, the mobile station 100
Receives, via the base station 31, the communication of the mobile station 100 and the prohibition of credit use.

IPR2025-00645 Page 01804

in step SP715, the mobile station 100
Performs communication and credit use prohibition processing. Here, in the communication use prohibition processing, each unit of the mobile station 100 that operates for the communication processing is not operated. In addition, the process of prohibiting the use of credit is performed by the credit ROM 123.
Delete credit contract information stored in.

[2-7. Operation when inquiring credit history etc.] The user can access the credit servers 60A, 60B... Using the mobile station 100 to inquire various information such as credit usage history and the next credit debit amount. It is. The operation at the time of inquiring the credit use history and the like will be described below. 7 and 16
9 is a flowchart showing an operation when a user uses the mobile station 100 to inquire about a credit use history. The operation shown in FIG. 7 is almost the same as the operation at the time of the credit contract,
in step SP107 in the figure, the user selects "credit history" as a desired service. Description of other operations is omitted.

In step SP801 of FIG. 13, all credit companies with which the user has contracted are displayed on the liquid crystal display 132.

In step SP803, the user selects a desired credit company from the displayed credit companies by key operation. Here, it is assumed that the credit company A is selected.

[0200] In step SP805, the mobile station 100 transmits the selected credit company name (company A) to the gateway server 32.

In step SP807, the gateway server 32 sends the credit company name (A
) And transmits a credit use history inquiry request to the credit server 60A.

At step SP809, the credit server 60A receives the credit use history inquiry request.

At step SP811, the credit server 60A searches the credit use history information stored in the credit database 62A.

At step SP813, the credit server 60A sends the credit use history information obtained as a result of the search to the Internet 70 with the mobile station 100 as a destination.

[0205] At step SP815, the gateway server 32 receives the credit use history information via the Internet 70 and transmits it to the mobile station 100.

In step SP817, the mobile station 100
Receives the credit use history information from the gateway server 32.

In step SP819, the mobile station 100
Displays the received credit usage history on the liquid crystal display 1
32.

[B. Modifications] [B-1. Modification Example at the Time of Credit Contract] In the above description, all operations at the time of a credit contract are performed in a continuous session, but this is not always necessary.
That is, a credit contract request operation from the mobile station 100 to the credit server 60 (ie, step SP101 in FIG. 7)
8 to step SP149 in FIG. 8) and the response operation from the credit server 60 to the mobile station 100 (that is, steps SP151 to SP173 in FIG. 8) may be separated. For example, there may be a case where a considerable amount of time is required for the examination process at the time of a credit contract, or a case where a part or all of the examination process is performed on behalf of another information processing device or a person. The communication between the mobile station 100 and the credit server 60 may be terminated once when the operation is completed, and the examination result may be notified to the mobile station 100 later when the credit server 60 acquires the result of the examination processing.

Also, the credit servers 60A, 60B
The process at the time of the credit contract in the... May be only the process related to the credit contract request operation. For example, the process ends in step SP149 of FIG. 7, and thereafter, as a result of the examination by the credit company, if the contract is not possible, the user is notified by telephone or the like, or if the contract is possible, is notified to the user by telephone or other means,
The user may go to a store of a credit company, and credit contract information may be given to the mobile station 100 by a dedicated ROM reader / writer installed there.

[B-2. Modification example when changing credit contract]
The contents of the change in the credit contract include, in addition to the above-mentioned name change and address change, various changes such as, for example, a

credit limit change and a card grade change (for example, a change from a normal credit card to a gold card). Can be considered. In such a case, in addition to the above-described operation steps, a step of examination by a credit company, a step of notifying (impossible) change from the credit server 60 to the mobile station 100 based on the result of the examination, and the like are necessary. Becomes

[B-3. Modification when mobile station 100 and credit use are prohibited] The mobile station 100 transmits transmission information not only when the power is turned on, but also various other timings can be considered. For example, the mobile station 100
May request the call service or the packet communication service from the mobile communication network, or the mobile station 100 may start the process of using the credit at the store. That is,
As long as the mobile station 100 is set to transmit outgoing information in response to a certain operation by the person holding the mobile station 100, any operation may be used as the trigger. Alternatively, the mobile station 100 may constantly or periodically transmit the transmission information while the power is on.

[0212] When the use prohibition information is registered in the control station 33, the control station 33 or the like may call the mobile station 100 related to the use prohibition and give the use prohibition information to the mobile station 100. On the other hand, when the mobile station 100 receives the use prohibition information, it transmits a reception confirmation signal, and the control station 33 confirms that the mobile station 100 has received the use prohibition information by receiving the reception confirmation signal. Further, the control station 33 may always transmit the above-mentioned use prohibition information to each jurisdiction area via many base stations 32. And
The mobile station 100 that has received the transmitted use prohibition information
May perform a credit function use prohibition process.

[0213] The control station 33 may have only the communication use prohibition information of the mobile station 100 and only give the mobile station 100 the communication use prohibition information. Then, the mobile station 100 that has received the communication use prohibition information may perform the credit use prohibition process by determining that not only the use of communication but also the use of credit is prohibited.

[B-4. Modification of Configuration of Gateway Server 32, Credit Server 60, and Store Server 80] In the above description, the credit server 60A,
60B ... and the store server 80 are connected to the Internet 7
In addition to those connected to 0, it may be connected to the gateway server 32 via a dedicated line, or provided inside a mobile communication network.

IPR2025-00645 Page 01805

[B-5. Modification of Role Allocation of Gateway Server 32, Credit Server 60, and Store Server 80] Gateway Server 32, Credit Server 60
The functions of each of the user server 80 and the store server 80 are not limited to the above-described embodiments. For example, various functions such as the gateway server 32 acting as a part of the functions of the store server 80 and the credit server 60 may be used. Is possible. An example will be described below.

Are not stored by the credit servers 60A, 60B,... As in the above-described embodiment at the time of a credit contract or change, but by the gateway server 32.
Information may be stored. Thereby, when a contract request or a change request is transmitted from the mobile station 100 to the gateway server 32, the gateway server 32 does not need to access the credit servers 60A, 60B,.
Input screen information and the like can be provided to the mobile station 100.

The credit servers 60A, 60B
Does not perform the examination for judging whether or not the credit contract is acceptable, but the gateway server 32 may perform the examination. For this purpose, the gateway server 32 stores contract availability determination conditions given in advance from each of the credit servers 60A, 60B,... For each credit company, and conducts an examination in accordance with those conditions.

The gateway server 32 may have a contract update candidate user file 601. In this case, the gateway server 32
From 0A, 60B, etc., the contract update candidate user file 6
01, and the subsequent processing with the mobile station 100 is performed based on the given contract update candidate user file 60.

In the above-described embodiment, the gateway server 32 has the credit servers 60A and 60B.
(For example, credit contract information and various notifications) are temporarily stored, and an information reception notification is transmitted to the mobile station 100. Then, in response to the notification, the mobile station 100
When there is a credit contract information acquisition request from, the gateway server 32 gives the mobile station 100 the credit contract information and the like.
However, this need not be the case. For example, gateway server 3
2 receives any information destined for the mobile station 100 from the credit servers 60A, 60B,... Without transmitting any information to the mobile station 100 in advance (or at the same time as notifying the mobile station 100). 100 may be given. In this case, the mobile station 100 is
When the gateway server 32 receives the information from the mobile station 100, the gateway server 32 confirms that the mobile station 100 has received the information by receiving the reception confirmation signal.

In the embodiment of the credit shopping using the mobile packet communication network 30, the input information transmitted by the mobile station 100 is received by the store server 80 via the gateway server 32, and the store Although the server 80 transmits the credit contract information and the usage amount information to the credit server 60 from the input information, this is not always necessary. For example,
The gateway server 32 classifies the content of the input information into a destination for the store server 80 and a destination for the credit server 60,
Each may be transmitted separately. That is, the gateway server 32 transmits the merchandise information from the input information to the store server 80, and transmits the credit contract information and the usage amount information to the credit server 60. Then, the credit availability information from the credit server 60 may be provided to the mobile station 100 via the store server 80, or may be directly provided from the credit server 60 to the mobile station 100 and the store server 80, respectively. . Further, the gateway server 32 may store a shopping screen, and when a request is received from the mobile station 100, the stored shopping screen may be given to the mobile station 100.

[B-6. Kind of Subscription Contract] In the above embodiments, the credit contract was described as a subscription contract, but the present invention is not limited to the credit contract, and other subscription contracts may be used. For example, it may be a deposit or loan contract with a financial institution, an insurance contract with an insurance company, or a membership contract for becoming a member of various organizations.

[B-7, Mobile Station 100 and CAT Terminal 4
Modification 0] [B-7-1, First Modification] The mobile station 100 transmits the credit contract information to the CAT terminals 40a and 40 using a barcode.
b ... may be given. FIG. 17 is a block diagram illustrating a configuration of the mobile station 100 that displays a barcode indicating credit contract information on the liquid crystal display 132. The mobile station 100 includes a user interface 13 having a transmitting / receiving unit 110, a control unit 120, and a liquid crystal display 132.
0, a data input / output terminal 140 and the like. The control programs stored in the program ROM 122 include:
A barcode creation program for creating barcode data indicating credit contract information is included. CPU 12
1, when it is necessary to display the credit contract information, it reads the credit contract information from the credit ROM 123 and creates barcode data indicating the credit contract information according to a barcode creation program.
The information is displayed on the liquid crystal display 132.

On the other hand, the CAT terminals 40a, 40b,.
is equipped with a bar code reader, and can read a bar code displayed on the liquid crystal display 132 of the mobile station 100. FIG. 18 is a block diagram illustrating a configuration of the CAT terminal 40 including the barcode reader. The CAT terminal 40 includes a user input interface 41,
A transmitting / receiving unit 42, an output interface 43, a control unit 44,
it comprises a barcode reader 45 and the like. Control unit 44
Controls each unit of the CAT terminal 40. The user interface 41 is for a clerk or the like to input a usage amount or the like. The barcode reader 45 reads a barcode displayed on the liquid crystal display 132 of the mobile station 100. The transmission / reception unit 42 exchanges various data with the CAFIS network 50. The output interface 43 is a credit slip printing device or the like. Other configurations and operations are the same as those of the first embodiment. What is displayed on the liquid crystal display 132 only needs to be optically readable, and may be, for example, a color code, a peri code, or the like.

[B-7-2. Second Modification] Mobile Station 100
May give credit contract information to the CAT terminals 40a, 40b,. FIG.
is a block diagram showing a configuration of the mobile station 100 that gives credit contract information to the CAT terminals 40a, 40b,... By infrared communication.
The mobile station 100 includes a transmitting / receiving unit 1
10, control unit 120, user interface 130, data input / output terminal 140, modulation unit 170, infrared radiation unit 1
80 and the like. When it is necessary to provide the credit contract information to the CAT terminals 40a, 40b,..., The CPU 121 reads the credit contract information from the credit ROM 123 and supplies the read credit contract information to the modulation unit 170. The modulation unit 170 modulates the infrared carrier with a signal wave corresponding to the given credit contract information, and
Give to 80. Infrared radiating section 180 radiates a given infrared ray.

Are provided with an infrared receiving unit and a demodulating unit. The CAT terminals 40a, 40b,... Receive the infrared rays radiated from the infrared radiating unit 180 of the mobile station 100, demodulate them, and transmit Can be obtained.
FIG. 20 is a block diagram illustrating a configuration of the CAT terminal 40 including the infrared receiving unit and the demodulating unit. This CAT terminal 4

IPR2025-00645 Page 01806

5 is a user input interface 41, a transmitting / receiving unit 42,
Output interface 43, control unit 44, infrared receiving unit 4
6, a demodulation unit 47 and the like. Other configurations and operations are the same as those of the first embodiment.

[B-7-3. Third Modification] Also, mobile station 1
00 may give credit contract information to the CAT terminals 40a, 40b,... Via existing data input / output terminals. FIG. 21 shows that the CAT terminals 40a, 40b,.
FIG. 3 is a block diagram showing a configuration of a mobile station 100 given to the mobile station 100. The mobile station 100 includes a transmitting / receiving unit 110, a control unit 12
0, user interface 130, data input / output terminal 1
40 and the like. When it is necessary to provide the credit contract information to the CAT terminals 40 a, 40 b,..., The CPU 121 reads the credit contract information from the credit ROM 123 and supplies the credit contract information to the data input / output terminal 140. The data input / output terminal 140 transmits the given credit contract information to the CAT terminals 40a, 40b,.
Is provided to the data input / output terminal.

FIG. 22 shows a CA having data input / output terminals.
FIG. 2 is a block diagram illustrating a configuration of a T terminal 40. This CAT
The terminal 40 includes a user input interface 41, a transmission / reception unit 42, an output interface 43, a control unit 44, a data input / output terminal 48, and the like. Other configurations and operations are the same as those of the first embodiment.

[B-7-4. Other Modifications of Mobile Station 100 and CAT Terminal 40] In the above description of mobile station 100 having a magnetic stripe, mobile station 100 has only one magnetic stripe 160, and magnetic stripe 160 Writer 150 writes credit contract information every time a credit is used,
It does not have to be. For example, magnetic card 1
A plurality of magnetic stripes 160 are provided on 61, and one magnetic stripe may correspond to one credit contract. That is, the magnetic stripes 160 are provided by the number of credit contracts. In this case, the CAT terminals 40a, 40b,.
Reads the magnetic stripe 160 in which the card information of the designated credit company is stored among the plurality of magnetic stripes 160.

[0229] When the user performs credit shopping only using the above-mentioned mobile packet communication network,
The mobile station 100 does not need to include the magnetic stripe 160 or the like. This is because in credit shopping using the mobile packet communication network, data can be exchanged with the credit servers 60A, 60B,... Only by the wireless communication function.

In the above description, the mobile station (so-called cellular, PHS, etc.) has card information of a credit card.
The mobile communication terminal is not limited to the mobile station 100 alone, and may be a mobile communication terminal without a telephone function (for example, a PDA).

In the above description, the CAT terminals 40A, 40B,...
00 may be given. For example, at the time of credit shopping, the CAT terminals 40A, 40B,.
Has information such as the date of use, the store used, the amount of use, etc. relating to credit shopping, and the information is stored in the mobile station 1.
00 may be given. Then, the mobile station 100 can accumulate the credit use history or calculate the credit debit amount based on the credit use history without having to access the credit servers 60A, 60B,... . For that purpose, in each of the above embodiments, the CAT terminals 40a, 40b,.
May have a data input / output terminal connected to the data input / output terminal of the mobile station 100 and capable of providing the information.

[B-8. Modification of User Authentication] In the above-described embodiment, the password stored in advance in the gateway server 32 is compared with the password input by the user to the mobile station 100 in response to the packet communication start request. Is a form in which user authentication is performed, but this is not always necessary. For example, a password for user authentication may be stored in the mobile station 100 in advance. By doing so, the mobile station 100 can perform user authentication without communicating with the gateway server 32.

The credit server 60 may store a password (second password) separately from the password (first password) stored by the gateway server 32. In this case, when starting packet communication,
The first password verification is performed between the mobile station 100 and the gateway server 32, and the mobile station 100 is used for credit shopping and credit use history inquiry.

A second password check is performed between the password server and the credit server 60. As a result, higher privacy protection and higher security when using credit can be expected.

As described above, according to the present invention, it is possible to perform the contract processing more quickly without imposing a large burden on the user in the contract of various electronic commerce services

[Brief description of the drawings]

FIG. 1 shows a mobile station 10 used in an embodiment of the present invention.
FIG. 3 is a block diagram showing a configuration of a 0.

FIG. 2A is a perspective view showing an appearance of a mobile station 100 in a state in which a magnetic card 161 is stored, and FIG.
FIG. 9 is a perspective view showing an appearance in a state where a magnetic stripe 160 portion of the magnetic card 161 is exposed from the mobile station 100.

FIG. 3 is a block diagram showing a configuration of a credit system using the mobile station 100.

FIG. 4 is a block diagram showing a functional configuration of the gateway server 32.

5A is a diagram showing a configuration of a subscriber database 331, and FIG. 5B is a diagram showing a subscriber registration information file 3;
04 is a data format diagram of FIG.

6A is a diagram illustrating a configuration of a user database 61, and FIG. 6B is a diagram illustrating a credit database 62;
(C) is a diagram showing a configuration of a contract update candidate user file 601.

FIG. 7 is a flowchart showing an operation performed before a credit contract, a credit shopping using a mobile packet communication network, a credit contract change, a credit contract cancellation, and a credit use history inquiry operation.

FIG. 8 is a flowchart showing operations of the mobile station 100 and the credit system at the time of a credit contract.

IPR2025-00645 Page 01807

FIG. 9 is a diagram showing a screen displayed on the liquid crystal display 132 of the mobile station 100 at the time of a credit contract.

FIG. 10 is a flowchart showing the operation of the mobile station 100 and the credit system at the time of credit shopping at a store.

FIG. 11 is a flowchart showing operations of the mobile station 100 and the credit system during credit shopping using a mobile packet communication network.

FIG. 12 shows a mobile station 1 when renewing a credit contract.
It is a flowchart which shows operation | movement of 00 and a credit system.

FIG. 13 shows a mobile station 10 in changing a credit contract.
0 is a flowchart showing the operation of the credit system.

FIG. 14 shows a mobile station 10 when a credit contract is canceled.
0 is a flowchart showing the operation of the credit system.

FIG. 15 is a flowchart showing a flow of an operation of prohibiting use of the mobile station 100 and credits.

FIG. 16 is a flowchart showing a flow of an operation when inquiring a credit use history.

FIG. 17 is a block diagram showing a configuration of a mobile station 100 that displays a barcode indicating credit contract information on a liquid crystal display 132.

FIG. 18 is a CAT terminal 40 having a barcode reader.
FIG. 3 is a block diagram showing the configuration of FIG.

FIG. 19: Credit contract information is transmitted by infrared communication to C
FIG. 2 is a block diagram showing a configuration of a mobile station 100 provided to AT terminals 40a, 40b,...

FIG. 20 is a block diagram showing a configuration of a CAT terminal 40 having an infrared receiving unit and a demodulating unit.

FIG. 21 is a block diagram showing a configuration of a mobile station 100 that provides credit contract information to CAT terminals 40a, 40b,... Through existing data input / output terminals.

FIG. 22 shows a CAT terminal 40 having a data input / output terminal.
FIG. 3 is a block diagram showing the configuration of FIG.

[Explanation of symbols]

20 mobile telephone network, 30 mobile packet communication network, 31 base station, 32 gateway server, 33 control station, 40 CAT terminal, 50
..CAFIS network, 60 ... credit server, 61
... user database, 62 ... credit database, 70 ... internet, 80 ... store server, 100 ... mobile station, 101 ... throttle, 110 ... transceiver, 120 .. .Control unit, 12
1 ... CPU, 122 ... ROM for program, 1
23: ROM for credit, 124: RAM,
130: user interface, 131: card storage / exposure key, 132: liquid crystal display, 1
40: data input / output terminal, 150: magnetic writer, 160: magnetic stripe, 170: modulation unit, 180: infrared radiation unit, 301: control unit,
302 ... subscriber information management unit, 303 ... data distribution management unit, 304 ... subscriber registration information file, 33
1 ... subscriber database, 601 ... contract update candidate user file

----------続き Continued on front page F-term (reference) HH11 SK101 KK12 KK17 LL00 LL02
LL12 MM07 NN18 NN21 PP04 RR05 SS07 TT06

Patent Citations (12)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
WO1994007205A1 *	1992-09-18	1994-03-31	Kim, Soon, ik	Method for providing service on credit utilizing telephone lines
US5966699A *	1996-10-11	1999-10-12	Zandi, Richard	System and method for conducting loan auction over computer network
US5898783A *	1996-11-14	1999-04-27	Lucent Technologies, Inc.	System and method for employing a telecommunications network to remotely disable a SIM or smartcard
JPH10143570A *	1996-11-15	1998-05-29	Susumu Miyake	Electronic transfer method for individual information of credit card, and miniature ic card, adapter card, terminal adapter, slip issuing machine and portable terminal therefor
JPH10198729A *	1996-11-18	1998-07-31	Fujitsu Ltd	Contract application processing system, contract mediating device, and recording medium storing contract application processing system program
EP0956673A4 *	1996-12-20	2005-04-06	Financial Services Technology	Method and system for processing electronic documents
JPH10232897A *	1997-02-18	1998-09-02	Nippon Shinpan Kk	Credit card system
JPH10312437A *	1997-05-14	1998-11-24	Hitachi Ltd	Internet banking system

IPR2025-00645 Page 01808

JPH10327147A *	1997-05-21	1998-12-08	Hitachi Ltd	Electronic authenticating and notarizing method and its system
CN1246941A *	1997-08-13	2000-03-08	松下电器产业株式会社	Mobile electronic commerce system
US5940812A *	1997-08-19	1999-08-17	Loanmarket Resources, L.L.C	Apparatus and method for automatically matching a best available loan to a potential borrower via global telecommunications network
US6065120A *	1997-12-09	2000-05-16	Phone.Com, Inc.	Method and system for self-provisioning a rendezvous to ensure secure access to information in a database from multiple devices

* Cited by examiner, † Cited by third party

Cited By (23)

Publication number	Priority date	Publication date	Assignee	Title
JP2003122928A *	2001-10-10	2003-04-25	Inkurimento P Kk	System and terminal of insurance contract, and information recording medium
JP2004021311A *	2002-06-12	2004-01-22	Japan Telecom Co Ltd	Information processor and information processing method
JP2004213382A *	2002-12-27	2004-07-29	Japan Research Institute Ltd	Electronic image display device and method, and program for making computer implement this method
Family To Family Citations				
US7113299B2 *	2001-07-12	2006-09-26	Canon Development Americas, Inc.	Printing with credit card as identification
WO2003079250A1 *	2002-03-18	2003-09-25	Fujitsu Limited	Card issuing system
US20040128239A1 *	2002-09-10	2004-07-01	Thami Smires	Method and apparatus for conducting transactions generated at point-of-sale locations
WO2005119607A2 *	2004-06-03	2005-12-15	Tyfone, Inc.	System and method for securing financial transactions
US20050269401A1 *	2004-06-03	2005-12-08	Tyfone, Inc.	System and method for securing financial transactions
GB2410113A *	2004-11-29	2005-07-20	Morse Group Ltd	A system and method of accessing banking services via a mobile telephone
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060226217A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card
KR100772859B1 *	2005-08-18	2007-11-02	삼성전자주식회사	Multi-user computer system and remote control method for the same
KR101379861B1 *	2006-10-20	2014-04-17	삼성전자주식회사	Apparatus, system and method for providing DRM
US7991156B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US7930249B2	2007-07-11	2011-04-19	Qualcomm Incorporated	Mobile wireless financial instrument for automatically selecting a payment instrument
US8938793B2 *	2007-10-03	2015-01-20	Gmx Sas	System and method for secure management of transactions
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
CN101939947B *	2008-02-29	2013-01-09	三菱电机株式会社	Key management server, terminal, key sharing system, key distribution program, key reception program, key distribution method, and key reception method
US8485112B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US8224375B2	2009-05-01	2012-07-17	Qualcomm Incorporated	Proximity purchase ringtones
JP5705899B2	2013-03-22	2015-04-22	株式会社アイキューブドシステムズ	Mobile terminal, information management system, information management method and program

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title

KR100554695B1	2006-02-22	Mobile communication terminal
KR100446480B1	2004-08-30	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
JP2001167187A	2001-06-22	Subscription contract mediation method and mobile communication network
US8583499B2	2013-11-12	System for secured transactions over a wireless network
KR20010100380A	2001-11-14	Method and apparatus for paying a charge of goods or service using a mobile phone
KR20000037471A	2000-07-05	bill-payment service method, and system for the same
EP1760649B1	2011-12-21	Method and system for electronic commerce
JP2001168980A	2001-06-22	Method for inhibiting use of mobile communication terminal, mobile communication network and mobile communication terminal
JP4071445B2	2008-04-02	Transaction mediation system, transaction mediation apparatus and program
JP2001237989A	2001-08-31	Charging acting system to owner of information display type portable telephone
CA2549387C	2012-01-24	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
JP2003069753A	2003-03-07	Communication rate processing method and managing server
JP2001169357A	2001-06-22	Mobile communication terminal and card information reader

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP35226599A	1999-12-10	1999-12-10	Subscription contract mediation method and mobile communication network

Applications Claiming Priority (53)

Application	Filing date	Title
JP35226599A	1999-12-10	Subscription contract mediation method and mobile communication network
CN200710128230.6A	2000-12-07	Mobile communication network for disabling mobile communication terminal equipped with memory for storing card information
HU0105484A	2000-12-07	Electronic commerce contract mediation method and mobil communication network
PCT/JP2000/008654	2000-12-07	Mobile communication terminal and card information reader
KR1020017010147A	2000-12-07	Mobile communication terminal and card information reader
US09/890,830	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
KR1020017010145A	2000-12-07	Electronic commerce contract mediation method and mobile communication network
AU17329/01A	2000-12-07	Mobile communication terminal and card information reader
CNB008083690XA	2000-12-07	Mobile communication terminal and card information read device
IL144746/00A	2000-12-07	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
BR0009958-9A	2000-12-07	Improvement in mobile terminal and credit card information reader
BR0008082-9A	2000-12-07	Improvement in method to disable a mobile communication terminal equipped with memory for the storage of credit card information, mobile communication network and mobile communication terminal
US09/868,477	2000-12-07	Electronic commerce contracts mediating method and mobile communication network
CN200410099883.7A	2000-12-07	Mobile communication terminal
AU17330/01A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
AU17327/01A	2000-12-07	Electronic commerce contract mediation method and mobile communication network
US09/890,910	2000-12-07	Mobile communication terminal and card information reading device

IPR2025-00645 Page 01810

CA002356357A	2000-12-07	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
HU0105368A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
EP0979968A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
IL144747A	2000-12-07	Mobile communication terminal and card information reading device
CA 2356361	2000-12-07	Electronic commerce contract mediation method and mobile communication network
BR0007805A	2000-12-07	Improvement in the method of intermediation of electronic commerce contracts and mobile communication network
KR1020047019020A	2000-12-07	Mobile communication terminal
PL34926000A	2000-12-07	Electronic commerce contract mediation method and mobile communication network
PL34926400A	2000-12-07	Method of immobilising a mobile communication terminal provided with a card information storing memory, mobile communication network and mobile communication terminal
KR10-2001-7010146A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
BR0008000A	2000-12-07	Improvement in portable telephone and terminal equipment
EP20000979965	2000-12-07	Electronic commerce contract mediation method and mobile communication network
EP0979967A	2000-12-07	Mobile communication terminal and card information reader
PCT/JP2000/008655	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
IL144584A	2000-12-07	Electronic-commerce contracts mediating method and mobile communication network
CA002356371A	2000-12-07	Mobile communication terminal and card information reading device
PL34925700A	2000-12-07	Mobile communication terminal and card information reader
HU0200051A	2000-12-07	Mobile communication terminal and card information reader
CA2549387A	2000-12-07	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
CN00803692A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
PCT/JP2000/008652	2000-12-07	Electronic commerce contract mediation method and mobile communication network
CNB008036950A	2000-12-07	Electronic business contract adjusting method and mobile communication network
TW089126278A	2000-12-08	Mobile communication terminal and card information reader
TW089126273A	2000-12-08	Operation denial method, mobile communication network and mobile communication terminal for mobile terminal equipped with memory card of data memory
TW89126275A	2000-12-08	Brokerage method for electronic commerce contract and mobile communication network
IL144584A	2001-07-26	Electronic-commerce contracts mediating method and mobile communication network
NO20013734A	2001-07-30	Mobile communication terminal and card information reader device
NO20013732A	2001-07-30	Procedure for electronic communication of trade contracts and mobile communication networks
NO20013733A	2001-07-30	Communication network to block a mobile communication terminal said like a mobile phone
IL144746A	2001-08-06	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
IL144747A	2001-08-06	Mobile communication terminal and card information reading device
HK02103108.1A	2002-04-24	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
HK02103103.6A	2002-04-24	Mobile communication terminal and card information reader
HK02105886.4A	2002-08-12	Electronic commerce contract mediation method and mobile communication network
US10/689,810	2003-10-21	Mobile communication terminal and card information reading device
US11/026,735	2004-12-30	Mobile communication terminal and card information reading device

IPR2025-00645 Page 01811

Legal Events

Date	Code	Title	Description
2004-01-05	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20031226
2004-03-30	A02	Decision of refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A02 **Effective date:** 20040330

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

IPR2025-00645 Page 01812

Patents CN1218276C

IC card

Abstract

The present invention relates to a multifunctional IC card (MFC) which has compatibility with a multimedia card, an SD card, etc. The compatibility comprises that connecting terminals (from #1 to #13) are configured into two rows on a base plate (1) in a tortuous mode; moreover, multifunctional installation is realized and is represented by that a memory card unit (3) and an SIM card unit (4) are respectively connected and installed on the presetting terminals of the connecting terminals (from #1 to #13); the memory card unit (3) and the SIM card unit (4) respectively and independently have areas used for saving safe secret codes. In this way, one IC card can realize multifunctional devices with different safety levels. Because a multi-line layout which corresponds to the distribution of the tortuous mode is adopted, a card inserting port can adopt a correspondingly simple structure, wherein the number of the convex points of the terminals of the card inserting port can be combined with a tortuous part to alternately change. The terminals of the card inserting port are integrally configured in parallel in a line.

Classifications

⩙ G06K19/0719 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e.g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips at least one of the integrated circuit chips comprising an arrangement for application selection, e.g. an acceleration sensor or a set of radio buttons

View 8 more classifications

CN1218276C

China

Download PDF Find Prior Art Similar

Other languages: Chinese

Inventor: 西泽修孝, 石原雅次, 浅川洋介, 白石敦

Current Assignee : Hitachi Ltd , Hitachi Solutions Technology Ltd

Worldwide applications

2000 CN WO JP CN EP US TW 2003 US 2006 US 2009 US

Application CN008194769A events

2000-04-28	Application filed by Hitachi Ltd, Hitachi ULSI Systems Co Ltd
2000-04-28	Priority to PCT/JP2000/002823
2003-10-29	Publication of CN1452763A
2005-09-07	Application granted
2005-09-07	Publication of CN1218276C
2020-04-28	Anticipated expiration
Status	Expired - Fee Related

Info: Patent citations (52), Cited by (135), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (5)

Hide Dependent

1. IC-card is characterized in that it being the IC-card with splicing ear of first functional block that is made of SIC (semiconductor integrated circuit) and second functional block and a plurality of exposures,

Described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrangement between the terminal of the splicing ear in first row and the row that are arranged between the terminal of the splicing ear in secondary series upwards are shifted mutually

Described splicing ear comprises first splicing ear that is connected to and is exclusively used in first functional block, is connected to and is exclusively used in second splicing ear of second functional block, and the 3rd splicing ear of sharing the shared operation power supply of first functional block and second functional block,

Splicing ear on the end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear to be pressed close to be disposed in described first row and is positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction, and

Splicing ear on the other end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear and presses close to be disposed in described first row and be positioned at the position of splicing ear of the other end that extends at column direction of its splicing ear at column direction.

2. as the IC-card in the claim 1, wherein said first functional block is the first storage card unit, comprise electrically rewritable first nonvolatile memory, with one first controller, described first controller is according to carrying out the access control of described first nonvolatile memory from the instruction of described first splicing ear and carrying out by the control of described first splicing ear with the interface in the external world

Wherein said second functional block is the second storage card unit, comprise electrically rewritable second nonvolatile memory, with one second controller, described second controller is according to carrying out the access control of described second nonvolatile memory from the instruction of described second splicing ear and carrying out by the control of described second splicing ear with the interface in the external world.

3. as the IC-card in the claim 2, wherein said first controller has function of keeping secret, to writing the data encryption in described first nonvolatile memory and carry out other encryptions to the data decryption read from described first nonvolatile memory or to data,

IPR2025-00645 Page 01813

And described second controller has function of keeping secret, to writing the data encryption in described second nonvolatile memory and carrying out other encryptions to the data decryption read from described second nonvolatile memory or to data.

4. as the IC-card in the claim 2, wherein said first splicing ear comprises clock terminal and data terminal, described second splicing ear comprises clock terminal and data terminal, and described the 3rd splicing ear comprises supply voltage power supply terminal and ground voltage power supply terminal, and

Wherein said first storage card unit and the described second storage card configuration of cells become a parallel work-flow multiple bank storage unit.

5. IC-card is characterized in that it being to have first functional block that is made of SIC (semiconductor integrated circuit) and a splicing ear of second functional block and a plurality of exposures,

Described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrange and be arranged in upwards displacement mutually of row at the column direction of the terminal of the splicing ear that is arranged in secondary series at the column direction of the splicing ear that is arranged in first row

Described splicing ear comprises first splicing ear that is connected to and is exclusively used in described first functional block, be connected to and be exclusively used in second splicing ear of described second functional block, and the 3rd splicing ear of sharing the shared operation power supply of described first functional block and second functional block

Described the 3rd splicing ear comprises the splicing ear that is positioned at first row and is used for supply voltage power supply, and provide and the corresponding splicing ear in secondary series so as and power supply power supply splicing ear adjoining position have terminal to the zone between terminal

Description

integrated circuit card

Technical field

The present invention relates to the expansion of the maintenance of the compatibility in the IC-card and function thereof, and relate to a kind of, such as, can under the condition that keeps with the multimedia card compatibility, effectively be applied to IC-card and be used for carrying out multiple bank (multibank) or multi-functional technology.

Background technology

Consider between cell phone and digital network equipment or similar devices and carry out information transmission, proposed a kind of storage card that dimensional weight reduces and interface is simplified of similar multimedia card.As, described in " interface " (in Dec, 1999 distribution) of publishing such as, CQ publishing company. multimedia card has 7 splicing ears as the external interface terminal and adopt serial ports.Compare with the ata interface that PC card or hard disk adopt, this can reduce the load of main system, and even also can obtain for fairly simple system.In addition, same list of references is also mentioned, and has proposed the storage card of a kind of SD card as the top compatibility of multimedia card.

The inventor once discussed the storage system IC-card, as multimedia card or similar card, the function expansion.Like this, the inventor has declared this invention before this: can keep the compatibility to the standardized terminal arrangement of multimedia card or the like when extended terminal is provided, thereby can make function be expanded into possibility, enroll the number (Japanese Laid-Open Patent Application No.2000-18030) that increases data bit In addition, the inventor once discussed the multiple bank that is intended to realize to use this kind extended terminal or multi-functional.Among GSM (the special seminar of the mobile communication) mobile communication system of SIM (subscriber identification module) card that uses IC-card etc., such as, SIM card has a single-chip microcomputer or analog, but storing subscriber information and account information or the like, these informational needs are used for carrying out user's affirmation and security management and realization communication protocol, and set up Nonvolatile memory card, as flash memory.When attempting storage card, as multimedia card, when being applied to the cell phone of this kind gsm mobile communication system, except the SIM card inserting mouth, storage card also needs one to insert mouth Like this, the inventor finds, exists with the space factor room for improvement.In addition, the inventor finds, the difference of safe level come across in the canned data between storage card and the SIM card inevitably and therefore safe level be allowed to be inevitable as multifunctional different.

Summary of the invention

An object of the present invention is to provide a kind of IC-card, can carry out the compatibility that keeps preassigned that terminal is arranged as multiple bank or multi-functional and so on expanded function simultaneously.

Another object of the present invention provides a kind ofly can expand the different multi-functional IC-card of safe level.

Above-mentioned purpose of the present invention, other purposes and new feature can obtain understanding from description of the invention and accompanying drawing.

(1) a kind of IC-card according to the present invention is considered compatibility and function expansion thereof.About the compatibility of IC-card, upward compatibility and downward compatibility can keep.Upward compatibility, such as, be that downward IC-card can the insertion mouth of IC-card uses by inserting upwards.Downward compatibility, such as, be that IC-card can use by the insertion mouth that inserts downward IC-card.IC-card has first functional block and second functional block, and the formation of each all comprises SIC (semiconductor integrated circuit) and has wherein a plurality of splicing ears is the configurations that expose.

With regard to the compatibility of IC-card, a plurality of splicing ears are the tortuous multirows in front and back between the row that are configured as in adjacency observing from the IC-card direction of insertion.If take to be different from the expression of its tortuous configuration, then can be described as a plurality of splicing ears and have one and observe the arrangements of two row that form before and after being from the IC-card direction of insertion, and the terminal in the middle of splicing ear that is arranged in first row arrangement and of terminal area is arranged in secondary series splicing ear in the middle of terminal to displacement mutually on the direction that is arranged in row of terminal area.If tortuous layout is adopted another different expression, then can be described as a plurality of splicing ears and have one and observe the arrangements of two row that form before and after being from the IC-card direction of insertion, and the row of splicing ear that are arranged in first row to layout and the row of splicing ear that are arranged in secondary series to layout in upwards displacement mutually of row.

Because the corresponding multiple row layout of canonical form that the tortuous mode in the arrangement of employing and splicing ear forms can adopt simple relatively structure in card inserting mouth, wherein its a large amount of mouth terminals that insert replace configured in parallel, and the while, its teat quantity changed.The splicing ear of IC-card is arranged and is adopted the splicing ear that is exclusively used in IC-card to arrange as it is downwards On the other hand, arrange if the IC-card special function that will make progress is given another tortuous splicing ear, then this kind can use also by the feasible upwards IC-card of the insertion mouth that is installed on downward IC-card and can realize downward compatibility.

IPR2025-00645 Page 01814

With regard to the expanded function of IC-card, the splicing ear of IC-card comprises first splicing ear that is connected to and is exclusively used in first functional block, be connected to and be exclusively used in second splicing ear of second functional block, and the 3rd splicing ear of sharing the shared operation power supply of first functional block and second functional block.By the data terminal beyond the power supply or other are exclusively used in first functional block and second functional block respectively, can promote the realization of upward compatibility and downward compatibility.

When attempt realizes three generations's IC-card or the above IC-card of three classes compatible, be to have supposed following situation, the splicing ear of first IC-card is arranged by adopting as it is with the corresponding splicing ear row of first row, the special function of adding second IC-card simultaneously to is given and the corresponding splicing ear row of another tortuous secondary series, and the special function of adding the 3rd IC-card to give with the corresponding dedicated terminals row of first row and with the corresponding splicing ear row of secondary series.At this moment, consider the upward compatibility between second IC-card and the 3rd IC-card and the realization of downward compatibility.For this purpose, the structure of adopting is that the splicing ear on the end that extends on the column direction of the wherein splicing ear in being disposed at secondary series extends to splicing ear and presses close to be disposed in first row and be positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction, and the splicing ear on the other end that extends on the column direction of the splicing ear in being disposed at secondary series extends to splicing ear and presses close to be disposed in first row and be positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction.In view of the above, this first to the 3rd IC-card even the insertion mouth and the operable compatibility that can be inserted into other IC-cards mutually can realize at an easy rate.

(2) expansion of the function of this IC-card is intended to, such as, the multiple bank storer.At this moment, first functional block is the first storage card unit, comprise electricity and rewrite first nonvolatile memory, with one first controller, first controller is according to carrying out the access control of first nonvolatile memory from the instruction of first splicing ear and carrying out by the control of first splicing ear with extraneous interface.Second functional block is the second storage card unit, comprise electricity and rewrite second nonvolatile memory, with one second controller, second controller is according to carrying out the access control of second nonvolatile memory from the instruction of second splicing ear and carrying out by the control of second splicing ear with extraneous interface.

If place multimedia card under this kind environment or other to obtain considering, although the special function of each splicing ear is random, then first splicing ear comprises a clock terminal and data terminal, second splicing ear comprises a clock terminal and data terminal, and the 3rd splicing ear comprises supply voltage power supply terminal and ground voltage terminal.

The first storage card unit and the second storage card unit are configured to a parallel work-flow multiple bank storage unit.

In order to increase the safety of data that is stored in each nonvolatile memory, first controller can have function of keeping secret, can be to writing the data encryption in first nonvolatile memory and carrying out other encryptions to the data decryption read from first nonvolatile memory or to data, and second controller can have function of keeping secret, can be to writing the data encryption in second nonvolatile memory and carrying out other encryptions to the data decryption read from second nonvolatile memory or to data.

(3) expansion of the function of this IC-card is intended to multi-functional.At this moment, first functional block is first data processing unit, comprise first nonvolatile memory and one first controller, first controller is carried out the access control of first nonvolatile memory and is carried out by the control of first splicing ear with extraneous interface.Second functional block is second data processing unit, comprises second nonvolatile memory and one second controller, and second controller is carried out the access control of second nonvolatile memory and carried out by the control of second splicing ear with extraneous interface.First data processing unit and second data processing unit have respectively and are used for the zone of storing secret security code separately.

Like this, an IC-card just can be realized the multifunctional equipment that safe level is different.

First data processing unit even can secret identification code be write the secret identification code memory block in the nonvolatile memory production phase.Second data processing unit even can secret identification code be write the secret identification code memory block in the IC-card production phase.Like this, just can set secret identification code by keeping secret necessary method or step according to the difference of safe level.Such as, set the storage card unit that becomes a conventional data storage application when first data processing unit, and second data processing unit is set when becoming microcomputer SIM card unit, then the security of the second data processing unit processing/account executive information is compared with first data processing unit and will be kept strict inevitably, thereby can fully satisfy this kind requirement.

Even ought set the storage card unit that becomes a conventional data storage application by first data processing unit, first controller also preferably adopt can to write in first nonvolatile memory data encryption and to data decryption of reading from first nonvolatile memory or the function of keeping secret that data are carried out other encryptions, purpose is the validity that strengthens copyright protection of being stored in the data in the storage card unit or the like.

When storage card unit and SIM card unit or the like are used as multifunctional equipment, such as, first splicing ear comprises clock terminal, long numeric data terminal and 1 order of the bit terminal, second splicing ear comprises clock terminal, data terminal and reseting terminal, and the 3rd splicing ear comprises supply voltage power supply terminal and ground voltage power supply terminal.

(4) when the splicing ear of supply voltage power supply be disposed at the corresponding splicing ear row of first row of observing from the IC-card direction of insertion the time, be listed in the corresponding splicing ear of secondary series and form in abutting connection with the position of supply voltage power supply splicing ear and have terminal to terminal area.If with other splicing ears of supply voltage power supply terminal adjacency be disposed at the corresponding splicing ear row of the secondary series of winding form in, just might be to insert mouthful in IC-card inserts the process of card inserting mouth, to insert with the terminal of the corresponding card inserting mouth of other splicing ear will both contact the power supply splicing ear of powering before mouthful contacting other splicing ears and also contact other splicing ears that are positioned at other splicing ear fronts.If power supply or power supply insert a mouthful terminal and contact with the supply voltage power supply terminal under this state, with regard to worrying power supply to power supply short circuit.If adopt to guarantee the structure of terminal to terminal area, then can adopt increase with the corresponding splicing ear row of first and second row between distance and the device of the width of each splicing ear of shortening

According to above-mentioned requirements, the invention provides following four kinds of IC-cards.

A kind of IC-card, it is characterized in that it being IC-card with splicing ear of first functional block that constitutes by SIC (semiconductor integrated circuit) and second functional block and a plurality of exposures, described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrangement between the terminal of the splicing ear in first row and the row that are arranged between the terminal of the splicing ear in secondary series upwards are shifted mutually, described splicing ear comprises first splicing ear that is connected to and is exclusively used in first functional block, be connected to and be exclusively used in second splicing ear of second functional block, and the 3rd splicing ear of sharing the shared operation power supply of first functional block and second functional block, splicing ear on the end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear to be pressed close to be disposed in described first row and is positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction, and the splicing ear on the other end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear and presses close to be disposed in described first row and be positioned at the position of splicing ear of the other end that extends at column direction of its splicing ear at column direction.

IPR2025-00645 Page 01815

A kind of IC-card, it is characterized in that it being splicing ear with first processing unit and second processing unit and a plurality of exposures, wherein said a plurality of splicing ear comprises first splicing ear that is connected to and is exclusively used in described first processing unit, be connected to and be exclusively used in second splicing ear of described second processing unit, and the 3rd splicing ear of sharing the shared operation power supply of described first processing unit and described second processing unit, wherein said first processing unit is carried out the access control of first nonvolatile memory and is carried out by the control of described first splicing ear with the interface in the external world, wherein said second processing unit is carried out the access control of second nonvolatile memory and is carried out by the control of described second splicing ear with the interface in the external world, wherein said first processing unit uses first secret identification code of storing in a zone of described first nonvolatile memory, and wherein said second processing unit uses second secret identification code of storing in a zone of described second nonvolatile memory.

A kind of IC-card, it is characterized in that it being to have first functional block that constitutes by SIC (semiconductor integrated circuit) and the splicing ear of second functional block and a plurality of exposures, described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrange and be arranged in upwards displacement mutually of row at the column direction of the terminal of the splicing ear that is arranged in secondary series at the column direction of the splicing ear that is arranged in first row, described splicing ear comprises first splicing ear that is connected to and is exclusively used in described first functional block, be connected to and be exclusively used in second splicing ear of described second functional block, and the 3rd splicing ear of sharing the shared operation power supply of described first functional block and second functional block, described the 3rd splicing ear comprises the splicing ear that is positioned at first row and is used for supply voltage power supply, and provide and the corresponding splicing ear of secondary series so as and power supply power supply splicing ear adjoining position have terminal to the zone between terminal.

A kind of IC-card, it is characterized in that it being to have first functional block that constitutes by SIC (semiconductor integrated circuit) and the splicing ear of second functional block and a plurality of exposures, wherein said first functional block is carried out the access control to nonvolatile memory, wherein said second functional block is carried out the security control to enciphered data, and described splicing ear comprises first splicing ear that is connected to and is exclusively used in described first functional block, be connected to and be exclusively used in second splicing ear of described second functional block, and the 3rd splicing ear that described first functional block is provided the operation power supply.

Description of drawings

Fig. 1 illustrates one to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multi-functional IC-card according to of the present invention.

Fig. 2 is the illustrated example figure of tabulation that the splicing ear function of multi-functional IC-card is shown.

Fig. 3 is the planimetric map of virtual condition that the circuit installation surface of multi-functional IC-card is shown.

Fig. 4 is the rear view of virtual condition that the circuit installation surface of multi-functional IC-card is shown.

Fig. 5 illustrates the skeleton view of mobile phone appearance.

Fig. 6 illustrates the planimetric map that multi-functional IC-card is installed on the state in the card inserting mouth.

Fig. 7 illustrates the planimetric map that multi-functional IC-card is installed on the state in the card inserting mouth that multimedia card uses.

Fig. 8 is the functional block diagram of storage card unit.

Fig. 9 is the functional block diagram of SIM card unit.

Figure 10 is the functional block diagram that can use the mobile phone of multi-functional IC-card.

Figure 11 illustrates second to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multiple bank storage card according to of the present invention.

Figure 12 is the illustrated example figure of tabulation that the splicing ear function of the multi-functional IC-card among Figure 11 is shown.

Figure 13 illustrates the explanation diagrammatic sketch of power supply to the comparative example of the splicing ear arrangement of power supply short circuit takes place.

Embodiment

< multi-functional IC-card >

Fig. 1 illustrates one to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multi-functional IC-card according to of the present invention.

Be shown in the multi-functional IC-card MFC of Fig. 1 and multimedia card, SD card or the like compatible part and be that the splicing ear 2 (#1 to #13) of card substrate 1 is configured as two row of winding form and the multifunctional equipments that are achieved as follows, promptly storage card unit 3 is respectively only to be mounted for to be connected with the predetermined terminal of splicing ear 2 (#1 to #13) with SIM card unit 4.Label 5 expression connects leads, illustrates to be used for storage card unit 3 and SIM card unit 4 are connected to the general symbol(s) of the line figure, welding lead or the like of splicing ear 2.

Suppose that multi-functional IC-card MFC can be used for being installed on the mobile phone herein.Storage card unit 3 is configured as data-storage applications, and it has a nonvolatile memory, as electric erasing flash memory (its details is stated as follows) and a controller, and telephone book data, melody data of entering or the like is stored in wherein.The formation of SIM card unit 4 comprises a microcomputer that has onboard flash memory, is used for storing subscriber information and account information, and these information confirm for the user of the mobile phone of GSM etc. and user management is essential.

Seemingly be directly connected to storage card unit 3 and SIM card unit 4 though be shown in the splicing ear 2 of the #1 to #13 of Fig. 1, in fact the splicing ear 2 of #1 to #13 is positioned at the back side (terminal surface) of card substrate 1, the connection pads that is connected to its existing splicing ear by through hole or line pattern is the surface (installation surface) that is disposed at card substrate, and storage card unit 3 is connected with these connection pads with SIM card unit 4.

Multi-functional IC-card MFC is based on the size of multimedia card and meet following standard: its thickness is 1.4mm, and planar dimension is 24mm * 32mm.The splicing ear 2 that the card substrate 1 of multi-functional IC-card is configured as #1 to #13 is by resin substrate, as glass epoxy resin etc., on the terminal surfaces of the substrate of making on the plug-in card direction (on its longitudinal direction) observe configuration before and after two row adjacent to each other.

IPR2025-00645 Page 01816

The splicing ear 2 of #1, #2, #5 to #8 and #13 is connected to storage card unit 3, and #9, #11 and #12 are connected to SIM card unit 4, and the splicing ear 2 of power supply #3 that is used for powering and #4 be connected to storage card unit 3 and SIM card unit 4 both.

The splicing ear 2 of #1 to #7 has layout and the function based on the multimedia card standard respectively.General application of multimedia mode card of multimedia card and SPI (serial peripheral interface).The selection of operational mode is according to the state decision of predetermined terminal of when energising.The terminal function of multimedia card is shown in the row of 7 pins (1) among Fig. 2.Multimedia card pattern and SPI mode difference point are shown in the bracket.In the multimedia card pattern, #1 is as keeping terminal NC (open a way or be fixed in logical value " 1 "), #2 is as command terminals CMD (fill order input and and answer signal output), #3 and #6 are used separately as circuit ground voltage (ground connection) terminal Vss1 and Vss2, #4 is as supply voltage power supply terminal Vdd, #5 is as clock input terminal CLK, and #7 is as data input/output terminal Data.In SPI (serial peripheral interface) pattern, #1 selects terminal CS as chip, #2 is as the sub-Din of data input pin (being used for from main equipment to card input data and order), #3 and #6 are used separately as circuit ground voltage (ground connection) terminal Vss1 and Vss2, #4 is as supply voltage power supply terminal Vdd, #5 is as clock input terminal CLK, and #7 is as the sub-Dout of data output end (carry out and snap into the data of main equipment and the output of state from storage).The multimedia card pattern is the operational mode that is suitable for using simultaneously the system of a plurality of multimedia cards.In order to discern corresponding multimedia card, adopt with the multimedia card initial order and multimedia card is set card identification id (relative address) by not shown main equipment.The SPI pattern is suitable in the system of simple cheap most.The selection of multimedia card is carried out according to the chip select signal that offers the #1 splicing ear from main equipment.In any operational mode, the command execution that the controller of storage card unit 3 response main equipment provides to the access control of storage chip and to the control of the interface of main equipment.

The splicing ear 2 of #8 to #13 is as the extended terminal to multimedia card.The splicing ear 2 of #1 to #7 constitutes arranging with the corresponding splicing ear of first row of relative card substrate 1, and the additional splicing ear 2 of #8 to #13 constitutes and the corresponding splicing ear arrangement of second row, and this journey is positioned at the corresponding splicing ear of first row arranges the position of leaving.The size of the splicing ear 2 of #9 to #12 is identical with other splicing ears 2.The splicing ear 2 of #13 places first row and observes the position that an end of arranging at splicing ear extends to thoroughly close #7 from its orientation.Be positioned at first row with the corresponding splicing ear 2 of terminal #8 and observe to extend to partly and overlap and adjoining position with the #1 splicing ear that splicing ear is arranged from its orientation.Arrange with the corresponding splicing ear of first row and arrange, observe displacement mutually the capable layout of splicing ear from line direction with the corresponding splicing ear of second row.In other words, arranging and arrange with the corresponding splicing ear of second row with the corresponding splicing ear of first row is to be configured as meander-shaped.

4 bit patterns shown in the row of 9 pins (4) of the extended terminal of #8 to #13 in Fig. 2 are selected when being used for multi-functional IC-card MFC is effective terminal.In other words, when selecting 4 bit patterns, the terminal of #2 to #7 is endowed and the corresponding identical pattern of multimedia card pattern.In corresponding multimedia card pattern, be used as the terminal #1 that keeps terminal, as and the 4th corresponding data terminal Data3, additional terminal #8 and #9 be used separately as with second corresponding data terminal Data1 and with the 3rd corresponding data terminal Data2.With first corresponding data terminal Data0 corresponding to the terminal #7 identical with the multimedia card pattern.Like this, when multi-functional IC-card MFC was selected 4 bit patterns, the I/O of data was enabled with 4 bit parallels At this moment, consider #8 to #13 splicing ear 2 shape will with the splicing ear compatibility of SD card.The data terminal function of #8 to #13 can transposition in 4 bit patterns.4 bit patterns also can have the compatibility with the SD card.

The storage card unit 3 of multi-functional IC-card MFC disposes the backward compatible pattern to multimedia card.In other words, the controller in the storage card unit 3 has the SPI pattern of multimedia card or is similar to 1 bit pattern of multimedia card pattern, and uses 4 bit data terminal #1, #7, #8 and #13 to carry out 4 bit patterns of data I/O with 4 bit parallels.1 bit pattern is to allow the operational mode of multi-functional IC-card MFC as multimedia card.

Operational mode can respond the state of predetermined splicing ear or set from the state of predetermined splicing ear order input.When multi-functional IC-card MFC was installed on the card inserting mouth of multimedia card, terminal #8 and #13 became unsteady.Therefore, controller can detect terminal #8 and #13 or any one quick condition wherein (floating state) and multi-functional IC-card is set at 1 bit pattern when energising.When it is installed on have respectively with the special-purpose card inserting mouths of 9 splicing ears, 2 corresponding card inserting mouth terminals in the time, make the card inserting mouth terminal corresponding of terminal #8 and #9 importing card inserting mouth with it.Therefore, when energising controller detect from main equipment to both or any one special signal or order that provides terminal #8 and the #9 at least, thereby can set 4 bit patterns to multi-functional IC-card MFC.

Extended terminal #9 to #12 is respectively the dedicated terminals that is connected with SIM card unit 4.The formation of SIM card unit 4 comprises that has a built-in nonvolatile memory, as flash memory, single-chip microcomputer.#9 represents data input/output terminal I/O, and #10 represents not splicing ear, and #11 represents clock terminal CLK, and #12 represents reseting terminal.The operate power of SIM card unit 4 is through #3 ground terminal Vss and #4 power supply terminal Vdd supply.If mobile phone etc. provide the corresponding card inserting mouth of describing in the row with 13 pins in Fig. 2 of terminal arrangement, and multi-functional IC-card MFC is installed in the card inserting mouth, then storage card unit 3 and SIM card unit 4 independent operating mutually.If multi-functional IC-card MFC is connected with personal computer etc. through card adapter etc., then corrects on the storage card of telephone book data or the like in multi-functional IC-card MFC and can implement expeditiously.

The planimetric map of the virtual condition of the circuit installation surface among the multi-functional IC-card MFC shown in Figure 3, and in Fig. 4 the virtual condition of terminal surfaces.The splicing ear 2 that the card substrate 1 of multi-functional IC-card is configured as #1 to #13 is by resin substrate, as glass epoxy resin etc., arrange with 2 row on the terminal surfaces of the substrate of making, in (on its longitudinal direction) observation configuration before and after row adjacent to each other on the plug-in card direction.Connection pads 7 is formed on installation or the package surface correspondingly with splicing ear 2.Connection pads 7 is formed by the conductive pattern of aluminium, copper or copper or ferroalloy or the like respectively.Gold-plated or nickel plating or the like forms splicing ear 2 by the conductive pattern that makes aluminium, copper or copper or ferroalloy or the like.The electrical connection of connection pads 7 and splicing ear 2 makes the front and rear surfaces conducting of card substrate 1 by enforcements such as wire pattern on the not shown card substrate 1 and through holes.

Storage card unit 3 has, and such as, electrically rewritable flash memory 8 be used for controlling the controller 9 of flash memory 8, all is disposed on the installation surface of card substrate 1.Although be not particularly limited, flash memory 8 and controller 9 have independently semi-conductor chip formation respectively.Certainly, both can be made by a chip or together by forming different chips is bonded to each other.

Controller 9 is according to the read-write operation of the instruction control flash memory 8 that provides from the corresponding splicing ear 2 of outside warp.When considering data security, controller 9 can also further be configured as to have the enciphered data of making and writes flash memory 8 and the data of reading from flash memory 8 are implemented deciphering or to applying close function of keeping secret in fact.

Controller 9 has shape long on vertical or the vertical direction, extends along the orientation of splicing ear 2.In splicing ear 2 sides, controller 9 comprises a plurality of connecting interface terminal 9Pi, is connected with splicing ear 2 through connection pads 7 respectively, and in flash memory 8 sides, comprises that a plurality of memory interface terminal 9Pj are connected with flash memory 8.Flash memory 8 has a plurality of control unit interface terminal 8Pk and is connected with controller 9 in controller 9 sides.Connection pads 7 is connected to the connecting interface terminal 9Pi corresponding with it of controller 9 by welding lead 10.The memory interface terminal 9Pj of controller 9 is connected to the control unit interface terminal 8Pk corresponding with it of flash memory 8 by welding lead 11.Connecting interface terminal 9Pi has respectively and #1 to #8 and the corresponding terminal function of #13.Memory interface terminal 9Pj is respectively, such as, be used for controlling the terminal of flash memory 8, and corresponding with a plurality of terminals with following function, export, write enable signal as chip enable signal and

IPR2025-00645 Page 01817

export, order enable signal output, data I/O, the output of output enable signal, the output of ready/busy signal, reset signal to export or the like.Control unit interface terminal 8Pk is a plurality of terminals with following function, as chip enable signal input, write enable signal input, the input of order enable signal, data I/O, the input of output enable signal, the input of ready/busy signal, reset signal and import or the like.In addition, card substrate 1 comprises calibrating terminal 13, is connected with controller 9 and flash memory 8 by welding lead (wire pattern) 12.

SIM card unit 4 is connected with connection pads 7 corresponding to #9, #11 and #12 through welding lead 17A.The operation power supply supply of SIM card unit 4 is such as providing through welding lead 17B.A pair of welding lead with label 16 marks is the interface lead that is used for connecting controller 9 and SIM card unit 4.Welding lead is to allowing in storage card unit 3 and SIM card unit 4 intermediate conveyor information.

Card substrate 1 is installed on and is fixed in housing 14, and its installation surface is towards its inside.Installation surface has housing 14 to cover and protection, and its terminal surfaces exposes from housing 14.

Outer Fig. 5 that is shown in of mobile phone.Multi-functional IC-card MFC is installed in the card inserting mouth of determining in the side of mobile phone 20.

Fig. 6 illustrates multi-functional IC-card MFC to be installed on state diagram in the card inserting mouth 21.Card inserting mouth 21 has card inserting mouth terminal 22 at its back side, and card inserting mouth terminal 22 outstanding and corresponding splicing ears 2 combine.Because splicing ear 2 is arranged as two row of meander-shaped, the card inserting mouth terminal (22 (L)) that the card inserting mouth terminal 22 of the card inserting mouth 21 that its overhang is little (22 (S)) and its length are long can alternately change in meanders Can adopt a kind of fairly simple configuration, wherein card inserting mouth terminal 22 is whole parallel, and the overhang of card inserting mouth terminal 22 is changed.The contact of contact splicing ear 2 is corresponding to the tip portion (with the ● mark) of card inserting mouth terminal 22.

Fig. 7 illustrates multi-functional IC-card MFC and is installed on situation in the card inserting mouth 23 that multimedia card uses.Because the arrangement of the splicing ear 2 of the #1 to #7 of multi-functional IC-card MFC is based on multimedia card, multi-functional IC-card MFC can be installed in the card inserting mouth 23 that multimedia card uses so that even be complementary with the application of independent use storage card unit 3.Label 24 is represented the card inserting mouth terminal of card inserting mouth 23 respectively, and this card inserting mouth terminal can be connected with the splicing ear 2 of #1 to #7.

Fig. 8 is depicted as the functional block diagram of storage card unit 3.Controller 9 has an interface controller 30, flash controller 32, encrypting and decrypting circuit 33 and secure circuit 34.Interface controller 30 is connected to mobile phone 20 through splicing ear 2, thereby and the command decode that mobile phone 20 is provided so as to carry out to the general control of the inside of storage card unit 3 and to the control of the interface of mobile phone 20.Although be not specifically limited, this kind control program or state exchange steering logic provide in interface controller 30 inside.Control program can place in the flash memory 8.

Interface control is with equivalent through the interface control of splicing ear 2 based on multimedia card pattern or SPI pattern.The general control of the inside of storage card unit is comprised the authentication control that utilizes secure circuit 34 as the first step, as the encrypt/decrypt control to the I/O data of flash memory 8 in second step, and the access control of carrying out through the file memory to flash memory 8 of flash controller 32.

Access control is a kind of consideration, such as, with the sector be the control of compatibility of the basic file system of data management.In order to manage data or the file in 512 byte sector units, such as, the storage that utilizes electricity to rewrite flash memory 8 is arranged, the directorial area that its data field that to be divided into a sector be 512 bytes and each data field are provided with.Each directorial area comprises the information of indication sector user mode, such as, data of whether remaining valid with to the directional information of next sector in corresponding data field, or the like.Sector management table 35 of the whole composition of these directorial areas.When access control, the sector of the file of ready access combines with the corresponding physical address that its electricity is rewritten flash memory 8, and the result makes can carry out each storage operation, as reads, wipes, writes and verification or the like

Encrypting and decrypting control is carried out, such as, make encrypting and decrypting circuit 33 at first to the data encryption that writes flash memory 8 and allow enciphered data to write the process of flash memory 8, and make 33 pairs in encrypting and decrypting circuit utilize flash controller 32 to rewrite data decryption or the logarithm that flash memory 8 reads to execute another time encryption factually, and allow treated data to output to the outside from interface controller 30 from electricity.The encrypting and decrypting method can adopt the suitable algorithm of utilizing private key or private key and PKI.

The following describes authentication control.Supposing to use storage card unit 3 to wait by mobile phone 20 provides music information, literature information or the like, then preferably considers the copyright protection to these information When telephone number or the like is stored in the storage card unit 3 and uses, will require the secret protection of this kind information and executing.

Although copyright protection is not specifically limited, in the fabrication phase of electricity rewriting flash memory 8, the predetermined authentication codes of relevant right of duplicating is write electricity and rewrite in flash memory 8 specific regions.When information provided, the relevant authentication codes that duplicates right sent to mobile phone 20 or the like from main equipment.This is arranged in the authorization code admin table 36 of secure circuit 34.The information that combines with authorization code that provides, such as, flash memory 8 is downloaded and write to music information or the like.It is write memory address and combines with authorization code and be arranged in the authorization code admin table 36 of secure circuit 34.Afterwards, multi-functional IC-card MFC takes off and this time appends to one from mobile phone 20 and duplicates end device etc.Respond the request of access that this end device sends, the interface controller 30 of multi-functional IC-card MFC makes secure circuit 34 utilize authorization code admin table 36 to judge whether the file storage address that is intended to visit is the memory block that combines with authorization code in the authorization code admin table 36.When the memory block is when combining with authorization code, secure circuit 34 does not allow file access, rewrites predetermined pass between the authorization code of flash memory 8 and ties up to its fabrication phase and set up unless remain in the authorization code in the secure circuit 34 and write electricity.Authorization code admin table 36 can be rewritten nonvolatile memory by electricity and constitute.Authorization code admin table 36 can place interface controller 30 or flash memory 8.

In case secret cognizance code is from an equipment; such as; mobile phone; be set in the secret cognizance code admin table 37 of secure circuit 34, as relevant secret protection described; finish at each multi-functional IC-card MFC initialization procedure, when request was for the first time carried out read access to electricity rewriting flash memory 8, secure circuit 34 required the corresponding secret cognizance code of interface controller 30 inputs.Before outside input and secret cognizance code that secret cognizance code being arranged at secret cognizance code admin table 37 is consistent, the memory access that secure circuit 34 makes interface controller 30 stop to respond read request is controlled.Secret cognizance code admin table 37 can be rewritten nonvolatile memory by electricity and constitute Authorization code admin table 36 can place interface controller 30 or electricity to rewrite flash memory 8.

Fig. 9 illustrates the functional block diagram of SIM card unit 4.SIM card unit 4 can be by chip microcontroller, it comprises CPU (CPU (central processing unit)) 40, be used as the RAM (random access memory) 41 of the workspace of CPU 40, be kept for the ROM (ROM (read-only memory)) 42 of the running program or the like of CPU 40, be used for carrying out serial interface circuit (SIO) 43 and flash memory 44 the data I/O of outside.In gsm mobile communication system, SIM card unit 4 keeps the telephonist of GSM to support and the necessary user profile of authentication/management GSM user, as the user profile of store/manage about security, and generation/leading subscriber PIN (personal identity number) or the like.In addition, SIM card unit 4 keeps account information, and GSM serves information necessary, as cripetura dialing/target Fixed Dialing or the like.CPU 40 carries out these information is retained in the flash memory 44 also by using RAM 41 these information of management.The program that in RAM 42, keeps its execution.In addition, the SIM card unit 4 implements communication agreement implementation, file management and safety managements.Safety management is by using authentication codes, as user PIN, confirms the validity of user's use authority and the validity of using

IPR2025-00645 Page 01818

system.Though concrete authentication formality is not described in detail the authentication codes that GSM service provider serves with the man-to-man corresponding relation storage GSM to each user in advance in the flash memory 44 of SIM card unit 4 Use the authentication codes that is registered in advance in the SIM card unit 4 to come to consistent with the code in being input to SIM card unit 4 such as all calling judgements.Validity is to confirm according to this judged result.Also have the relation with accounting, and therefore the safe level of SIM card unit 4 is set usually than the safe level height of storage card unit 3.In multi-functional IC-card MFC, SIM card unit 4 and storage card unit 3 are endowed intrinsic splicing ear respectively as the data input/output terminal.So, to its secret identification code, as security information, read-write just can carry out independently.This makes can carry out different transaction mutually aspect safe level.In other words, allow the difference on the safe level as multi-functional difference.

Can use the functional block diagram of the mobile phone of multi-functional IC-card MFC shown in Figure 10.

Microphone 51 is caught and is grabbed sound and be transformed to digital audio signal as the analog audio signal and by A/D transducer 52, is input to data processor 53 then.Data processor 53 is carried out acoustic coding processes and channel encode-decode process or the like and is handled and export treated signal as sending signal as the layer to the digital audio signal that receives.Although do not specifically illustrate, can utilize DSP to carry out acoustic coding processing and channel coding/decoding processing.Although do not specifically illustrate, data processor 53 can be set up accelerator for channel coding and decoding device and sound coder-decoder therein.

By the transmission signal of data processor 53 generations, by, such as, GMSK modulation circuit 54 is modulated, and further is transformed to simulating signal by D/A transducer 55, sends from high frequency transmitting element (RF transmitting element) by antenna 57 again.

The signal that antenna 57 receives is received by high frequency receiving element (RF receiving element) 58 and is transformed to digital signal by A/D transducer 59, sends into data processor 53 afterwards.Data processor 53 is carried out Viterbi (Viterbi) decode procedures, and voice codec process or the like is to take out sound or audio signal and with its output.The Veterbi decoding process, voice codec process or the like is carried out by DSP or not shown accelerator.

The audio signal of these data processor 53 outputs is transformed to the analog audio signal by D/A transducer 60, is re-used as sound through loudspeaker 61 outputs.

Data processor 53 in the mobile phone 20 shown in Figure 10 comprises CPU (central processing unit) (CPU) 62, direct memory access controller (DMAC) 63, the ROM (read-only memory) (ROM) 64 of working procedure of maintenance CPU 62 usefulness or the like, be used as the random access storage device (RAM) 65 of the workspace of CPU 62, and input/output circuitry (I/O) 66, as input/output end port, serial ports etc.In the example of this mobile phone 20, although be not particularly limited, running program, as be used for the acoustic coding decode procedure of acoustic coding/decoding, system's control procedure of carrying out as the channel encode-decode process of layer process and by data processor 53 or the like remains among the ROM 64.The process that is used to DMAC 63 to set transmission controlled condition is implemented by being stored in ROM 64 corresponding running programs by CPU 62 execution.

Although be not particularly limited, input switch unit 70, display controller 71 and card interface controller 72 are connected to the I/O 66 of data processor 53.But input switch unit 70 comprises a large amount of input switches that function is specified input digit and character that passes through.Multi-functional IC-card MFC and data processor 53 middle interfaces that card interface controller 72 is implemented to be installed in the card inserting mouth 21 are controlled.Data processor 53 has carries out following control function: show suitably on LCD 75 that through display controller 71 state of mobile phone 20 is as sending telephone number, caller ID, communications status, cell voltage or the like

< multiple bank storage card >

Figure 11 illustrates second to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multiple bank storage card according to of the present invention.

Multiple bank storage card MBC shown in Figure 11 has with multi-functional IC-card MFC shown in Figure 1 and similarly arranges.The splicing ear 2 of #1 to #13 on the card substrate 1 is configured as 2 row of winding form.Storage card unit 3 is connected with the splicing ear 2 of #1 to #13 with 3A and forms the multiple bank storer of parallel running.Label 5 expression connects leads, illustrates to be used for storage card unit 3 and 3A are connected to the general symbol(s) of the line figure, welding lead or the like of splicing ear 2.

Storage card unit 3 is connected to the splicing ear 2 of #1 to #8 and #13 and has the configuration same with the storage card unit 3 of multi-functional IC-card MFC shown in Figure 1.Like this, storage card unit 3 can use as the multimedia card shown in 7 pins among Figure 12 (1 's) the row in mode described above.In addition, the similar mode of SD card that illustrates during storage card unit 3 can be listed as with 9 pins (4) with Figure 12 is carried out the I/O operation of 4 bit parallel data.When being connected to card inserting mouth as mentioned above, its operational mode is determined according to the state of splicing ear 2.As mentioned above, the multimedia card pattern and with the SPI pattern of the operational mode of multimedia card compatibility according to to by main equipment the appointment during to 3 initialization of storage card unit determine.

Storage card unit 3A only has as the function that can carry out based on the storage card of 1 bit serial I/O of multimedia card.The power supply of storage card unit 3A has ground voltage Vss1, supply voltage Vdd and ground voltage Vss2, and from #3, #4 and #6 share with storage card unit 3.In the multimedia card pattern, #9 is as keeping terminal NC-2 (open a way or be fixed in logical value " 1 "), #10 is as command terminals CMD-2 (being used for fill order input and answer signal output), and #11 is as clock input terminal CLK-2, and #12 is as data input/output terminal Data-2.In the SPI pattern, #9 selects terminal CS-2 (negative logic) as chip, #10 is as the sub-Din-2 of data input pin (being used for from main equipment to card input data and order), #11 is as clock input terminal CLK-2, and #12 is as the sub-Dout-2 of data output end (carry out and snap into the data of main equipment and the output of state from storage).As mentioned above, multimedia card pattern and SPI pattern according to to by main equipment the appointment during to the 3A initialization of storage card unit determine.

When multiple bank storage card MBC shown in Figure 11 is installed on as shown in Figure 6 the card inserting mouth with 13 card inserting mouth terminals 22 21 so that during with host device interface, can introduce the operational mode of storage card unit 3 and 3A when two storage card unit 3 and 3A concurrent working respectively, at first be to be used for the both is set at the multimedia card pattern in the multimedia card compatibility mode in 13 pins (A) row that are shown in Figure 12 or the form of SPI pattern.Secondly, as shown in 13 pins (B) row of Figure 12, operational mode is to be used for that storage card unit 3 is set at the form of the pattern that can carry out 4 bit parallel I/O and to be used for the form of the multimedia card pattern in the multimedia card compatibility mode that storage card unit 3A is set at.In all case, main equipment can controlling packet be contained in the IC-card mutually independently two storage card unit 3 and 3A, and even can make its parallel running fully.

< prevent that power supply is to power supply short circuit >

In multi-functional IC-card MFC shown in Figure 1 and multiple bank storage card MBC shown in Figure 11, the power supply of the arrangement of two row splicing ears 2 is to power supply short circuit before and after having considered to prevent.In above-mentioned example, there is not terminal at rear portion with the corresponding #4 terminal of power connector end.When splicing ear 2 was configured as winding form shown in Figure 6, short terminal 22 (S) in the card inserting mouth terminal 22 of card inserting mouth 21 and long terminal 22 (L) were alternately configurations thick and fast, each spacing equal each splicing ear 2 spacing 1/2.On the other hand,

IPR2025-00645 Page 01819

if the rear portion does not have splicing ear 2 to exist, as occasion, then at the not long card inserting mouth terminals 22 in both sides (L) of the card inserting mouth terminal 22 (Vdd) of the splicing ear 2 of the #4 that is equivalent to be used to provide supply voltage (Vdd), as shown in Figure 6 at #4.

Suppose IC-card 25, contrast illustrates as Figure 13 (A), and the rear portion that the data terminal of #10 and #11 is disposed at #4 is used to provide supply voltage (Vdd).With IC-card 25 corresponding card inserting mouths 26 in, long card inserting mouth terminal 26Ab is disposed at the adjoiner with the corresponding card inserting mouth terminal of the splicing ear of #4 26Aa

When the IC-card 25 of Figure 13 inserts card inserting mouth 26, the superficial sliding contact of the splicing ear of the splicing ear of the #4 of the contact point of card inserting mouth terminal 26Ab (with the position of ■ mark) and input supply voltage Vdd and the #3 of input circuit ground voltage Vss is shown in Figure 13 (B).At this moment, when the splicing ear conducting of card inserting mouth terminal 26Aa that has supply voltage Vdd and #4 and have the card inserting mouth terminal 26Ac of circuit ground voltage Vss and during the splicing ear conducting of #3, supply voltage Vdd and ground voltage Vss are through the contact point short circuit of contact point and #3 and the 26Ac of contact point, #4 and the 26Ab of 26Aa, shown in Figure 13 (C).

Because, as shown in Figure 6, there is not splicing ear at rear portion with the terminal of the corresponding #4 of power connector end, the possibility of this kind power supply short circuit can prevent from can not take place.

Though the inventor is the specific embodiment shown in the basis to the description of the invention described above, the invention is not restricted to this.In the scope that does not break away from spirit of the present invention, can carry out various changes to it.

Such as, the present invention even can be applicable to get rid of the storage card of the outside standard of multimedia card, such as, based on the IC-card of other standards, as pocket flash memory or the like.Therefore, the function of the number of the size of card substrate, splicing ear and splicing ear all is not limited to above-mentioned and can suitably changes The storer that is installed to IC-card of the present invention is not limited to nonvolatile memory.Storer can be volatile memory (SRAM, DRAM or the like).Nonvolatile memory is not limited to flash memory and can makes ferroelectric memory.

The present invention can be used as IC-card and is applied to as GSM mobile handset, and other personal digital assistants.The present invention also can be used as the multiple bank IC-card and is widely used in the auxilary unit in digital camera, digital static camera and other electronic installations.In addition, the function of bank book, credit card, IC-card or the like also can combine as the function of multi-functional IC-card with memory function.

Patent Citations (52)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US3934122A *	1974-08-15	1976-01-20	Ricciteili James A	Electronic security card and system for authenticating card ownership
US4447716A *	1982-03-01	1984-05-08	Seiichiro Aigo	Information card
JPH041683082 *	1984-01-31	1992-03-25	Tokyo Shibaura Electric Co	
US4650975A *	1984-08-30	1987-03-17	Casio Computer Co., Ltd.	IC card and an identification system thereof
US4641193A *	1984-12-07	1987-02-03	New York Institute Of Technology	Video display apparatus and method
JPS6339586A *	1986-06-30	1988-01-16	Toshiba Corp	Memory card
JPS63176193A *	1987-01-14	1988-07-20	Nec Corp	Information card
JPH0261680A	1988-08-26	1990-03-01	Seiko Instr Inc	Contact type heat fixing device
JPH0261680U	1988-10-27	1990-05-08		
JP2712497B2 *	1989-03-02	1998-02-10	キヤノン株式会社	Solid camera
US5237609A *	1989-03-31	1993-08-17	Mitsubishi Denki Kabushiki Kaisha	Portable secure semiconductor memory device
US5236372A *	1991-02-20	1993-08-17	Nec Corporation	No-insertion force connector assembly
JPH0557635A	1991-08-27	1993-03-09	Matsushita Electric Works Ltd	Driving tool
EP0532166B1 *	1991-09-11	1995-06-14	ITT INDUSTRIES, INC. (a Delaware corporation)	Memory card grounding apparatus
JP3231832B2	1991-11-26	2001-11-26	株式会社日立製作所	Semiconductor disk using flash memory as storage medium
TW261678	1991-11-26	1995-11-01	Hitachi Seisakusyo Kk	
FR2686171B1 *	1992-01-14	1996-09-06	Gemplus Card Int	MASS MEMORY CARD FOR MICROCOMPUTER WITH FACILITIES FOR EXECUTING INTERNAL PROGRAMS.
FR2698195B1 *	1992-11-19	1994-12-16	Gemplus Card Int	Encryption and authentication method and circuit for synchronous memory card.
ATS183888T *	1993-06-15	2011-08-15	Celltrace Llc	TELECOMMUNICATIONS SYSTEM
DE69318839T2 *	1993-10-22	1998-11-12	Molex Inc	System for discharging electrical charges in connection with memory card connectors

IPR2025-00645 Page 01820

JPH07302318A *	1994-03-09	1995-11-14	Seiko Epson Corp	Card type electronic device
IT1272863B *	1995-01-04	1997-07-01	Ausimont Spa	THERMOPROCESSABLE COPOLYMERS OF TETRAFLUOROETHYLENE
DE19536169A1 *	1995-09-29	1997-04-03	Ibm	Multifunctional chip card
US5999811A *	1996-02-16	1999-12-07	Ericsson, Inc.	Mobile telephone for roaming using dual mode/band equipment including SIM cards
JP3774260B2 *	1996-03-25	2006-05-10	株式会社ルネサステクノロジ	Memory card security system device and memory card thereof
US5772448A *	1996-04-02	1998-06-30	Compaq Computer Corporation	Edgecard circuit board
DE19617943C2 *	1996-04-29	1998-12-17	Mannesmann Ag	Process for making microprocessor cards accessible
US5828753A *	1996-10-25	1998-10-27	Intel Corporation	Circuit and method for ensuring interconnect security within a multi-chip integrated circuit package
US5839058A *	1996-11-01	1998-11-17	Ericsson Inc.	Recyclable cellular telephone and method and apparatus for supporting the use of a recyclable cellular telephone within a cellular telephone network
JPH10334205A *	1997-05-30	1998-12-18	Toshiba Corp	Ic card and memory package
US6094724A *	1997-11-26	2000-07-25	Atmel Corporation	Secure memory having anti-wire tapping
FR2773900B1 *	1998-01-22	2000-02-18	Gemplus Card Int	CARD WITH INTEGRATED CONTACT CIRCUIT (S), COMPRISING A DETACHABLE MINICARD
JPH11273400A	1998-03-24	1999-10-08	Hitachi Ltd	Storage
JPH11282989A *	1998-03-26	1999-10-15	Toshiba Corp	Portable electronic device
US6315195B1	1998-04-17	2001-11-13	Diebold, Incorporated	Transaction apparatus and method
FR2779849B1 *	1998-06-15	2000-07-28	Schlumberger Ind Sa	SECURE INTEGRATED CIRCUIT DEVICE USING COMPLEMENTARY BUS LINES
JP4029234B2 *	1998-07-16	2008-01-09	ソニー株式会社	Information processing apparatus and information processing method
US6401208B2 *	1998-07-17	2002-06-04	Intel Corporation	Method for BIOS authentication prior to BIOS execution
US5933328A *	1998-07-28	1999-08-03	Sandisk Corporation	Compact mechanism for removable insertion of multiple integrated circuit cards into portable and other electronic devices
GB9822697D0 *	1998-10-19	1998-12-09	Nokia Mobile Phones Ltd	Data card holder
FI107973B	1999-03-11	2001-10-31	Nokia Mobile Phones Ltd	Method and means for using option cards in a mobile station
JP3389186B2 *	1999-04-27	2003-03-24	松下電器産業株式会社	Semiconductor memory card and reading device
US6634561B1 *	1999-06-24	2003-10-21	Sandisk Corporation	Memory card electrical contact structure
JP3815936B2	2000-01-25	2006-08-30	株式会社ルネサステクノロジ	IC card
CN1218276C *	2000-04-28	2005-09-07	株式会社日立制作所	IC card
US20030112613A1 *	2002-10-22	2003-06-19	Hitachi, Ltd.	IC card
TW516296B *	2000-07-20	2003-01-01	High Tech Comp Corp	Plug-and-play SIM card holder
JP4671484B2	2000-10-11	2011-04-20	ケル株式会社	Card connector
TW495110U	2000-11-27	2002-07-11	Kinpo Elect Inc	Common seat for memory card
GB2377825A	2001-07-19	2003-01-22	Inventec Appliances Corp	Device with expansion adaprot slotted into battery
US6612492B1	2002-06-06	2003-09-02	Chant Sincere Co., Ltd.	Four-in-one memory card insertion port
DE10303740B4 *	2003-01-30	2006-09-14	Infineon Technologies Flash Gmbh & Co. Kg	Security memory card and manufacturing process

* Cited by examiner, † Cited by third party

Cited By (135)

IPR2025-00645 Page 01821

Publication number	Priority date	Publication date	Assignee	Title
CN101765242A *	2008-12-25	2010-06-30	深圳富泰宏精密工业有限公司	User identification card and connector thereof as well as portable communication device provided with connector
Family To Family Citations				
TW460846B *	1998-12-10	2001-10-21	Toshiba Corp	Data recording media having certification information
JP3822768B2 *	1999-12-03	2006-09-20	株式会社ルネサステクノロジ	IC card manufacturing method
JP3815936B2 *	2000-01-25	2006-08-30	株式会社ルネサステクノロジ	IC card
CN1218276C *	2000-04-28	2005-09-07	株式会社日立制作所	IC card
US20030112613A1 *	2002-10-22	2003-06-19	Hitachi, Ltd.	IC card
US7295443B2	2000-07-06	2007-11-13	Onspec Electronic, Inc.	Smartconnect universal flash media card adapters
US6438638B1	2000-07-06	2002-08-20	Onspec Electronic, Inc.	Flashtoaster for reading several types of flash-memory cards with or without a PC
US6824063B1	2000-08-04	2004-11-30	Sandisk Corporation	Use of small electronic circuit cards with different interfaces in an electronic system
KR20020016430A *	2000-08-25	2002-03-04	윤종용	Multimedia modular card, modular card operating device and incorporated multimedia system
US7107378B1	2000-09-01	2006-09-12	Sandisk Corporation	Cooperative interconnection and operation of a non-volatile memory card and an input-output card
US7137003B2 *	2001-02-27	2006-11-14	Qualcomm Incorporated	Subscriber identity module verification during power management
JP2002259869A *	2001-03-01	2002-09-13	Fujitsu Ltd	Method of controlling portable equipment, method of preventing illicit use of ic card, program for changing setting of portable equipment, and program for preventing illicit use of ic card
US7066819B2	2001-03-29	2006-06-20	Interactive Telegames, Llc	Method and apparatus for identifying game players and game moves
US20020183118A1 *	2001-05-30	2002-12-05	Scott Wolinsky	Method and apparatus for simulating game accessories
AU2003220678A1	2002-04-08	2003-10-27	Socket Communications, Inc	Wireless enabled memory module
US7090256B1	2002-04-26	2006-08-15	Sandisk Corporation	Retractable card adapter
US20030211888A1	2002-05-13	2003-11-13	Interactive Telegames, Llc	Method and apparatus using insertably-removable auxiliary devices to play games over a communications link
JP2004126889A *	2002-10-01	2004-04-22	Sharp Corp	Electronic seal, removable memory medium, advance authentication system, portable device, cellular telephone system, and vihicular starting controller
US7137052B2 *	2002-10-23	2006-11-14	Micron Technology, Inc.	Testing a multibank memory module
US7366803B2	2002-11-13	2008-05-06	Sandisk Corporation	Universal non-volatile memory card used with various different standard cards containing a memory controller
US8037229B2	2002-11-21	2011-10-11	Sandisk Technologies Inc.	Combination non-volatile memory and input-output card with direct memory access
US20050055479A1 *	2002-11-21	2005-03-10	Aviad Zer	Multi-module circuit card with inter-module direct memory access
JP4152178B2 *	2002-12-03	2008-09-17	株式会社ルネサステクノロジ	Memory card and electronic device
JP2004240795A *	2003-02-07	2004-08-26	Renesas Technology Corp	Nonvolatile storage device
US20040164170A1 *	2003-02-25	2004-08-26	Marcelo Krygier	Multi-protocol memory card
JP4308551B2 *	2003-03-06	2009-08-05	株式会社ルネサステクノロジ	Memory card and host device
JP3958243B2 *	2003-04-14	2007-08-15	松下電器産業株式会社	IC card and its OS startup method

IPR2025-00645 Page 01822

US7305535B2 *	2003-04-17	2007-12-04	Sandisk Corporation	Memory cards including a standard security function
US20040245620A1 *	2003-06-03	2004-12-09	Jackson Hsieh	Memory card capable of indicating an inserting direction
EP1647136A4	2003-06-09	2009-07-08	Wavien Inc	A light pipe based projection engine
KR20100107057A *	2003-07-03	2010-10-04	로데사스 일렉트로닉스 카부시키가이샤	Semiconductor card device
US6902412B2 *	2003-08-26	2005-06-07	Motorola, Inc	Apparatus for intrinsically safe power interface
US7237719B2 *	2003-09-03	2007-07-03	Stmicroelectronics, Inc.	Method and apparatus for a USB and contactless smart card device
JP4412947B2	2003-09-08	2010-02-10	株式会社ルネサステクノロジ	Memory card
JP2005085089A *	2003-09-10	2005-03-31	Renesas Technology Corp	Ic card and manufacturing method thereof
JP2007041629A *	2003-11-04	2007-02-15	Renesas Technology Corp	Memory card and semiconductor device
US7209995B2 *	2003-12-09	2007-04-24	Sandisk Corporation	Efficient connection between modules of removable electronic circuit cards
KR101083366B1 *	2003-12-11	2011-11-15	삼성전자주식회사	Memory system and method for setting data transfer speed between host and memory card
JP4072503B2 *	2004-02-04	2008-04-09	シャープ株式会社	IC card with built-in coprocessor for auxiliary operation and control method thereof
US7112082B2 *	2004-03-17	2006-09-26	Wieson Technologies Co., Ltd.	Miniature memory card/SIM card dual-function connector
US8267780B2	2004-03-31	2012-09-18	Nintendo Co., Ltd.	Game console and memory card
US7771280B2 *	2004-03-31	2010-08-10	Nintendo Co., Ltd.	Game console connector and emulator for the game console
US7837558B2 *	2004-03-31	2010-11-23	Nintendo Co., Ltd.	Game console and emulator for the game console
US8016681B2	2004-03-31	2011-09-13	Nintendo Co., Ltd.	Memory card for a game console
KR101149887B1 *	2004-04-01	2012-06-11	삼성전자주식회사	Multi-channel memory card and control method thereof
US7710736B2	2005-08-02	2010-05-04	Sandisk Corporation	Memory card with latching mechanism for hinged cover
US7748726S2 *	2004-04-16	2009-02-03	Sandisk Corporation	Memory card with two standard sets of contacts and a hinged contact covering mechanism
US7152801B2	2004-04-16	2006-12-26	Sandisk Corporation	Memory cards having two standard sets of contacts
JP4651332B2	2004-04-26	2011-03-16	ルネサスエレクトロニクス株式会社	Memory card
JP2005322109A *	2004-05-11	2005-11-17	Renesas Technology Corp	Ic card module
JP4591754B2 *	2004-07-30	2010-12-01	ソニー株式会社	COMMUNICATION DEVICE, ELECTRONIC DEVICE, AND COMMUNICATION SYSTEM
KR100579053B1 *	2004-08-26	2006-05-12	삼성전자주식회사	Method of multi-interfacing between smart card and memory card and multi-interface card
CN100465933C *	2004-09-07	2009-03-04	瑞昱科技股份有限公司	Removable electronic device and its method
US7269383B2 *	2004-09-15	2007-08-28	Inventec Appliances Corp.	Apparatus and a method for extending phone book records of a subscriber identification module (SIM) card
TWI282517B *	2004-10-15	2007-06-11	C One Technology Corp Ltd	Multi-functional integrated circuit card module having mixed interface
JP4515218B2 *	2004-10-22	2010-07-28	ソニー株式会社	Memory card
WO2006045344A1 *	2004-10-29	2006-05-04	Telecom Italia S.P.A.	Method for establishing a secure logical connection between an integrated circuit card and a memory card through a terminal equipment
JP4586966B2 *	2004-10-29	2010-10-20	三洋電機株式会社	Memory element
CN100375102C *	2004-11-30	2008-03-12	國际商业机器公司	Non-contact card reader and information processing system
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card

IPR2025-00645 Page 01823

JP2006253430A	2005-03-11	2006-09-21	Renesas Technology Corp	Semiconductor device and its manufacturing method
JP2006268459A	2005-03-24	2006-10-05	Ricoh Co Ltd	Nonvolatile memory card and shape conversion adapter
US7729660B2 *	2005-04-15	2010-06-01	Sony Corporation	Communication device, non-contact type IC card mounting same, and information apparatus
JP4864346B2 *	2005-05-18	2012-02-01	ソニー株式会社	Memory card and card adapter
EP1727080A1 *	2005-05-27	2006-11-29	Axalto S.A.	SIM with double sets of contacts protected against short-circuit
JP2007011708A	2005-06-30	2007-01-18	Ricoh Co Ltd	Integrated-type memory card and shape transformation adaptor
JP2007065956A *	2005-08-31	2007-03-15	Renesas Technology Corp	Memory card
TWM284108U *	2005-09-02	2005-12-21	Tai Sol Electronics Co Ltd	Connector for a card with a function for avoiding a short cut
KR101155220B1 *	2005-09-13	2012-06-13	엘지전자 주식회사	Uim card including external memory in mobile phone
US7529491B2 *	2005-09-15	2009-05-05	Xerox Corporation	Apparatus and method for adapting a machine to communicate with customer replaceable unit monitors having different interface formats
JP4944442B2 *	2005-12-28	2012-05-30	株式会社エヌ・ティ・ティ・ドコモ	Mobile communication terminal system
EP1804196A1 *	2005-12-29	2007-07-04	Motorola, Inc.	Method and devices for data access in combined SIM and mass storage cards
US7193161B1 *	2006-02-15	2007-03-20	Sandisk Corporation	SiP module with a single sided lid
WO2007094624A1 *	2006-02-17	2007-08-23	Ktfreetel Co., Ltd.	Ic card, terminal with ic card and initializing method thereof
JP2007280347A *	2006-03-14	2007-10-25	Ricoh Co Ltd	Memory card and memory card control changeover method
US20090100238A1 *	2006-03-14	2009-04-16	Masaharu Adachi	Memory card and memory card control changeover method
JP2007317170A *	2006-04-28	2007-12-06	Renesas Technology Corp	Ic module and cellular phone
US9198025B2 *	2006-05-04	2015-11-24	Sandisk Il Ltd.	High-capacity SIM storage control
US8060142B2 *	2006-05-24	2011-11-15	Lg Electronics Inc.	Method for reducing power consumption for detachable card and mobile communication terminal thereof
US8843768B2 *	2006-09-05	2014-09-23	Netapp, Inc.	Security-enabled storage controller
WO2008029206A2 *	2006-09-05	2008-03-13	Nokia Corporation	Device interface
TW200816056A *	2006-09-27	2008-04-01	Renesas Tech Corp	IC card and IC card socket
DE102006045906A1 *	2006-09-28	2008-04-17	Infineon Technologies Ag	Module with a controller for a chip card
KR100770220B1	2006-10-16	2007-10-26	삼성전자주식회사	Memory card and method of manufacturing the same
US7827323B2 *	2006-12-08	2010-11-02	Marvell Israel (M.I.S.L.) Ltd.	System and method for peripheral device communications
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US8079528B2 *	2007-01-10	2011-12-20	Taiwan Semiconductor Manufacturing Co., Ltd.	Input/output pads placement for a smart card chip
JP2008257506A *	2007-04-05	2008-10-23	Renesas Technology Corp	Semiconductor device
US7572152B2 *	2007-06-27	2009-08-11	Sandisk Il Ltd.	Memory interface card with SIM functions
JP2009032214A *	2007-07-24	2009-02-12	Renesas Technology Corp	Semiconductor integrated circuit, display device, and electronic circuit
JP2009054061A *	2007-08-29	2009-03-12	Renesas Technology Corp	Semiconductor device
KR20090025530A *	2007-09-06	2009-03-11	삼성전자주식회사	Subscriber identify module card and terminal connectable of the same
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US7983099B2	2007-12-20	2011-07-19	Mosaid Technologies	Dual function compatible non-volatile memory device

IPR2025-00645 Page 01824

			Incorporated	
CN101578607B *	2008-05-08	2012-05-30	鸿富锦精密工业（深圳）有限公司	Pad and circuit board used thereby
US8473974B2 *	2008-05-13	2013-06-25	Nbcuniversal Media, Llc	Activation system and method for activating an optical article
US8387876B2 *	2008-05-13	2013-03-05	Nbcuniversal Media, Llc	Activation system and method for activating an optical article
JPS20217282 *	2008-08-06	2013-06-05	富士通コンポーネント株式会社	Memory card connector
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US8782433B2 *	2008-09-10	2014-07-15	Inside Secure	Data security
US9653004B2	2008-10-16	2017-05-16	Cypress Semiconductor Corporation	Systems and methods for downloading code and data into a secure non-volatile memory
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
KR101555637B1 *	2009-03-27	2015-09-24	삼성전자주식회사	Smart card
CN101587557B *	2009-06-29	2015-12-09	北京握奇数据系统有限公司	A kind of Subscriber Identity Module and manufacture method thereof and system
EP2465040A1	2009-08-14	2012-06-20	SanDisk IL Ltd.	Dual interface card with backward and forward compatibility
JP4906135B2 *	2009-10-21	2012-03-28	ルネサスエレクトロニクス株式会社	Memory card
US8275188B2 *	2009-12-03	2012-09-25	Condel International Technologies Inc.	Systems and methods for managing storage devices
CN1047945238 *	2009-12-07	2018-10-12	三星电子株式会社	Storage card and electronic device
US8666386B2 *	2010-05-03	2014-03-04	Apple Inc.	Wireless network authentication apparatus and methods
CN102289710A *	2010-06-18	2011-12-21	黄金富	Secure digital (SD) memory card having function of subscriber identity model (SIM) card
CN102289711A *	2010-06-18	2011-12-21	黄金富	SD (Secure Digital) memory card for mobile phone payment and with function of contactless smart card
JP5396415B2 *	2011-02-23	2014-01-22	株式会社東芝	Semiconductor device
WO2013013189A2	2011-07-20	2013-01-24	Visa International Service Association	Security gateway communication
US9635549B2	2011-09-01	2017-04-25	Nokia Technologies Oy	Providing subscriber identity module function
US8649820B2 *	2011-11-07	2014-02-11	Blackberry Limited	Universal integrated circuit card apparatus and related methods
USD667830S1 *	2011-11-29	2012-09-25	Samsung Electronics Co., Ltd.	SD memory card
EP2645307B1 *	2012-03-29	2020-11-04	Uros Technology S.à r.l	Apparatus having a plurality of SIMs
US8936199B2	2012-04-13	2015-01-20	Blackberry Limited	UICC apparatus and related methods
USD703208S1	2012-04-13	2014-04-22	Blackberry Limited	UICC apparatus
USD701864S1	2012-04-23	2014-04-01	Blackberry Limited	UICC apparatus
WO2013166278A1	2012-05-02	2013-11-07	Visa International Service Association	Small form-factor cryptographic expansion device
US8904078B2 *	2012-10-22	2014-12-02	Lenovo Enterprise Solutions (Singapore) Pte. Ltd.	High speed serial peripheral interface system
USD707682S1 *	2012-12-05	2014-06-24	Logomotion, S.R.O.	Memory card
CN103164737A *	2013-01-29	2013-06-19	三星半导体(中国)研究开发有限公司	High-density memory smart card module and manufacture method thereof

IPR2025-00645 Page 01825

CN104795651B *	2014-01-22	2017-10-13	富士康(昆山)电脑接插件有限公司	Electronic card coupler
EP2908593B1 *	2014-02-12	2018-08-01	Alcatel Lucent	Apparatuses, methods and computer programs for a base station transceiver and a mobile transceiver
KR10216817081	2014-06-30	2020-10-20	삼성전자주식회사	Memory card
USD783622S1 *	2015-08-25	2017-04-11	Samsung Electronics Co., Ltd.	Memory card
USD783621S1 *	2015-08-25	2017-04-11	Samsung Electronics Co., Ltd.	Memory card
DE102016110780A1 *	2016-06-13	2017-12-14	Infineon Technologies Austria Ag	Smart card module and method for manufacturing a smart card module
CN1063041968 *	2016-08-03	2020-06-09	惠州Tcl移动通信有限公司	FDN-based data flow control method and system
US10027079B2 *	2016-10-27	2018-07-17	Amphenol Shouh Min Industry (Shen Zhen) Co., Ltd.	Connector applied to USF card and micro SD card
KR20190083242A	2018-01-03	2019-07-11	삼성전자주식회사	Memory card and electronic system

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
CN1218276C	2005-09-07	IC card
US7201581B2	2007-04-10	IC card
US7296754B2	2007-11-20	IC card module
JP4937736B2	2012-05-23	Memory card with standard security functions
JP2007183776A	2007-07-19	Semiconductor device
JP2004133843A	2004-04-30	Ic module provided with three types of interfaces, 3-way sim and sim holder, and 3-way ic card and ic card holder
WO2005008453A1	2005-01-27	Universal serial bus driving device having a function of smart card reader
KR100745514B1	2007-08-02	Ic card
JP4761479B2	2011-08-31	IC card
CN1932857A	2007-03-21	Integrated circuit card
CN1916944A	2007-02-21	Integratel circuit cards
KR100743084B1	2007-07-27	Ic card
JP2006202336A	2006-08-03	Non-volatile memory device
CN1434379A	2003-08-06	Method for executing operation to intelligent card from computer

Priority And Related Applications

Child Applications (3)

Application	Priority date	Filing date	Relation	Title
CN200610099656A	2000-04-28	2000-04-28	Division	Cellphone
CN200510078595SA	2000-04-28	2000-04-28	Division	IC card
CN200610101765SA	2000-04-28	2000-04-28	Division	Non-volatile storage device

Priority Applications (1)

Application	Priority date	Filing date	Title

IPR2025-00645 Page 01826

PCT/JP2000/002823	2000-04-28	2000-04-28	ic card

Legal Events

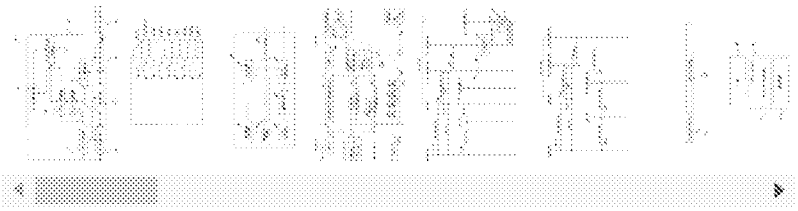
Date	Code	Title	Description
2003-10-29	PB01	Publication	
2003-10-29	C06	Publication	
2004-01-07	C10	Entry into substantive examination	
2004-01-07	SE01	Entry into force of request for substantive examination	
2005-09-07	GR01	Patent grant	
2005-09-07	C14	Grant of patent or utility model	
2017-06-16	CF01	Termination of patent right due to non-payment of annual fee	**Granted publication date**: 20050907 **Termination date**: 20160428

About Send Feedback Public Datasets Terms Privacy Policy

Patents JP4624732

how to access

Images (47)



Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 7 more classifications

JP4624732B2
Japan

Download PDF Find Prior Art Family

Other languages: Japanese

Inventor: 佳彦 高木, 睦文 菊地

Worldwide applications

2004 JP WO TW US TW KR EP KR 2005 IL

Application JP2004197453A events

2003-07-16 Priority to JP2003275672
2004-07-02 Application filed by パナソニック株式会社
2004-07-02 Priority to JP2004197453A
2005-02-24 Publication of JP2005050320A
2011-02-02 Application granted
2011-02-02 Publication of JP4624732B2
Status Active
2024-07-02 Anticipated expiration

Info: Patent citations (70), Cited by (30), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (16) Hide Dependent

1. An access method from a device to a memory device,
The device is
Transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area and the verification information on the designation information together;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification information, and verifying the designation information using the verification information;
If the verification is successful, executing the processing instruction;
Having an access method.

2. An access method from a device to a memory device,
The device is
Sharing with the memory device possible area information regarding an accessible area to the memory device; and
Referring to the possible area information and transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area and the verification information on the designation information together;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification information, and verifying the designation information using the verification information;
If the verification is successful, executing the processing instruction;
Having an access method

3. An access method from a device to a memory device,
The device is
Sharing a verification key with the memory device;
Transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area together with verification data obtained by encrypting verification information related to the specified information with the verification key;
The memory device is
Receiving the specified information;

IPR2025-00645 Page 01828

Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

4. An access method from a device to a memory device,
The device is
Sharing with the memory device possible area information regarding an accessible area to the memory device, and
Sharing a verification key corresponding to the accessible area with the memory device;
Referring to the possible area information and transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area together with verification data obtained by encrypting verification information related to the specified information with the verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

5. An access method from a device to a memory device,
The device is
Using the first processing command with the memory device, sharing the possible area information regarding the accessible area to the memory device;
Referring to the possible area information and using a second processing command to transmit designation information for designating an access area to the memory device;
Using the second processing command, a process command to the access area and verification information related to the designation information are transmitted together,
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification information, and verifying the designation information using the verification information;
If the verification is successful, executing the processing instruction;
Having an access method

6. An access method from a device to a memory device,
The device is
Sharing a verification key with the memory device using a first processing command;
Using a second processing command to send designation information for designating an access area to the memory device;
Using the second processing command, and sending together the processing instruction to the access area and verification data obtained by encrypting the verification information related to the designation information with the verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

7. A memory device that is read and written from a device,
Processing instruction receiving means for receiving specification information specifying an area to be accessed and receiving verification information based on the specification information together with a read or write command;
A designation information verification means for performing a verification process on the designation information using the verification information;
A storage area for storing data;
A storage area access means for reading from or writing to the designated area of the storage area in response to the processing instruction when the verification process is successful,
Data transmission means for transmitting data read by the storage area access means to the device;
Data receiving means for receiving write data from the device;
A memory device comprising:

8. 8. The memory device according to claim 7, wherein the verification process of the specified information verification unit is performed using the verification information and a verification key.

9. 9. The memory device according to claim 8, further comprising verification key sharing means for sharing the verification key with the device.

10. 8. The memory device according to claim 7, further comprising possible area information sharing means for sharing possible area information indicating an accessible area to the memory device with the device.

11. An information device that reads and writes memory devices,
A designation information determining means for deciding an area to be read or written and determining designation information for designating the area;
Verification information generating means for generating the verification information from the designation information;
A processing command transmission means for transmitting the designation information, and sending the verification information and a processing command for reading or writing together;
If the processing instruction is a write, data transmission means for transmitting data to the memory device,
If the processing instruction is read, data receiving means for receiving data from the memory device;
Data storage means for storing data to be transmitted to the memory device or storing data received from the memory device;
An information device comprising:

12. 12. The information apparatus according to claim 11, wherein the verification information generation process of the verification information generation unit is performed using the designation information and a verification key.

13. 13. The information apparatus according to claim 12, further comprising verification key sharing means for sharing the verification key with the memory device.

14. 12. The information apparatus according to claim 11 , further comprising possible area information sharing means for sharing possible area information indicating an accessible area to the memory device with the memory device.

15. An access method from a device to a memory device,
The device is
Transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area and verification data obtained by encrypting verification information related to the specified information with a verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and a verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

16. An access method from a device to a memory device,
The equipment is
Sharing possible area information related to an accessible area to the memory device using a first processing command;
Sharing a verification key corresponding to the accessible area using a first processing command;
Using a second processing command to send designation information for designating an access area to the memory device;
Transmitting a processing command to the access area using a second processing command and verification data obtained by encrypting verification information related to the designation information with the verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

Description

The present invention relates to a memory card that is used by being inserted into a terminal such as a PC or a mobile phone, and an access method for the memory card.

Conventionally, a memory card is inserted into a terminal, and the terminal stores data.
An example of a conventional memory card will be given below (for example, see Patent Document 1 below).

The card has a command terminal (CMD line) for receiving various commands from the terminal and returning a response to the command, and a data terminal (DAT line) for receiving data input and outputting data.

In the example of the conventional memory card shown in FIG. 46, the terminal 4602 is a CMD line, the terminals 4607, 4608, and 4609 are DAT lines, which are DAT0, DAT1, and DAT2, respectively. A terminal 4601 is a CD / DAT 3 that serves both as data input / output and card detection (CD). As for DAT0 to DAT3, there are a mode in which only DAT0 is used and a mode in which DAT0 to DAT3 are simultaneously used and a transfer rate four times that in the case of using only DAT0 is realized.

Next, the in-card module configuration of the conventional card will be described with reference to FIG.

The in-card module includes processing command receiving means 4701 for receiving commands and sending responses connected to the CMD line 4602, and data transmitting / receiving means 4702 for sending and receiving data connected to the DAT lines 4607, 4608, 4609 and 4601. The storage area 4704 and storage area access means 4703 for reading and writing data to and from the storage area 4704 according to the received command.

Next, the processing operation at the time of data reading in the conventional memory card will be described. Here, the data output is set to a mode that uses only the DAT0 terminal 4607, but a mode in which the DAT1 terminal 4608, the DAT2 terminal 4609, and the DAT3 terminal 4601 are used together may be used.

First, the terminal transmits a data read command to the CMD line 4602 of the card. This read command has the format shown in FIG. 7 and is composed of a 6-bit command code 401 and a 32-bit command argument 402. The command argument in the data read command stores a read start address.

The processing command receiving unit 4701 that has received the command from the terminal refers to the command code 401 and recognizes that it is a data read command.

Next, the processing command receiving means 4701 refers to the command argument 402 to check whether the specified address is correct, that is, whether the specified address is within the range supported by the card. If is not correct, a response code indicating an error is returned as a response. If the address is correct, a response code indicating that the address is normal is returned.

The processing command receiving means 4701 sends a response to the terminal, and then makes a read request to the storage area access means 4703 together with the designated address.

The storage area access unit 4703 reads data from the specified address in the storage area 4704 and transmits it to the data transmission / reception unit 4702.

The data transmission / reception means 4702 outputs read data to the terminal through the DAT0 line 4607.

Such a memory card can be freely read and written by designating an address from a terminal.
JP 2003-91704 A

In the memory card as described above, when it is desired to restrict access using a specific area of the flash memory as a security protection area and access is possible only from a specific terminal to which access is permitted, it is possible to perform flexible authentication using card commands. However, the APDU (Application Protocol Data Unit), which is the standard command format for IC cards, can only send and receive 256 bytes of data, and because of the half-duplex protocol, it receives a response each time a command is sent from the host. Therefore, high-speed data transfer is difficult. Therefore, a method of performing data transfer using a memory card command after performing authentication processing using a method flexibly matched to a security policy using an IC card command can be considered. It is difficult to confirm that the applications on the host that issued the card command are the same.

Therefore, if the information generated during the authentication process using the IC card command is included in the memory card command as verification data for verifying the identity of the IC card command and the issuer of the memory card command, the command argument is accessed. The area designation information (address to be accessed, etc.) and verification data for authentication are included, but the size of the command argument 402 of the data read command is fixed to 32 bits as described above, so authentication is performed to improve security. If the size of the verification data is increased, the length of the access area designation information is shortened and the accessible area is limited. On the other hand, if the size of the verification data is reduced, the security strength is lowered.

If the format of the conventional data read command is changed to solve this problem, there is a possibility that the conventional memory card cannot be accessed.

In addition, if the conventional data read command and the data read command to the memory card having the security protection area coexist separately, it is necessary to switch the command depending on the type of the memory card on the terminal side. Access to the card is complicated, making it difficult for the terminal to use. Therefore, it is necessary to define a command for transmitting verification data and a memory card command for reading or writing data, and to access the security protection area by combining the two commands. The identity of the command issuer cannot be confirmed between.

Therefore, in the present invention, when accessing an area where access is not restricted in the memory card, a memory card command represented by the above-mentioned data read command is used. After the access area designation information is sent to the memory card by the memory card command for designating the access area, it is shared between the host and the memory card using a flexible authentication process using the IC card command or is shared in advance. Sending the memory card command for reading or writing the security protection area including the key information and the verification data for authentication generated using the access area specification information to the memory card, and sending the data to the security protection area Write, data from security protection area An access method that enables access to the security protection area without changing the format of the memory card command and reducing the security even with a small number of command arguments by adopting a two-stage command configuration of reading. The purpose is to provide.

A first invention is an access method from a device to a memory device, wherein the device transmits designation information designating an access area to the memory device, a processing instruction to the access area, and the designation information verification information, and the memory device receives the specified information; receives the processing instruction and the verification information; and verifies the specified information using the verification information And a step of executing the processing instruction when the verification is successful.

According to the present invention, the access area designation and security protection area access commands are separated, and the verification data is included in the security protection area access command so that the access area designation and the security protection area access command are performed. The memory device can verify that the device application that holds the verification key shared between the device application that issued the certificate and the memory card, that is, the device application that has the authority to access the security protection area is the same. It becomes. In addition, with the two-stage configuration of access area designation and security protection area access commands, using memory card commands for conventional memory access avoids the complexity of the command, and security with fewer command arguments It is possible to access the security protection area without degrading the security level.

A second invention is a method for accessing a memory device from a device, wherein the device shares with the memory device, the available area information related to an accessible area to the memory device, and the available area information. The step of transmitting designation information for designating an access area to the memory device, a process command for processing to the access area, and verification information relating to the designation information, and the memory device, Receiving the designation information; receiving the processing instruction and the verification information; verifying the designation information using the verification information; and executing the processing instruction if the verification is successful. And an access method

According to the present invention, it is possible to explicitly set whether or not each area in the security protection area can be accessed by the security protection area access command.

A third invention is a method for accessing a memory device from a device, wherein the device shares a verification key with the memory device, and designation information for designating an access area to the memory device. Transmitting the processing instruction to the access area, and verification data obtained by encrypting the verification information related to the specified information with the verification key; and the memory device is configured to transmit the specified information. Receiving the processing instruction and the verification data, verifying the designation information using the verification data and the verification key, and executing the processing instruction if the verification is successful And an access method.

According to the present invention, the strength of security can be improved by updating the verification key as necessary.

A fourth invention is a method for accessing a memory device from a device, wherein the device shares with the memory device shared area information regarding an accessible area to the memory device, and the memory device And a step of sharing a verification key corresponding to the accessible area, referring to the accessible area information, transmitting designation information for designating an access area to the memory device, and Transmitting a processing command and verification data obtained by encrypting verification information related to the specified information with the verification key; the memory device receiving the specified information; the processing command; Receiving verification data and verifying the specified information using the verification data and the verification key; If successful in verification, an access method and a step of executing the processing instructions.

According to the present invention, when access is not made to an area in which only the device can read and write, access by a security protection area access command can be invalidated, security strength can be improved, and a verification key can be obtained. The security strength can be improved by updating as necessary.

A fifth invention is a method for accessing a memory device from a device, wherein the device uses the first processing command to obtain possible area information relating to an accessible area to the memory device. A step of sharing, a step of referring to the possible area information and using a second processing system command to transmit designation information specifying an access area to the memory device, and the second processing system command Using the processing command to the access area and the verification information related to the designation information in combination, the memory device receiving the designation information, the processing command and the verification information. Receiving the verification information using the verification information, and executing the processing instruction if the verification is successful. Tsu and up, which is an access method having a.

According to the present invention, it becomes possible to separate sharing of information about accessible areas by a command processing system different from the access area designation and security protection area access commands, and the device application that has designated the access area and security protection. The memory device can verify that the device application that has issued the area access command is the same as the device application that has the authority to access the security protection area.

A sixth invention is an access method from a device to a memory device, wherein the device shares a verification key with the memory device using a first processing command, A step of transmitting designation information for designating an access area to the memory device using a processing command; a processing instruction for the access area using the second processing command; and verification of the designation information A step of transmitting verification data obtained by encrypting information with the verification key, a step of receiving the designation information, a step of receiving the processing information and the verification data, and the designation information being received by the memory device. And using the verification data and the verification key, and executing the processing instruction when the verification is successful. It is Seth method.